A.M. Turing Award
An Interview with Martin Hellman
Recipient of the 2015 ACM Turing Award
Interviewer: Hugh Williams
May 19, 2017, Palo Alto, California, USA

HW: Hugh Williams, interviewer
MH: Martin Hellman, ACM Turing Award Recipient

HW: Hello. My name is Hugh Williams. It is the 19th day of May, 2017, and I am sitting in the home of Stanford Professor Emeritus Martin Hellman. I am here to interview Martin for the ACM Turing Award Winners project.

Now Marty, tell me a bit about your ancestors, where they came from, say up to the time you were born.

MH: My father's family came from what my grandfather always called "Russia," but it was probably Lithuania or Belarus, if I can pronounce that. But when the czar's in charge and you're Jewish, it's "Russia." He came probably 1904. He'd been drafted into the czar's army once and with the Russo-Japanese War on the horizon, he was going to be drafted again. He left a wife and two children, my two oldest uncles, in Russia, came and worked in New York as a tailor, and sent over for them. My grandmother, the family story is probably true that, she had to sneak across the border. The czar didn't like Jews, but he didn't like them leaving either, and so she had to bribe border guards with these two toddlers in tow.

My father was born in this country in 1908. I used to think he was the first one born in this country, but it turns out there was another boy born before him who died at about two years of age. I only learned that when I found a picture that was taken about 1906 and there's a baby in it. It can't be my father.

My mother's family came a little bit later, maybe 1910, something like that, before World War I, from what was then the Austro-Hungarian Empire. It was really fun when I gave the Turing Lecture, my Turing Lecture because Whit gave his separately, it was in Vienna and it was in the Imperial Palace. I was thinking what my grandparents would think, long since passed of course, if they could see their grandson being honored and giving this lecture in this ballroom basically in the Imperial Palace. Now I think it would be Poland, but I'm not sure.

My mother's family, he started out with a pushcart and then had a feather store when feathers were in fashion. He ended up with two apartment buildings in the

Bronx, which is where I grew up. I mean not luxury buildings by any means. Walk-up. Actually most Americans would see them as slums probably, but that's where I lived for the first five years of my life and we didn't think of it that way.

My father's family had fun. My mother's family had money. [laughs] I think the two of them together were able to have fun with a little bit of money. They took a trip cross-country in 1940, when that was quite an adventuresome thing to do.

I was born in October 1945. I have an older brother born in 1942. I was born October '45, right after World War II ended. One of the things that I only thought about starting about 35 years ago when I was doing a lot of personal work was what it was like for my mother, pregnant with me and with a two-and-a-half-year-old, my older brother, to put my father on a troop train headed for the west coast. Every time I think about it, it hits me. I had never thought about that before. I mean just what it must have been like for her. Fortunately when he got on the troop ship in Seattle… well, he didn't know where he was going. When he got to Hawaii, they said, "Hellman, you get off here instead of Okinawa," so he actually had a pretty easy time of it given that it was wartime. But with the difficulty of bringing those millions of men back, and some women but mostly men, from overseas, he didn't get back until I was six months old, in I think March of '46.

You said from ancestry through when I was born. Did that cover it?

HW: Pretty good. What did your parents do subsequent to your birth?

MH: Well, even before my birth, my father had majored in physics. He'd actually gotten a teaching position in the New York City high school system as a physics teacher around '39, something like that. He'd gotten out of school during the Depression and was lucky to get a job as a timekeeper in a factory. But then he got this plum job paying maybe 50 bucks a week or something like… Maybe less. Maybe 30 bucks a week. I don't know. But it was a steady job, steady paycheck as a teacher.

My mother had intended to be a teacher too, but jobs were really hard to get. In those days, there were also prejudices against all groups including Jews. I mean not all groups, but all minority groups including Jews. It was hard, harder for Jews to get teaching positions. So she was a secretary initially in private industry. Then when I was, oh, about 10, she started working as a secretary in the school system, and then became a substitute teacher actually later.

Then of course my father was in the service during the war, actually quite a bit of time before he was shipped overseas. Then he taught. And he stayed in the Army Reserves, which he always loved. He died in 2007, and when I used to go back to New York to visit, he lived about 30 miles from West Point. He loved going up to West Point and getting saluted. Because he had the sticker on his car that said he was a retired reserve officer, and they would salute him going through the gate, and he loved that.

My uncle also taught physics, which is important – my father's younger brother by two years – because he was my physics teacher.

HW: What are your earliest memories?

MH: Oh, earliest memories? When I was five, we spent a summer up in the Adirondacks. We rented a bungalow. I remember usually though we tent camped, because that was cheaper, and we'd go for two weeks at a time. But the bungalow was maybe a month. Tent camping, having fires, cooking over the fire. Oh, and Rudd Pond State Park, New York State Park, which was actually in the Catskills rather than the Adirondacks, where we did a lot of tent camping. There was the local farmer Earl – funny what you remember, I was about eight – and he had a dairy farm, but he would deliver ice to the campers and sell ice to us. He used to let me come and help him take care of the cows, which I loved doing, so that was a fond memory.

My older, Howie, let me tag along. My younger brother by three… We were three years apart, older, and I'm in the middle. Younger brother couldn't keep up being six years behind at this point, but Howie let me tag along. He made fun of me, his friends made even more fun of me, but I loved tagging along, especially since when I was about seven or eight, I felt friendless and it was really nice to have this older brother.

HW: Tell me a bit about your siblings and their education.

MH: Well, okay. My older brother Howie or Howard, younger brother Steve, we all agreed we weren't going to be teachers. We didn't want to follow in my father's footsteps. [laughs] It's really funny. My older brother of course became a teacher in the New York City high school system, a science teacher, and my younger brother for a while was a teacher, and here I am, a professor.

But I'll never forget when I was finishing my PhD, my advisor Tom Cover asked me if I had thought about teaching, because I'd done a very good PhD thesis and was actually able to get a teaching position at MIT in 1969 based on that thesis. Tom said to me, "Have you thought about teaching?" I said, "No, I don't want to be poor." I mean I was really naïve. I didn't know the difference between high school teachers and Stanford professors, especially in engineering and consulting and starting companies, which actually wasn't that big a thing back then.

But I also had formed that opinion when I wasn't going to get married till I was 35. I wanted to see the world. When we travelled as a kid, when I was a kid and we travelled, it was tent camping, it was staying inexpensive motels. If we had to stop at a restaurant to eat, I knew to order the hamburger. The idea that a company would fly me places… I mean the first time I flew in an airplane was in my senior year of college when I went interviewing. They would fly you places, put you up in

nice hotels, and you could order steak. I mean that sounded good. That's why I was going to be… One of my undergraduate professors, István Palócz – still alive at 95 and a very nice man, came over in '56 from Hungary – I remember talking with him in my senior year at NYU and I told him what I wanted to do. He said, "Oh, so you want to be a captain of industry?" [laughs]

That was my plan, but I also wasn't going to get married till I was 35. Here I was, it was in 1968, I was 22 years old finishing my PhD and I'd gotten married when I was 21, and we weren't going to have kids for five years, but that changed. We had our first child two years into the marriage, planned. All of a sudden I thought it through and I thought, "Wait a minute, I wanted to travel the world when I was going to be single. Do I really want to be travelling the world when I have a family?" So I reconsidered the whole teaching thing and I ended up being a teacher.

But coming back to my brothers, as I said, Howie let me tag along. We also, the three of us – the more Howie and I initially and then Steve and I later as Howie got interested in stupid things like girls, you know? [laughs] – we would take hikes, like three miles from our house in the Bronx up to Van Cortlandt Park. Early in the morning, we'd pack eggs, we'd pack them in paper towel and aluminum foil so they wouldn't break, and we would cook them over a fire.

And Steve, well, he majored in nuclear engineering, worked at the patent office for a while. This was during Vietnam and draft deferments were a big issue. He eventually ended up… Chemistry was always his big thing and he ended up working largely in pharmaceuticals, between research and the business side of the company, translating what the researchers were doing into language that the businesspeople could understand. Like at one company – he worked at Clairol for a while – he saw that they were spending something like two-thirds of their R&D budget on non-hair products and, I don't know, maybe 90% of their revenue came from hair products. He said, "If we want to get into new areas, that's fine. But has this actually been thought out?" and I don't think it had. He did good things like that. We're still very close, all three of us.

HW: Let's switch gears a bit. What was your favorite subject in school? And least favorite?

MH: Oh. My favorite subject in school was science early on and then physics by the time I got to high school, which is why my uncle was my high school physics teacher. Most students in those days, and I think now, take physics in their senior year and more chemistry in their junior year. But since I was interested in physics, I took it in my junior year so I could take a physics elective in my senior year. This was at the Bronx High School of Science. My uncle was the only one who taught the physics course that the juniors took, so that's how I ended up taking it from him. He died just, by the way, a few months ago at 106. He had I think two Nobel Laureates in his physics classes. But I was always pleased when he said… he

always called me his best physics student. I'm sure there's a certain amount of nepotism in that, but…

HW: [laughs]

MH: What was the question again?

HW: Oh. [laughs] I just wondered what your…

MH: What was my favorite subject?

HW: …favorite subject… Well, we've got physics.

MH: Physics, yeah.

HW: What was your least favorite?

MH: Well, but then I didn't know anything about electrical engineering in high school. It's only when I got to college, and I had been a ham radio operator in my senior year, that I thought of electrical engineering. And computer science and electrical engineering are often the same subject.

My least favorite subject? Probably music. But that was because when I was seven… I'm probably second grade, so seven years old, I must have sung a song for the class. You know, the teacher will say, "What do you want to do?" and she'll go through, and it was usually a woman, always a woman in those days. I must have sung a song and someone made fun of me, so I made up the thought that I was tone-deaf, I had no musical ability. And I was quite surprised later in life when my daughters, born in 1969 and '71, when they were small, Dorothie, my wife, got them recorders and a little book to teach them how to play recorder, and I picked it up and I was able to make music. I wasn't anywhere near as bad as I thought. But probably that was my least favorite subject because I had embarrassed myself so badly.

HW: [chuckles] Who were the teachers you liked the most?

MH: My fourth and fifth grade teacher, I had her for both, Mrs. Donovan. I really liked her and she I think took an interest in me and encouraged me. Then in junior high, Miss Blake, my math teacher and homeroom teacher. I really liked her. Oh, Miss Martin , later Mrs. Loranger, my seventh grade homeroom teacher and English teacher. She was this beautiful young woman and here we are, 12 years old and all the boys were madly in love with Miss Martin. But she was also a really sweet woman. And my uncle, Charles Hellman. Oh, and István Palócz, my E&M] professor in my senior year at NYU. My first technical paper was written with him, which was really a gift from him. I did some programming, but he had really done

all the theory and he included me on the paper. And of course my PhD advisor Tom Cover. Oh, so many, too many to name, but I think that gives an idea.

HW: Was there a moment when you thought electrical engineering is interesting and is something that you might want to learn more about?

MH: Yeah. It was when I became a ham radio operator. My father by the way and my uncle, my physics teacher uncle, had both been ham radio operators. Actually their younger brother, who became a police inspector in New York, working his way up from a beat cop, also was a ham radio operator. That's what got me interested in electrical engineering. But I remember thinking in my undergraduate years, even in my senior year, all I could think of electrical engineers doing was designing transmitters and receivers, with tubes in those days. How many transmitters and receivers did they need? I mean I couldn't think of things like public-key cryptography, the Internet, computers. All that was beyond my understanding.

HW: Do you recall any textbooks that might have been important to you when you were in university?

MH: [laughs] I'm laughing because the first book that comes to mind is one that I read as a junior high in high school student. It was *Ganot's Physics*, published in 1898. It was in the 1890s. I forget the exact year. My father had it on his bookshelf. I don't know, he must have bought it in some used bookshop. It had a number of experiments you can do. I think, yeah, one of my science fair experiments came out of there. It was a perpetual motion machine, which of course… I mean it was powered by the sun, so it's semi-perpetual motion. But it used ether and it had a tube and bulbs at either end, and the ether would evaporate and go to this bulb. But then there was muslin cloth over it, moist cloth, so it would condense, and it would go like this and it would go back and forth. *Ganot's Physics*.

Other texts? Let me think. Niven, number theory. And it wasn't in school. This was when I got interested in cryptography. I learned a little bit of number theory in my graduate work, but not enough to do what I needed to do, so I got Niven's text – I'm pretty sure that was the author – his standard graduate text on number theory.

Oh, Knuth. I mean again, this isn't when I was a student, but later Knuth's volumes, his series on *The Art of Computer Programming* was just unbelievably helpful. One of my students, Justin Reyneri, was working on a problem that involved random graphs. I'm pretty sure it was Justin's thesis. I called Don Knuth up – this was phone era – and I described the problem to him and I said, "Do you have any thoughts on how we might tackle it?" He says, "Oh yeah. Get volume 2 or 3" – I forget which it is. He pulled it off the shelf in his office on campus and I half a mile away pull it off mine, and he goes and he says, "Oh, turn to page so-and-so, problem number so-and-so." There was a problem there that only he would have recognized that it could be massaged into the problem I was working on. So Knuth's series was very helpful, very important.

Those are the ones that stand out.

HW: Tell me about your current family – your children, your spouse, how you met.

MH: My spouse. I'm going to get teary-eyed if I really think about her. Her name is Dorothie, which means "gift of God." Forty years ago I would have disputed that. We were headed for divorce at that point in time, although I didn't know it, I was too busy. But over the last 37 years, we've really worked on our relationship and I really see her as a gift, a gift of God. She saved my life. I'd be Mr. Spock if it weren't for her. And there's so much to the human side of life that we need.

In fact, in my Turing Lecture, which will be online, and in the book she and I wrote, I go back to something I learned in my second year of graduate work. I was taking a course, an advanced math course, and in the book I just talk about it as Gödel's incompleteness theorem, which proves that logic is incomplete. What I say there is what I should have done… at the time when I learned this, I came home to Dorothie – we were newly married I think just maybe a year – and I told her I felt like I was having a mental breakdown because I'd based my whole life on logic, and here logic was telling me very logically that logic was incomplete. What I wrote in the book and repeated in the paper is what I should have done is what I did maybe 20 years later, which is to stop basing my life on logic. I mean it's just one piece of life, one piece of our intelligence. But I mistakenly kept… illogically I kept applying logic everywhere, even though it wasn't working very well.

Let's see what else about Dorothie. She's amazingly intuitive. She's very sensitive. In our book, I describe her as "the Princess and the Pea of relationship conflict," and how it drove me crazy early on because she would pick up on conflicts within me that I wasn't even aware were there. But now I treasure her sensitivity and I describe it as being analogous to a scientist who will spend countless hours keeping a sensitive instrument working so he can delve into the secrets of the universe more deeply than anyone else. And Dorothie helps me delve into the secrets of the universe, particularly this universe, learning about myself and where I need to improve. She's unbelievably valuable to me and worth all that fine-tuning and care that one needs to put into a fine instrument.

HW: How did you meet her?

MH: Well, we have two different stories, and they're both true. She would say we met on Catalina Island, which is true. I would say we met on a Girl Scout campout, which is also true. Because people picture me climbing over a fence. Dorothie had been in the Girl Scouts all through high school, and the seniors, the girls who had just graduated from high school in 1966 had gone with their skipper, their troop leader to Catalina and rented a house. So it wasn't like I had to climb over fences. They were on the beach and they weren't wearing Girl Scout bathing suits and they were kind of cute. So that's how we met. I had just come to California to work for

the summer before… to L.A. I was working for Aerospace Corporation in their solid state research lab before coming up to Stanford to do my graduate work.

So other family. We have two daughters, Sonja and Gretchen, two years apart. Sonja is a therapist, a psychologist in Boulder, Colorado, and does wonderful work using something called Rapid Resolution Therapy. It's very fast interventions. The only trouble is it's not a very good business model. [laughs] But she loves doing it and she's really been very helpful with some very difficult cases.

And Gretchen, her younger sister, went into the family business after a while. She was in information security for about 20 years, but is now reinventing herself as a career coach, because she needed to change her own career. She'd had enough of high tech. She'd done very well in it, but she wanted to really work with people. In fact, they've pointed out, it's funny that all four of us work on helping improve the human condition.

We have three grandchildren. Each of the daughters has a daughter 22 years old. Zoe, Sonja's daughter, has just finished her nursing program at University of San Francisco and is in the process of getting licensed. And Gretchen's daughter Celeste has just finished her first year at USC film school, although it's really her junior year because she transferred in from a junior college, and is just loving working in film and it's a fantastic place for her to be.

Then Max, our just recently turned 17-year-old grandson, is figuring out life. He needs to talk to Gretchen about the career coach. But when you're 17, that's okay. He's brilliant mathematically. I mean when I used to drive him to camp and places like that – because he went to camp locally, he'd fly in from Colorado – we'd talk in the car about all kinds of things, why diesel engines were more efficient than gasoline engines, and I would do math with him that was years ahead of his ability. But he and school just don't get along very well. But Gretchen and school didn't get along very well, and her life worked out well. So we'll see what happens.

HW: Did you ever change careers?

MH: Oh, I've changed careers several times. First of all, I wasn't going to be a teacher, remember, and here I am, I taught at MIT and then Stanford. But that was a change in plans. But early on, I was an information theorist, so my early work is in more traditional information theory. Then I worked in cryptography, which might look like a career change, except what I realized is that information… I'm sorry, cryptography is a branch of information theory. Information theory is concerned with coding information for error correction – like on DVDs, there has to be error correction because not all of those billions upon billions of bits can be stamped out correctly – or for data compression like JPEG. Most information theorists just knew those two, but it turns out coding for privacy and authentication, which is cryptography, is an integral part of information theory. In fact, Claude Shannon's

development of information theory owes a large debt to his work during the war, during World War II on cryptography. So that was a career change in a way.

Then in 1980 when I finally woke up and realized that I can't base my whole life on logic, that it wasn't… Well, I can, but it was going to ruin my life. I tried to base the family on logic. And especially with me being the only male in the family, that was not a smart thing to do. Very illogical. So in 1980 with some help from Dorothie, [laughs] I eventually realized I needed to change, so I started opening up to seemingly crazy ideas, some of which actually were crazy but many of which just had seemed crazy to me. The most important ones for me to open up to were Dorothie's seemingly crazy ideas, many of which were brilliant but just seemed crazy because I had my blinders on, my limited view.

Then I changed careers. I continued to do a little work on information security, but I really started working on international security. Because we came to see that the same problems that had nearly caused nuclear war so to speak in our marriage, which is called "divorce," those same mistakes were being made at the international level and were likely to cause a real nuclear war. So I started working on those issues and have continued to work on them, but see them as totally interconnected to the interpersonal. That is, the best thing that someone can do to reduce the nuclear threat I'm convinced is to bring peace to his or her own personal relations, because you will get a benefit from that. You will be motivated to continue to persevere and you will be able to… when people say, "Well, how do you know you're making a difference? Because how many nuclear weapons did you get rid of today?" "Well, I can't say I got rid of any. But if I resolved a conflict that would have been a huge fight years ago and instead we resolved in a way we were both happy with the solution, that is really something to be proud of and something that allows me to be a more convincing advocate for peace at the international level." So that was a change of career.

HW: Do you have any hobbies or other activities that you enjoy?

MH: Well, I'm 71 now. I still go bike riding for exercise and love it. I mean I should do pushups and other calisthenics, and I occasionally do them, but I have to really force myself. Whereas getting out on the bike, I just love it. I've always loved bike riding. My two brothers and I were into bike riding in the '50s and '60s when people thought we were crazy. We had 10-speed bikes in the very early days, and then I had a 15-speed bike, which actually is not that unusual today. So I love bike riding.

I haven't gone speed skating in several years, but I did love… I need to get out there again. I did it as a kid, I mean as an adolescent. Then when my granddaughters, now 22, took up ice skating, I was taking them and I got a new pair of speed skates and got out there and was loving that.

And sailing. I did a lot of sailing. I haven't done it in years, but I loved sailing.

Then maybe the most unusual was soaring. Sailing in the sky. Sailplanes. I have about 2,700 hours in gliders. But I only fly about once a year now, I mean very infrequently, and always with an instructor. I don't go up by myself. But I was really flying intensively from '94 to whenever it was, about 2010.

HW: What was your first job?

MH: Oh goodness, I had many jobs, first jobs. I mean, do you count delivering groceries?

HW: No.

MH: No. I mean I'd go down to get my groceries. I grew up in the Bronx and I'd go down to buy groceries for my mother, you know, get a quart of milk, and the owner of the grocery store would say, do I have time to deliver a box of groceries to someone? It meant sometimes climbing five flights of stairs carrying this heavy box of groceries for a 10-cent tip, if I was lucky 25 cents. But that doesn't count.

I had a job in a dry-cleaning store doing deliveries when I was in high school.

My first legal job was shelving books in the library for probably 90 cents an hour in it must have been 1961 or something like that.

First technical job was the summer of 1965, so after my junior year at NYU. I got a job at a microwave plumbing house. They were a house that designed waveguides and switches for radars and things like that. These were all pipes and we had a machine shop there. I would do mechanical drawings and I would specify, "I want this to be 1.5 inches plus or minus a thousandth," and the machine shop would make it. That was my first technical job.

HW: Can you describe what the computing world was like when you first entered it?

MH: Oh yeah, that's fun. First of all, it's even more fun to describe the computing world when I was resistant to entering it. I mentioned that I went to Bronx High School of Science. That was 1959 to '62 that I was there. In those days, ninth grade was still junior high school, so it was only tenth, eleventh, twelfth that I did there. Bronx Science had a 1620, an IBM 1620 computer when most colleges did not. But it seemed to me you had to be some kind of weird math genius, which I did not think of myself as being interestingly, to be able to program these things. I mean I hadn't actually looked into it. So I didn't have anything to do with the computer at Bronx Science.

It was my sophomore year, so probably 1963 or '64, at NYU, I was forced to take a two-unit FORTRAN programming course. Working in a high-level language like that was so easy. I mean the fact that if you have an 8% tax, "tax equal 0.08 times

price," I mean how much simpler could you get? I was blown away by how easy it was. Of course we had 24-hour turnaround time. I'd put the punch cards in and have to wait 24 hours to get back that I'd left off a parenthesis or an END statement.

And interesting thing. I learned that computing was actually easy. When I had that job at Aerospace Corporation when I met Dorothie, the summer of 1966 between finishing my bachelor's degree in June '66 and starting my graduate work at Stanford in September 1966, as I mentioned I was working in the solid state research lab. I was making Schottky barrier gallium arsenide diodes, and I would lap the wafers and then we'd sputter them and do all this stuff. I remember hearing the two guys I was working for, two PhD physicists, solid-state physicists, saying, "I wish we knew the" – oh goodness – "the Fermi, I wish we knew the Fermi level of gallium arsenide as a function of temperature." I knew enough about how to calculate it. I went to them, I said, "Oh. Do you need just a graph or do you actually need a closed-form equation?"

Because closed-form equation I couldn't do, but with a computer, you could do the graph. Because there's a formula for the number of energy levels versus energy, and then at a certain temperature you have a certain number of free electrons. The higher the temperature, the more electrons boil off so to speak. Then you fill that up. We know this equation. You just fill it up until you have that number of electrons and that's the Fermi level, at least if I remember it right. And you could do that on a computer. It took thousands upon thousands of calculations, but even in 1966, you could do that on a mainframe very quickly.

And they said, "Oh, all we need is the graph." So I said, "I can have that for you tomorrow." So I programmed the thing up, and they were so amazed that one of the guys, a PhD physicist, went and took a course that Aerospace offered on programming, because he just saw how this opened up possibilities.

HW: What was the first computer you actually worked on?

MH: [laughs] The first computer I worked on, I was probably eight or nine years old. So it's 1953 or 1954. My father – remember, a physics teacher – brings home a box called a GENIAC. It was a computer in a box. I was old enough to be skeptical, like "Could this really be a real computer?" which of course it wasn't. But I was young enough to be naïve enough to hope it really was a computer. It wasn't a stored program computer. It was just switches that you could wire up in series or in parallel to do simple Boolean logic. But the amazing thing is now of course you can bring home a computer in a box and it is a real computer. So that was the first "computer" I worked on, but it wasn't really a computer.

The first computer I owned – let me answer that one – was an HP-45 pocket calculator. I left MIT and came to Stanford in 1971. I joined the faculty. It was right around then that HP came out with the HP-35 scientific pocket calculator. $400. Today, that's like $4,000 I would imagine. But it was amazing. I really

lusted after one, but I didn't have the money for it. About a year later after spending a night doing a lot of calculations by hand – I needed four decimal places of accuracy and you couldn't get that on a slide rule, which is what I had, so I was actually doing multiplications by hand – I said, "I'm going to buy one of those things." Fortunately the HP-45 had come out. The 45 was $400 and they dropped the price of the 35, but I think there were three memories in the 45, whereas the 35, it had one. There were a few other minor differences. That was my first computer.

HW: What projects did you work on in the early part of your career prior to your interest in cryptography?

MH: What projects did I work on in my career?

HW: What projects, yes.

MH: Well, in my senior year at NYU, I did a paper for the IEEE student paper contest on car driver systems. It actually won first prize in the New York area and I think second prize in the Northeastern region. The idea was that if you think of a feedback system, the driver is watching where he is on the road. If he's to the right of the line, he turns the wheel to the left; if he's to the left of the line, he turns the wheel to the right. But if you're drunk or a new driver, it can go into oscillations and why that happens. I realized it had to do with delay. If you're drinking, your delays go up. So I actually analyzed that using… I think I should have used Nyquist criteria but I used root locus approach instead. That was maybe my first project.

Oh, and then in my senior year, one of the professors, Codalessa, at NYU in the solid state area, some company had donated an infrared laser, solid-state laser. Remember, lasers at that point tended to be these big devices and here you had this little solid-state laser. It needed liquid nitrogen. I mean today you have things like that in your DVD player. And he said, did I want to try to get it working? So I wired it up and using I think a diffraction grating to tell when I was getting interference, I could tell whether the light coming out was coherent or not. So that was a project that I did.

Then my thesis, my PhD thesis was *Learning with Finite Memory*, which was really more statistics than it was information theory, although the two are very related. But it relates to computation. If you have… Well, I'll describe it this way. I'm going to make a trick coin so that we can bet. I'll bet on tosses of the coin. You don't know that I've made a trick coin – you're very naïve in this model – and so you're willing to give me even odds as I flip the coin that I've provided. I've designed it very carefully so it shows heads three-quarters of the time, and I'm of course going to bet on heads and make money like a bandit.

The trouble is before I stamp heads and tails on it, I drop the coin on the floor. I pick it up and I don't know which side it's weighted towards, then I stamp heads and tails kind of arbitrarily. Now I have two simple hypotheses – either the coin

will show heads three-quarters of the time or one-quarter of the time. I want to learn which it is so that before we start betting, I know which way to bet.

Now if you have unlimited memory, you can toss the coin a thousand times and have a very small probability that you'll be betting on the wrong side. If it shows 740 heads and 260 tails, you bet on heads, and vice versa. But what if you have a finite memory? What if you have just two bits of memory, a finite-state machine with four states? What can you do there? And what do you do when you have two arbitrary probability distributions, not just coin tosses?

I was able to solve that problem. I was able to show that there was a lower bound on performance and I was able to achieve the lower bound, so I knew that this was the optimal machine. That created quite a stir, because there are very few results like that where we actually know the best you can do and then you can do it.

That was my project. There were lots of projects, but does that give an idea prior to cryptography?

HW: Now let's switch to your interest in cryptography. Or cryptology, because I think you're also interested in cryptanalysis.

MH: Yeah. I use the two interchangeably. David Kahn would tell me I'm wrong, and he's probably right, but "cryptography" has a nicer ring to it than "cryptology."

HW: As an academic, you're very much a pioneer in studying it. At the time, it was a taboo subject.

MH: Yes.

HW: Indeed, it's no exaggeration to call you "the father of academic cryptography." Can you tell us how you began in this field and what inspired you to work on it?

MH: Yeah. I would say I was one of the fathers of academic cryptography. Whit Diffie certainly deserves equal credit, Ralph Merkle, and Horst Feistel before us.

I don't know if I've already mentioned, when I finished my PhD rather suddenly in 1968 – and actually I technically had not finished it because I hadn't paid enough money, but I'd finished the work – I went to work at IBM Research in Yorktown Heights for a year, '68 to '69, before joining MIT's faculty in 1969. I was in the Pattern Recognition Methodology Department if I remember the name. A really nice man, Joe Raviv was the head of the department. They had just hired Horst Feistel from MITRE Corporation to start IBM's research effort in cryptography, and they put him in this same department. They didn't have any better place to put him. Later he was in the math department.

So Horst and I were on the same general area. While I did not work in cryptography, I would have lunch with him, and he described to me some of the classical systems. I mean simple substitution cipher is easy to break. I already knew how to do that. But he described for example the coherent running key cipher. That's where you write your message out, for us in English, and then the key is the text of a book. Like it might be the Bible – "In the beginning God created the heavens and the earth." You then add the two, the text and the key mod 26, to produce the ciphertext. It seems impossible to break a system like that, but it is in fact quite possible to break a system like that.

Horst described to me what you do is you use a probable phrase or probable word attack. Like you assume that "T-H-E" appears somewhere in one of the messages, either the plaintext or the key. In this case, "In the beginning…" it's right there – "In *the* beginning…" Second word. So you subtract "T-H-E" mod 26 from the ciphertext. When you subtract it in the right place, you get meaningful-looking text coming out. When you subtract it in the wrong place, you get gibberish. So you're able to start filling things in. This just blew my mind. It also told me that IBM was spending good money developing cryptography, so there was probably… it reinforced my belief or created the belief that there was a commercial market for cryptography.

What was the question? I was trying to say why Horst Feistel deserves a lot of credit as an academic father of cryptography.

HW: But he wasn't an academic.

MH: No, he was… Well, okay. What do you want to call it? Unclassified research, although he'd started in the classified domain.

HW: Well, you've mentioned Horst Feistel, so this brings me to the question of what is the Data Encryption Standard, DES?

MH: DES.

HW: And why was it so important in the '70s and later?

MH: Okay. Whit and I connected in the fall of 1974. We were working and we knew that… We were working on cryptography. It helps to make explicit, almost all my colleagues, I think maybe all my colleagues other than Whit thought I was crazy to work in cryptography. You called it a taboo subject. Jim Omura for example, who is a professor at UCLA, another information theorist, has said I can quote him on this, and I have. He thought I was crazy to work in cryptography. The really ironic thing is Jim when he left UCLA started a Silicon Valley company that got sold for I think $35 million that was based on public-key cryptography.

But I missed things too, I mean just to show it's not just my colleagues. When Google was first formed… Actually it hadn't even been formed as a company maybe. It was this great search engine. Being at Stanford where it came out, I was using Google as a search engine before almost anybody else except my colleagues. I was talking with Dan Boneh, a brilliant cryptographer here at Stanford, and he said I can quote him on this too. We're both using this great search engine, but we turn to one another and say, "But how in the hell are they ever going to make money from free search?" Well, we should have asked that question more deeply, because they made a fortune from free search, and we could have made a fortune if we'd invested in the company. We probably could have while it was private because of our Stanford connections. So we missed it too.

But coming back to DES, Whit and I knew that the National Bureau of Standards as it was then called, now NIST, the National Institute of Standards and Technology, had issued a request for proposals for a national data encryption standard, because they saw that there was a growing commercial need for protecting unclassified but sensitive data – oil companies' drilling data, banking records, medical records. We were wondering what they were going to come up with. What they came up with is what is now called DES or the Data Encryption Standard.

It was proposed in March 1975 in the *Federal Register* as a proposed standard. We were naïve enough to think it actually was a proposed standard at that point. What we didn't understand is by the time it's published as a proposed standard in the *Federal Register*, it's in concrete, it's not going to change. It came out of IBM. So in fact the group that Feistel, Horst Feistel at IBM pulled together developed different systems, but the ultimate one was the Data Encryption Standard. This is what NBS proposed and IBM gave a royalty-free license to use in connection with implementing this standard.

But Whit and I looked at it and quickly realized – and actually Whit was the first one to realize this – that the 56-bit key was at best marginal. Now with a 56-bit key, you have 2^{56} possible keys. To an order of magnitude, that's a hundred thousand million million keys. That seems impossible to search unless you're a computer scientist and unless you're actually a very forward-thinking, in 1975 at least, computer scientist.

What we realized is you could probably build… since DES could be implemented on a single chip with 1975 technology – that was one of the requirements – you could also implement a search engine, a cryptanalytic search engine on a single chip searching keys. We estimated that that chip could search a million keys per second in 1975. You would then buy a million of these chips, and you're searching a million million keys per second. So how long does it take to search a hundred thousand million million keys? A hundred thousand seconds, which is about a day. A day is closer to 80,000, but order of magnitude, it's a day.

We then estimated that these chips would cost $10 each. That's $10 million for the chips. We very cavalierly assumed another $10 million for the printed circuit boards and power supplies and so on. We then depreciated the machine I think over five years and ended up with $10,000 per solution, which seemed marginal to us, especially with the cost of computation dropping very rapidly.

That was DES. Do you want me to go into the controversy?

HW: If you want.

MH: Yeah. Naïvely, Whit and I sent off an analysis to NBS saying, "Hey, by the way, you want to increase the key size." [laughs] They wrote back after a couple of months saying, "Thank you very much, but this is fine." That got me – and this was more me than Whit – to talk to people at an integrated circuit labs and to refine our estimate. That estimate I gave you before of $10,000 is the refined estimate. The initial one was back-of-the-envelope calculation. It became clear that this really was a dangerously insecure standard, especially 5 or 10 years in the future when the cost of computing would fall by a factor of 10 to 100, a factor of 10 every five years. Even if we were off by a factor of 10 in our estimate in 1975, that error would be erased in five years when the standard was in widespread use.

After about six months of writing letters to NBS and their writing back garbage in my opinion, it was someone, it was the IEEE Computer Society Standards Committee, the guy who was chairman of it, I thought, "He can do something. I'm just a professor, but he's in charge of this important committee." And he said, "No, I'm not going to have any more success than you. You have a political problem on your hands, not a technical one. If you want to get in a better standard…" That was important by the way, because if your medical records are protected with an insecure standard, that's a real problem.

Actually Admiral Inman, who was Director of NSA around this time, who was initially fighting us on this, two years ago in an interview, he was asked, with what he now knows, would he still try to suppress our work? He said quite the opposite. Given how the Chinese have stolen defense secrets from contractors because of inadequate encryption, he would try to get our work out as quickly as possible. But we had a huge fight with NSA over this and we lost. The standard stayed at 56 bits.

But we won 20 years later roughly when they did the Advanced Encryption Standard, which is now being used. That has a minimum of 128-bit key size. Equally important, maybe more importantly, the selection process was very open and transparent. It was not… One of our other criticisms of DES is we had no idea what the other submissions were, what the design principles were behind DES, whether there could be trapdoors hidden in these large number tables, seemingly random number tables that went with the standard. But the Advanced Encryption Standard was done very publically and with public comment. It was really done the right way.

HW: Now you've mentioned the NSA. We're probably going to talk a bit more about the NSA. Did they get upset with you in your attempts to sort of show they might have had something to do with the key size?

MH: Oh. I think it's fair to say there was apoplexy within NSA over two things – over our criticism of the Data Encryption Standard and our publishing our papers on cryptography, publishing good work in cryptography that NSA viewed it had control over, that this was born classified. But as Admiral Inman's statement of two years ago indicates, it was a shortsighted view, but it's an understandable one. I mean they'd been used to having a monopoly.

Now why do I say… I have to assume there was apoplexy there. There's a joke that NSA stands for "Never Say Anything" and "No Such Agency." So we didn't know a lot of what was going on. But enough leaked out that we knew that they were unhappy with us and there were some threats that we could be thrown in jail for publishing our papers. Do you want to hear about that?

In the summer of 1977, July I believe it was, the IEEE, Institute of Electrical and Electronics Engineers, where we were publishing most of our papers, gets a letter from a member from his home address in Maryland saying, "As an IEEE member, I am deeply concerned that the organization appears to be breaking the law by publishing papers in certain areas that are covered by the International Traffic in Arms Regulations, or ITAR." He then cited I think six or seven IEEE journals that he felt had papers. He never said what the papers were. Whit and I had papers in five out of the six or something like that. He was basically saying, "Quit publishing Hellman's papers." Whit was able to determine through his spy network, which is very good, that this man worked at NSA. There was kind of a hint of that with the Maryland address. So we didn't know, but it seemed like this might be NSA's way of putting us on notice. It later turned out that this guy was probably a loose cannon, but he did represent an attitude and a concern that was prevalent within the agency.

So the IEEE writes back to Meyer was his name, J.A. Meyer I think, saying, "Thank you very much. We are well aware of the ITAR, but it's always been our position that we, the IEEE, cannot act as the gatekeeper. It's up to the authors and their institutions to make sure that they're not in violation of the law." And it's interesting. Whenever people start talking about cryptography, they talk in code. Meyer did not say, "Hellman's publishing papers he shouldn't," but he cited these six journal issues roughly and I was in all but one. IEEE sends me a copy of this, but they don't copy it "Martin Hellman, troublemaker." It's "Martin Hellman, Board of…" – I was on the board of governors of one of the groups, IEEE groups that was publishing these paper – but they didn't send it to all the governors. Again, it's code – "Hellman, pay attention to this."

I take the letter to Stanford's general counsel, John Schwartz at the time, and he reviews it. I come back a few days later after he's had a chance to review it and he says, "It's my legal opinion that if the ITAR are construed broadly enough to cover your work, then it's unconstitutional, because it's abridging your freedom of speech, freedom of the press. But," he said, "I've got to warn you, that's only my legal opinion. The only way we can really settle this is in a court of law." Actually I have a copy of his memo. He says, "There's at least one contrary legal opinion, that of Mr. Meyer, that we are breaking the law." So he said, "If you are prosecuted, Stanford will defend you. If you're convicted, we will appeal. But I have to warn you, if all appeals are exhausted, we cannot go to jail for you." I think it was 5 or 10 years in jail was part of the potential punishment.

But with Stanford's backing, I felt comfortable going ahead. In fact nothing did happen, although later Phil Zimmermann of PGP did have to get legal representation. He was not indicted though, fortunately.

HW: Did NSA make any attempt to get you behind the fence?

MH: Hmm?

HW: Did NSA make any attempt to get you behind the fence?

MH: Oh. Sure. Early on, even before we had good results, when I was going to conferences and giving talks on much more mundane things, much less important results, there would always be people at the conference, the nametags were always… "Department of Defense" was NSA and "US Government" was CIA. It was a very simple substitution cipher, more of this silly cryptography. Now they're more open about it and they often will say "NSA."

But several people from NSA approached me before all this was a conflict and said, "We'd love to hire you as a consultant." They were always needing new blood, new ideas. I said, "Oh, I'd love to know what you know, but I'm not willing to then limit myself in what I can publish if I come up with things independently," which I knew I couldn't do, and they always then said, "No, then you can't." Those were the only attempts, and they were not nefarious. They were just very open.

HW: The citation for your Turing Award is "For inventing and promulgating both asymmetric public-key cryptography, including its application to digital signatures, and a practical cryptographic key-exchange method." In fact this investigation led, among other things, to the eventual establishment of the Diffie–Hellman key exchange protocol, which is one of the most widely used encryption techniques, with applications throughout the Internet to secure online transactions. What is public-key cryptography and why is it so important?

MH: Public-key cryptography does two things. It gets rid of the key distribution problem for privacy. In the old days before public-key cryptography, if the cameraman and I

wanted to exchange a message but didn't want you to know what we're saying, we had a problem. We had to have agreed on a key ahead of time. Then I could encrypt a message and I could call it out to him across this room, you could hear the encrypted message, and he could decrypt it knowing the key. But if we had not prearranged a key, as in fact is the case, we couldn't do it.

What public-key cryptography allows us to do is I tell him the protocol. You hear it too. We then do some calculations and create some random numbers each of us, and at the end, he and I have exchanged information that you cannot understand. Which sounds impossible, and from one point of view it is. If you have unlimited computing power, you can learn anything that we've said. But of course you don't have unlimited computing power, nor do we. The real question is, can we come up with something that will just take a few seconds or a fraction of a second of CPU time for the two legitimate parties that would take you billions of years?

That's what we were able to come up with in this algorithm that you mentioned, Diffie–Hellman key exchange, which I have always tried to call "Diffie–Hellman–Merkle key exchange." When Whit and I published the paper with that in it, we were very careful… we never called it "Diffie–Hellman." We called it "alpha to the X1 X2". It's an algorithm that I came up with in the study right over there late one night. We'd been trying to find an implementation of the idea that Whit had actually come up with initially. By that time, Ralph, who had had some similar ideas, Ralph Merkle, was involved. We were all working and I was very fortunate to come up with the first such algorithm.

But the interesting thing is Ralph came up with a slightly different formulation from Whit and me. His is called public-key distribution, whereas Whit and mine is public-key cryptosystem. The system I actually came up that night in May of 1976 was one of Ralph's systems, not one of ours. So it's kind of a losing battle to get it to be called "Diffie–Hellman–Merkle key exchange," but Ralph really deserves equal credit. And he is listed as an inventor on that patent for that reason.

That's the first thing that it does, is it gets past the… And I can give you a quick idea of how one can do the seemingly impossible. Let's think in terms of strongboxes. Instead of calling the message out across the room, I want to put a message in a strongbox and send it to the cameraman, but I have to pass it through you and I don't want you to be able to open it. What I do is I put a combination lock on the strongbox that only I know the combination to. When I pass it to you, you cannot open it. Of course the cameraman can't open it either.

But I've made the hasp on the lock big enough for him to put a second combination lock on that only he knows the combination to. So now it's doubly locked. He passes the doubly locked box to you. You still cannot open it. I can take off my lock but not his. But now it's only his lock that's on it. I pass it back to you. You still cannot open it. When he gets it, he can open it and read the message that I put there.

That's roughly how it works. In fact, this Diffie–Hellman–Merkle key exchange algorithm, a key thing is that it uses a commutative one-way function. What's commutative about the strongbox, imagine that I had not made the hasp big enough to put two locks on. You can only put a single lock on. Well, then when the cameraman got it, he could put my strongbox in a bigger strongbox and lock that, but now it's no longer commutative. You cannot take the locks off in any order. You have to take the outer lock off first and the inner lock off second. When I get the doubly locked strongbox, I cannot get inside to take my lock off. That's roughly a plausibility argument for how Diffie–Hellman–Merkle key exchange works.

The second thing that public-key cryptography does – and again Whit was the first one to formulate this – is digital signatures. We realized that you needed a digital equivalent of a written signature. It had to be easy for the signer to reduce, it had to be easy for the authenticator, the recipient to authenticate it, but it had to be hard for anyone including the recipient to change the contents of the message or to forge a new signature. Written signatures are inadequate here because my written signature looks the same on a $10 check or a million-dollar check. If you get my written signature, you can copy it onto the million-dollar check. The digital signature is message-dependent. That's really important. The signature, it depends both on your identity and the contents of the message, and changing even one bit of the message, in particular changing from $10 to a million dollars, which is more than one bit, would totally invalidate the signature.

The way public-key cryptography works is to have two keys. One key is public and one key is secret. Normally in cryptography, the same secret key is used to encrypt and decrypt. But by breaking it this way, you're able to do these two things.

At first, it flew in the fact of conventional wisdom in cryptography. In fact, when I tried describing it to Horst Feistel before we had a workable system – we only had 10 minutes, he was leaving for a doctor's appointment – he said, "You can't do that." It's understandable. It's a little bit… There's an analogy to Einstein's winning the Nobel Prize in Physics for explaining the photoelectric effect. Max Planck, who was 10 or 20 years Einstein's senior, had actually come up with the quantum theory of light around 1900 to explain black-body radiation.

But as you know, a couple of hundred years earlier there was this big debate in the physics community. Was light a particle or a wave? In I think the 1870s, James Clerk Maxwell came up with Maxwell's equations, which clearly showed that light behaves as a wave. So saying that light behaved as a particle – the quantum theory of light – seemed to be going back to the Dark Ages. So when Planck could only explain black-body radiation using what we now would call quantum theory, he wrote it off as a purely theoretical construct. Einstein, to explain the photoelectric effect, had to take it seriously and won the Nobel Prize in Physics for that.

In the same way, in the dark days, the dark past of cryptography, people would come up with ways to make really secure cryptographic systems if you could keep the system secret. But of course you never can do that if it's a standard like the data encryption standard is public, and even in the military, it can be captured by your adversary. So again in roughly the 1870s, Kerckhoffs, a famous cryptographer, came up with certain principles, one of which is "The general system must be thought of as public, even if you're trying to keep it secret, and all of the security must reside in the secrecy of the key." Now to talk about public-key cryptography sounded like we might be going back to the Dark Ages, but we weren't. There still is a secret key. There's just a public key and they're inverses to one another.

The way it works, if I want to send you a message privately, I look up your public key and I encrypt the message using your public key. Only you who know your secret key can decrypt it. If I want to sign a message, I act on it with my secret key that only I know. You can use my public key to verify it. That's public-key cryptography in a nutshell. Big nutshell probably.

HW: [chuckles] In your 1976 seminal paper co-authored by Whit, "New Directions in Cryptography," you established the subject of public-key cryptography. Could you tell us about this work, what inspired it, and what the individual contributions were?

MH: Sure. The Data Encryption Standard actually played a role here. As we started to think about how commercial encryption would work, the key distribution problem was horrendous. Because in the military you have a chain of command, so a private over here in one battalion does not talk directly to a private in this other battalion. He worked up through his sergeant, lieutenants, captains, etc., and then back down. That limits the number of connections. If you have *n* users, you don't have *n* squared over two possible connections. Whereas in commerce, any two people might want to talk to one another. So the key distribution problem was going to be horrendous. That gave rise to our thinking about ways to simplify key distribution, which ended up with public-key cryptography. Also, as we thought about ways, "How can you do digital commerce if you don't have signatures?" it led there.

Whit and I were working on these things. We didn't yet have an implementation, but we were working on these ideas. Even before public-key cryptography, we were working on cryptography. Jim Massey, now deceased, was the editor of the *Transactions on Information Theory*, where that paper appeared. Also obviously an information theorist. Jim had invited me to write a paper – so an invited paper, which is an honor – on cryptography for the *Transactions*. I asked him, I said, "I'm working with this guy named Diffie. I'd like to include him," and that was fine. So we were working on this paper that became "New Directions." When we had the idea of public-key cryptography, that was nice, but it wasn't going to be the groundbreaking paper that this was.

But then when we came up with the actual algorithm, Diffie–Hellman–Merkle key exchange… I'll never forget, I came up with that, as I said, in May 1976 and I had

a talk scheduled in Sweden at an international symposium on information theory on cryptography. I quickly included this result in it. Jim Massey, the editor, was at the conference of course and I remember him telling me, he said, "You get that result in the paper and I'll have it in the November issue of the *Transactions*." From June to November, five-month publica-… Unheard of. And we did and he did. Whit is fond of pointing out that the November *Transactions* came out in January of '77, two months late. They were always a little bit behind.

But one reason Ralph often gets overlooked is his paper did not appear until I think 1978. Here an editor at the ACM, at *CACM* owes him an apology, and a reviewer at the *CACM*. I detail this in my Turing Lecture. Ralph wrote up his work independently because he'd been working independently of us and he submitted it to the *CACM*. And it was rejected. The reviewer, who probably worked at NSA, said, "You can't do this," and the editor… And Ralph still has the letter. The editor – the first editor, not Ron Rivest, I'm careful of that because Ron is listed as one of the editors on the paper, but that came later – wrote to him saying, "It bothers me that you have no references." There were absolutely no references in Ralph's original draft. "Has no one ever thought of doing anything remotely resembling this before?" And the answer is no, they hadn't. But it was so unusual that she hadn't thought of that possibility.

Now in her defense, Ralph should have included references. I mean even when you have a totally new idea, there is something it's building on. But he was a master's student, and maybe even at that point still an undergraduate at Berkeley and had no idea how to write a technical paper.

Let's see. You were asking about "New Directions." Did I answer that?

HW: Pretty much. I guess the question that comes up is… You talked about what inspired it, you talked about the individual contributions. That was the question.

Now you must have run afoul of NSA during this work.

MH: Yes. There were two things going on simultaneously, the DES controversy and then development of public-key cryptography, both of which caused apoplexy within NSA. Pointing out that 56 bits is an inadequate key size really annoyed them, because up to that point, most of the commercial systems had 40-bit keys, and in fact they had something to do with that probably. 56 bits was a huge advance and a huge barrier to them compared to what they were dealing with, and most people did not encrypt messages at all. This was creating… Even $10,000 per solution is a huge barrier compared to nothing. But I believe they reasoned that key exchange was such a mess that people would use the same key for years, maybe forever, and so amortizing $10,000 over years of communications is okay.

But then we came up with public-key cryptography that allows you to change keys every day, every second even very cheaply, and that added to their concern. That's

when things like the Meyer letter came out. There was basically a war with NSA. I was not a peacemaker at the time, so when I felt they made war on me, I made war back on them, and I may have actually started it. I mean that's how wars start, each side thinking the other has started it.

The good news is fairly early on, in 1978, peace was declared between me and NSA. Not the whole community. I mean other people still saw them through negative eyes. I have to give the credit for that peace deal to Admiral Inman, the Director of NSA at the time. I got a call from his office in 1978 saying, "The Admiral is going" – or "the Director," whatever they called him – "is going to be in California and would like to meet with you if you're willing." We had been fighting it out in the press and never talking directly to one another. I jumped at the opportunity. He came to my office and he told me that he was meeting with me against the advice of all the other senior personnel at the agency. They must have been depicting me as the devil incarnate, because he looked over to me. He said two things. He said, "I don't see the harm in talking." The other thing he said, he looked over at me and said, "It's nice to see you don't have horns," because that's how I was being depicted.

Well, I had been seeing NSA not quite as the devil, but I had been seeing them as Darth Vader – remember, this was around the time the *Star Wars* movie had come out – and I was Luke Skywalker. I'm 71 now, but back then I was 30 years… Let's see. Yeah, 30. I was in my early thirties. I was the young hero. I had seen them as kind of a devil and I looked over at him and said, "Same here." Out of that grew an initially cautious relationship but that became a friendship. And he would agree. We're good friends now and have helped each other out in various ways. We try to understand each other's perspectives. We don't see everything eye-to-eye, but we respect one another, and that's a big difference.

HW: Did you patent any of these ideas?

MH: You bet. [laughs] Stanford had a very generous patent policy in those days. I don't know what it is now, but in those days, if you developed a patentable idea at Stanford, you owned it, unless it was done under government, a contract where the government would not allow you to own it. But in that case, the government allowed Stanford to own it. That was the case here – NSF, the National Science Foundation was supporting this research. So Stanford had to own the patents, but the inventors would get one-third of the royalties. If you think of three of us, Whit, Ralph, and myself, we'd each get about 10%. With that motivation, we in fact were very careful to patent things, though I didn't understand the patent system very well. The bottom line is even though we patented it and there was a big patent fight between Stanford's licensee and MIT's licensee, we ended up getting clobbered and we made no money, and RSA – Rivest, Shamir, Adleman, and Bidzos as the CEO – sold their company I think for $250 million. So yes, we patented, but it didn't do very much good.

HW: Sort of leads to my next question. These results are the cornerstone of Internet commerce. Did you gain anything from it beyond the gratification of your intellectual curiosity?

MH: Yes, I did. Although it's all a question of how you look at it. Early on – and as I was learning to be a peacemaker, before I'd really learned how to do it, and it really as I say started with the marriage but it carried over to the international, and it also carried over to cryptography, initially when I was still in war-making mode – I was really pissed with Jim Bidzos and Rivest, Shamir, and Adleman, because in their paper, RSA, I mean Bidzos wasn't on the paper, they credit Whit and me with inventing public-key cryptography. They didn't know about Ralph. When it came time to pay royalties, they said, "Your patents are invalid. Sue us." My perspective initially was "They're stealing money out of my pocket."

Well, there's a difference… But then I thought it through. Some years later I thought it through. I reframed it. Instead of RSA stealing money out of my pocket, they'd actually put money in my pocket. How did that work? RSA Data Security, the company that they formed and that Jim Bidzos really made into a success, established public-key cryptography and cryptography in general at a much earlier stage than I think it otherwise would have been. Jim's a great marketer. You could argue that we gained 5 to 10 years because of his marketing efforts with RSA. Now they made a lot of money out of it, but then I ended up making money out of the market that they created. Not off of our patents, but for example PayPal. I was on PayPal's technical advisory board, scientific advisory board before they were PayPal, when they had a whole different product. I made money from that. I've been involved with other companies. So I reframed it. Instead of being pissed at Jim Bidzos and RSA, I should thank them, and we're now good friends. And by the way, it's a lot better having friends than enemies.

HW: What was Hellman Associates?

MH: Oh, Hellman Associates.

HW: And what became of it?

MH: Most Stanford engineering professors have consulting practices. So I was doing consulting. I decided to try to build it into a company rather than just an individual consultant. Initially we designed a communication system for offshore drilling. They were moving from mechanical control to electronic control and they needed to make sure that when they pressed the button up here that said, "Open a valve," it didn't shear the drill pipe, which you might do if you have to get out of there in a hurry. So they needed very strong error-correcting and error-detecting codes, which I was able to design for them. We did that through… Actually that was an earlier incarnation, but basically Hellman Associates.

Then Harry Van Trees, who had been a professor at MIT and was then at CommSat, I think he was chief scientist at CommSat, when the work in cryptography was becoming a big thing, he asked me to come back and do a short course for top management at CommSat, which I did. And someone else asked me to do a course. I realized if there were two or three companies asking me to do this, there were probably a lot more people that wanted it. So I decided to offer a short course on cryptography and data security. I had no idea how to market it, but I figured I had such a reputation at that point, such a head start that even if I screwed it up, which I did, I could probably still make money and learn what I needed to learn.

It started out as a continuing education short course company and I got Gene Franklin, who was in many ways the father of digital control, to do a course on digital control with one of his students, former students. Ned Weldon from Hawaii asked me about "Hey, what about including one on error-correcting codes?" which he'd written… he was co-author of the most widely used text. So it became a short course company.

But we also then moved into product development and tried to get a non-exclusive license to RSA. [laughs] Remember that there are limitations when you do work under NSF or other government contract. Like I couldn't own the patents. Stanford had to own them. There's another requirement that, if possible, the university has to license non-exclusively rather than exclusively. So Stanford had been talking with MIT about pooling the patents and creating a patent pool, and MIT kept telling us it was much too early. Well, then Ron Rivest pays me a visit and he lets drop that he's formed a company, which became RSA, and they're about to get an exclusive license to MIT's patents. I was livid. I mean here MIT's been telling us this, and yet Ron was nice enough to tell me this.

So I got my vice president, a former student of mine, at Hellman Associates to write a letter to MIT's technology licensing saying, "We understand that they are interested in licensing and we would like to know the terms for a non-exclusive license," and I don't know if they ever got back to us. But when I thought through the patent fight… See, again, my original view was MIT and RSA were the bad guys and had lied to us, etc. When I tried reframing it, how could MIT and in particular RSA see me as the bad guy? I put myself in Ron's shoes – "Here I go and tell Marty this thing and he goes and gets this letter written trying to kill our company." So both sides made mistakes.

So that's a little more on Hellman Associates than you asked for.

HW: Did you become involved in the computers privacy debate?

MH: Yeah. Well, the DES controversy was part of the privacy debate. How much security should people have and does the government have the right, does NSA have the right to decide what level of privacy we get? Basically 56 bits is a minimal privacy. So yes, I was very involved in that.

HW: One of the mathematical problems that acquired prominence from your work was the discrete logarithm problem. It had been known for a long time and now it assumed great importance. Can you tell us about this problem and your contributions concerning it?

MH: Yeah, and actually I'll start with John Gill's contributions. I came on the faculty here in '71. John was hired in '72, also in the same lab that I was. He had done his PhD in math at Berkeley under Manuel Blum, who's usually thought of as a computer… is a computer scientist, and John's thesis on oracles and things like… I mean I don't understand it all, but it was a seminal work.

But when I was looking… I think by this time I was with Whit. I was looking for one-way functions, which are the simplest form of cryptographic entity. They're functions that are easy to compute but hard to invert. In general when you're doing research, even if you want to find a cryptographic system which is more complex than a one-way function, you usually start with one-way functions and try to build up.

So I went to John, who knew more math than I did. Oh, and I should mention John's undergraduate work was at Georgia Tech and he's one of the first black graduates of Georgia Tech. A very interesting man. And brilliant. I went to John and I said, "I'm looking for functions that are easy to compute, hard to invert. Do you have any suggestions?" I think the first one he threw out was factoring, which of course is the basis of RSA and which Whit and I had already tried unsuccessfully to use in public-key cryptography, although we should have seen it for various reasons. I said, "No, we thought of that one. We haven't seen how to make it work." I said, "Any others?" He said, "What about indices?" which is the mathematical term for discrete logarithms. I said, "What's an index?" and he explained it's this discrete logarithm and exponentiation is easy to do but discrete logs appear to be very hard.

So I was playing with that function and Steve Pohlig, a former student of mine who unfortunately just passed away about a month ago, worked at Lincoln Labs most of his… in fact his entire career after his PhD, Steve and I came up with a conventional cryptographic system which we published based on discrete logarithms. If we had done the arithmetic mod n instead of mod p, that is mod a composite number instead of modulo a prime, we would have had RSA. We actually had looked at doing the arithmetic mod n. Then you had to the computation mod phi of n instead of mod q minus 1. It was a little more complicated and I think we were doing this before Whit and I had come up with the public key concept, so we didn't actually think of using it that way and we didn't come back to it.

But yes, we looked at discrete logarithms a lot. That was the basis of the Diffie–Hellman–Merkle key exchange. I was playing with this one-way function and

trying different things, and I was trying to create a public-key cryptosystem, but what I created was a public-key distribution system, a Merkle system.

HW: Of course the Diffie–Hellman protocol is broken once a quantum computer with enough qubits is constructed. What do you think of this possibility?

MH: Well, once you can build quantum computers with enough qubits, I don't work deeply enough in this to be able to comment, but I've talked to various colleagues, not in the last year or two, but most of them think it's at least 10 years off before we have to get worried about the possibility and then we'd have another 10 years. So it might happen.

But the other question is "Can we increase the number of bits?" and "Will they be able to build 10,000-qubit machines?" But I have been arguing, and I think I argue this in the write-up of my Turing Lecture, separate from quantum computing, there's another real risk to discrete logarithms and factoring. There have been major advances in both factoring and discrete logarithms, and the same advance always seems to apply to both. In 1970, 1980, and 1990, roughly 10 years apart, each of those roughly doubled the size of the key that was needed. Now since 1990, since the number field sieve, we have not seen any major advances. That's 27 years now roughly. Well, it could be closer to 30 years. So many cryptographers have tended to say, "It looks like factoring and discrete logarithms have hit a brick wall. We're not going to make any more progress."

But with the work I've done on estimating the risk of nuclear deterrence failing where people point to 72 years since World War II or 50 or 60 years with having had enough nuclear weapons to call it deterrence with no catastrophic failures, but I've analyzed that and said, "Wait a minute. How far into the future do we need to project? And with what confidence?" If you want 95% confidence, you can only project a third as far into the future as you can see back into the past. If you want 50% confidence, you can project roughly as far into the future as we can see into the past. But in terms of being confident that we will not have a nuclear war, we probably need 99.9% confidence.

Anyway, I looked at things like this and I then applied it here. I thought of each decade as a coin toss. In the 1970s, the coin was tossed and we had a major advance in factoring. In the 1980s, the same happened. 1990s, we got number field sieve. The aughts, we tossed a coin – no major advance. And in the cu-… Oh, …….. Yeah. So we've had roughly two decades, two tosses without, maybe getting close to three without a major advance. But if you have three heads in a row – that's advances – followed by three tails in a row when you toss a coin, would you dare predict that heads is never going to occur again? Absolutely not.

Now that's a model. Maybe it's not the right model, but it's not an unreasonable model. So I think we need to be, especially if we want 99.9% confidence that our digital commerce will not be brought to its knees, that we ought to be thinking about

backup systems. And actually not just thinking about them but building them in so that right now while public-key cryptography is still usable, you still have a backup system that if public-key cryptography was broken tomorrow by either a quantum computer or a major advance in factoring or discrete logs, that we would be fine. You'd still be able to make do with the second system.

It's like NSA talks about "belts and suspenders." They never want to be caught with their pants down, so they wear belts and suspenders. If your belt is cut, you still have the suspenders. If the public-key cryptography is broken, you'd still have Merkle tree signatures for example for signing things. Or if public-key cryptography is broken, you would still have key distribution centers. Or if the key distribution center is compromised, you would still have public-key cryptography. You just work along seamlessly even if one of them is broken.

HW: Are you happy with what happened to public-key cryptography subsequent to your involvement?

MH: Yes. I try to be happy with what's happened in any way. I mean we have two choices when things happen – we can be happy with them or miserable. And if you can't change them, it's better to be happy than miserable.

Take the election of President Trump. Many things I don't like about it. On the other hand, he's bringing the nuclear threat back into sharp focus for people. A bill was introduced in Congress as a result of Trump's election – it hasn't gotten any traction, but it might – that says that the president cannot legally authorize a nuclear first strike without congressional approval. A second strike, you can't get Congress together, yes. That should have been there under Obama too, but only under Trump are we getting the traction to have that even introduced as a bill.

So am I happy with how public-key cryptography has worked out? Yes, on two counts. First of all, I have no choice, and so I'd rather be happy. But secondly, it's worked out pretty well. It's widely used. Whit and I won the Turing Award – I can't complain about that. While I didn't make $250 million as RSA did, I'm comfortable. I'm a lot better off than delivering groceries up five flights of stairs for a 10-cent tip. So yes, I'm happy.

HW: [chuckles] What was your reaction to the news that the Diffie–Hellman protocol – perhaps I should say "Diffie–Hellman–Merkle protocol" – and public-key cryptography had been discovered a few years earlier by researchers at GCHQ in the UK?

MH: I was a little bit pissed. I was particularly pissed when I got an email sent to a large number of people – I was part of the distribution – from a colleague at another university who shall remain nameless saying, "For the true story of the discovery of public-key cryptography, go here." Well, when my colleagues, including Jim Omura, told me that I was crazy to work in cryptography, one of their reasons was

"How can you hope to discover anything they don't already know? They've had billions of dollars' head start, decades' head start." I kept saying, "It doesn't matter what they know. It's well established that the first to publish publically gets the credit, not the first to discover and keep secret."

But even there, I'm okay with this. First of all, it's important to note a couple things. We don't know what they published in the classified literature and when they published it. They've told us. I believe that they're telling us the truth, but there's no way to be sure. Also, they had nothing on digital signatures, and they weren't careful to point that out in the early papers, and they should have. Also, I don't know if they realized the importance of it.

But where I've ended up is we have two parallel universes – the public universe where Whit and Ralph and I deserve credit, and RSA for public-key cryptography; and then there's this parallel uni-… And in that universe, GCHQ is a footnote with all the caveats – you know, "Whoever publishes first gets the credit" and "We don't know for sure what they had published or if…" I mean they've produced it now. Although I'm 99.9% certain they're telling us the truth about that, but still it is a caveat. And in the classified literature, they get the credit and we're a footnote. That's how it should be. But fortunately it's worked out pretty well. I was a little concerned at the time, like with this colleague's email. But largely the public universe has treated GCHQ as a footnote. An important footnote, but a footnote.

And my heart goes out to these guys. They toiled in anonymity and it's got to be really hard for them to see us getting more of the credit publically than they. To the extent that the work they did benefitted my security, I have to be thankful. To the extent that they contributed to things like Vietnam and Iraq, I mean things like that in the past, it's fine with me that they toiled in anonymity.

HW: Much of what we're discussing was written up for popular consumption by Steven Levy in his book Crypto. What do you think about this book?

MH: Let's see. I think Steven did a great job. There was a problem though, that Steven, as I think many authors, likes to have a hero in each chapter. In the chapter on public-key cryptography, Whit is the hero and I am almost an afterthought, and in the chapter on DES, I'm the hero and Whit's an afterthought. Unfortunately only the first one, the one where Whit's the hero, was published in *Newsweek* I think it was, and a cousin of mine who got *Newsweek* said she wanted to murder somebody. She's my best publicist. But I think… I mean he did a wonderful job of publicizing it and I understand why he liked… To create interest and to get the large readership, you have to do that kind of thing.

HW: The Turing prize is the equivalent in computing to the Nobel Prize in other areas of human achievement. How did you react to the announcement that you had won this very prestigious award?

MH: I'm going to tell a story on myself. My professional association has been primarily with the IEEE. That's where I published, that's where I was an editor, and I actually wasn't even a member of the ACM when I won this award. I knew it was the top award, but I didn't know a lot about it. So I get the call from ACM and they're telling me I've won the Turing Award, and I think what a great and wonderful thing. But I didn't realize, among other things, that there was a million dollars connected with it. [laughs] The next day, so it's almost 24 hours later, I'm talking with one of Stanford's PR people and he says, "So Marty, it's a crass question, but you're going to get asked this. What are you going to do with all the money?" I had to say, "What money?" And he explained to me.

So I was pleased, very pleased to be honored this way. I thought it was particularly gracious of the ACM to give the award to somebody they felt deserved it who was not a member, I mean. But then when we learned that there was half a million, at least my half of the award, I talked with my wife about this, Dorothie, and we quickly agreed to use my half of the million to further our efforts to build a more peaceful, sustainable world.

And we are doing that, with the initial focus being on publicizing the ideas in a book that we wrote that combines the… Someone described it as a "unified field theory of relationships." Unified field theory of physics would take quantum mechanics, the very small, and unify it with relativity, the very large. Here we take the very large, nuclear war, take it through conventional war, because the most likely way a nuclear war would start is some small conventional conflict escalating out of control likely – Turks shooting down the Russian jet a year and a half ago. But we also take it down to the micro, to the microscopic level, in our case the marriage or how I interact with Jim Bidzos. Do I demonize him? Do I demonize NSA? Or do I try to understand their perspective? Do I have respect for them? I might disagree with them, but do I respect them. And we explain how not only are the same tools needed to avoid divorce and nuclear war, like "Getting curious instead of furious" is one of the ways we summarize it.

But we also found that working on both at the same time actually accelerated progress on the two of them. You might think that if you're working on your marriage, as we were, putting energy in on the global challenges would take energy away from this. But we found quite the opposite, that this actually accelerated our efforts. Just one example. It was very hard in the early phases of making our marriage work for me to face my part in the fights we had, and it was hard for Dorothie to face her part. Each of us was into blaming the other, just like NSA and I were each seeing the other as the devil.

There were times… We both had this, and this is Dorothie's part of the book. She says, "Sometimes I would go into the bedroom and throw myself down on the bed with my arms outstretched" – she admits to being dramatic – and she would plead to the heavens for help. She says, "I don't know why I kept asking, because the answer was always the same," and it was just in her head, it wasn't a voice booming

out of the clouds, and it was "If you cannot make peace with the man that you're supposed to love most of all on earth, how can you expect world leaders to overcome their conflicts and avoid a nuclear war?" It literally would be the end of the world if she did not make peace with me, and that gave her the motivation to persevere when otherwise she would have given up.

HW: You published a number of research papers on various aspects of cryptology up to about 1983. Then, apart from producing a few scattered articles, many of them expository, you seem to lose interest in the subject. I think you alluded a little bit to this earlier, but what happened?

MH: I changed careers. In 1980, I realized, I woke up to the fact that if I kept doing what I was doing, if I kept Spock-like using logic when it didn't apply, illogically, my marriage was going to blow up in my face. And it surprised me that I was willing to change radically, and part of that radical change was to take on these international challenges that I was just talking about, particularly nuclear weapons.

Remember, Ronald Reagan became president in 1981, and while the world was very dangerous under Jimmy Carter, his predecessor, we only realized that under Reagan, just like, as I said before, we should have had a law – we should have a law, we still don't have it – that prevents the president from unilaterally initiating a nuclear first strike. That's a dictatorship. That's not democracy. And what's the point in allowing that? It's a very dangerous situation. But only with Trump bringing the nuclear threat into focus for people has that bill even made its way to be introduced in Congress, much less passed. In the same way, Ronald Reagan brought the nuclear threat into focus to us by talking honestly about the war-fighting plans that our government had. That's what got me working on that other issue.

HW: Now I want to turn to your achievements subsequent to your cryptologic work. I know in the 1980s you became very interested in the problem of nuclear deterrence, and you've mentioned it several times in this interview. In fact, I can recall that you returned from a trip to the USSR sometime in the '80s and were very excited by what you were doing there. Can you tell us something about how and why you became involved in this project?

MH: Sure. The simple two-word answer is "my wife." As I've explained, I was so illogical in my use of logic that it was ruining my marriage, but I was so oblivious that I didn't realize it. Dorothie was looking for catalysts to improve things. Starting in 1980, she found something that was working, and we worked at both the interpersonal and the global level at the same time. Initially the group was working… The group doesn't exist anymore, by the way. It was working on environmental issues. Then Reagan became president in January 1981 and his honest or loose talk, a little bit of both, about fighting and winning a nuclear war, we began to realize, the group realized that the biggest environmental threat of all was a nuclear war. It could happen while we're sitting here and it would be over and the environment would be totally destroyed.

So we started to research that problem. It was a really capable group of people. A number of Silicon Valley entrepreneurs had left their careers to work with the group full-time as volunteers. We concluded that you actually could not solve the nuclear threat in isolation from the war system itself. I still very much agree with that, that there's a problem that too many groups working on nuclear disarmament for example don't see the need to build a more peaceful world before you can ever have a hope of nuclear disarmament.

But one of the big questions was "What about the Russians?" As we talked, we developed a grassroots movement in this country called the Beyond War movement. We'd have people into rooms like this and show a video and talk and try to get people, new people who wanted to work on changing this behavior so we would survive as a civilization. But the question that came up repeatedly was "What about the Russians? We can sit here and debate and encourage our government to change. The Soviets, the Russians cannot do that. What's the point?" We had two answers, one of which was "It's a system." If we change, they'll change. We can't be for sure, but we have open, that's all we can do, is try to change.

But the other answer was Dorothie and I had been very lucky to have had relationships with Soviet information theorists. We'd had them in our home. I'd met them at conferences. Not always, because when the Russians are around, then there might be hidden microphones. In the Soviet Union, they could not talk honestly. But in the same study where I came up with that Diffie–Hellman–Merkle key exchange in May '76, a few years earlier, it must have been 1973, there was a Russian information theorist visiting at Berkeley and he'd come down and stayed overnight here. I remember him asking me, he says, "Martin, in school we are taught that the United States and the West held up on opening the second front" – you know, D-Day – "so that the Soviet Union would bleed itself dry. What are you taught?" He was curious. We'd had honest discussions like that. We said if there was a way that more Americans could have that, could experience that, that they wouldn't be asking these questions.

Now we knew they had censorship, so we knew we couldn't have those openly. But still, in September 1984, Dorothie and I went over to the Soviet Union to an international symposium on information theory sponsored by their Academy of Sciences. The IEEE sponsored one and there were two not quite competing but parallel international symposia. With help from Pief Panofsky, now deceased but a very significant advocate on arms control in this country and Director of the Stanford Linear Accelerator at the time, and Sid Drell, who passed away within I think the past year or two, or past year actually, who was also very big on arms control and also prominent at SLAC, with help from them, we were able to meet with key people in the Soviet scientific community working on arms control. Because I knew information theorists, I didn't know arms control people.

We didn't know it, but we were meeting with people who, once Gorbachev was in power and we knew about the reform movement, they were in the precursor to that reform movement. We could tell by the way they talked with us that they were different from anything else over there. So we came back extremely excited, but we had trouble even getting people in our own group to believe the experience that we'd had.

But out of this eventually grew a project two years later, after Gorbachev was in power and after he lifted censorship, we could do the kind of project we'd always wanted to do. We published a book in Russian over there and in English over here simultaneously. I mean obviously different languages, but otherwise word-for-word the same, and we had to be very careful on that because we knew anyone would pick up on differences. It was called *Breakthrough: Emerging New Thinking*, and it was a breakthrough. It talked about the equations of survival in the nuclear age and how we had to change. It was the first time in print I'm sure that any Russian author, especially for a Western audience, questioned their invasion of Afghanistan. That was questioned in there.

The book came out in November '87. It actually has a 1988 copyright, but it came off the presses in time for Christmas gifts that year. Beyond War had about 20,000 people involved, so I think we sold 50,000 copies in this country and there were 50,000 roughly sold in the Soviet Union. It was a question of how many they could print. And, well, almost no one has heard of the book, so you could say it made no difference, and maybe it didn't. I think it had a… I like to think it had a profound impact, not necessarily in how many people read it, but we were talking with people who advised Gorbachev. We would talk with them about how the image of the enemy was a major problem, the demonization. Like Inman saying to me, "It's nice to see you don't have horns," or as we now demonize Putin and the Russians. I mean they make mistakes, but they're not the devil incarnate. We talked about this image of the enemy and how dangerous it was, and a few months later I'm reading a new report and Gorbachev was talking about the image of the enemy. Now we weren't the only group talking about it. There were other Western groups bringing it up. But I think we had some impact that way.

In January 1988, soon after the book was out, Beyond War, the group that no longer exists that we worked with, had about 8 or 10 of the Soviet contributors and 8 or 10 people from the West who had worked on the book pair up in teams. So a Russian… a Soviet and an American, and we'd go around Iowa for example – we had a presence in Iowa – New Hampshire. I was teaching so I could only do it in Northern California and only for one of the two weeks. Someone else had to fill in me for the other. But I will never forget. I think it was Modesto. We had about 200 people there.

Remember, this was right after the INF agreement had been signed in December '87 in Washington, and Gorbachev had gotten out of the car and all of a sudden, we took him seriously. Up to that point, the attitude had been "He's a communist.

He's just talking a good line. Don't trust him." But when he got out of that limousine and, like an American politician, shook hands with people. There was this sudden phase change in American beliefs.

And very fortunate – we can't take credit for the timing – the next month we had this speaking tour. I was with Rauschenbach, who was a Soviet German – I mean you can tell from his name, his family had moved there 200 years earlier to help, I don't know, with the navy or something under Catherine the Great. I was teamed up with Rauschenbach, who was a rocket scientist, literally. Someone in the audience says, "What about Stalin?" after our talk, our presentation's over. I'll never forget Rauschenbach saying, "He was a murderer and a terrorist." The audience was stunned that a Russian, a Soviet could say that, and it was the first time they could say things like that.

We all convened back in Washington and had a meeting at the State Department. We did a satellite broadcast. I mean Beyond War was amazing. We were organized with all these Silicon Valley types involved. But we had a meeting at the State Department with Whitehead, who was the number two man, the Deputy Secretary of State. And he's lecturing the Soviets on things like Stalin. The woman at the State Department who'd arranged things was an old high school friend of mine, I mean just coincidentally. I was sitting next to her, and I whispered to her, I said, "Bekhtereva's father was executed by Stalin," one of the Soviet scientists who was there, Natalia Bekhtereva, a very prominent scientist, member of the Academy of Sciences. And Elly, my friend, says, "I wish I had known that. I could have told the deputy secretary and he wouldn't…" I mean, but it was just amazing. You can see why we were excited.

And unfortunately we blew it. I mean the Soviets blew it with the corruption and the stealing of the economy, and we blew it by claiming victory in the Cold War, which is ridiculous. We did not defeat them. It was they tore down communism. And Jack Matlock, who was Reagan's ambassador to Moscow, has said that very same thing – we did not win the Cold War.

HW: You're still very much involved in defusing the nuclear threat. Are you optimistic?

MH: I'm always optimistic. It's just like "Am I happy about how public-key cryptography has worked out?" You have two choices – you can be optimistic or you can pessimistic. Actually something that one of the founders of what became Beyond War… It was a husband–wife team, and the husband was a professor of business law here at Stanford, Harry Rathbun, who was really very prominent. Sandra Day O'Connor credits him with being perhaps *the* major influence in her life, her professional life, why she went into law. She gave the first lecture in his memory, the Rathbun lecture series. The Dalai Lama gave one recently.

Harry died in the 1980s, I think 1987. He was born in the 19-… I'm sorry, the 1890s, so he lived into his own nineties. I remember one of Harry's favorite

questions was "Why not assume the noble hypothesis? What's the harm?" So when it comes to the nuclear threat, there are two hypotheses. The noble hypothesis is that humanity is capable of the great changes required to survive in the nuclear age. The less noble hypothesis is "We're doomed. Let's just party." What Harry pointed out is if we assume the less noble hypothesis, we're doomed even if we were capable of the radical change, because we won't be motivated. But if we assume the noble hypothesis, what's the worst that happens? The worst that happens is we go down fighting and we might just make it through. I can remember him saying, and he always had a twinkle in his eye when he said it, "Why not assume the noble hypothesis?" So yes, I'm an optimist.

HW: What is the Daisy Alliance and what is your connection to it?

MH: Daisy Alliance is an NGO in Atlanta, Georgia, a Georgia-based NGO, which takes its name from the famous, at least to people of our generation, daisy advertisement, political ad that Lyndon Johnson used in the 1964 election. Remember, he's running against Barry Goldwater, who he portrayed as a loose cannon. Actually I've read *The Conscience of a Conservative*, which is Goldwater's campaign book basically, and he wanted to use nuclear weapons just like they were conventional weapons. He says that very clearly. So Johnson had this ad where there's this little girl and she has a daisy and she's counting, "One" – she's picking off the petals – "two, four" – you know, she's little – and then she gets to 10 and then this male voice comes on, "10, 9, 8…" and it counts down and then there's a mushroom cloud and just a flash I think. And it says, "Vote for Johnson. It's too important."

The Daisy Alliance takes its name from that ad. Bruce Roth, who founded it, is very dedicated to resolving this threat, and in particularly working in the Southeast. I'm on their board of advisors. I think I'm actually on their board of trustees. So I've worked with them, given talks there. A very good group.

HW: During the late 1980s, you received at least three awards for your efforts to defuse racial tension at this university. Can you tell us something about this?

MH: Oh sure. That's fun. So 1980… Beyond War was very unusual. As I said, we had Silicon Valley types, entrepreneurs, venture capitalists, one of them at least. These men had made enough money that they could do whatever they wanted to for the rest of their lives. What they decided they wanted to do was work as full-time volunteers on ending war. I mean really strange. Dorothie was working as an accountant, a CPA at Touche Ross, one of the Big Eight accounting firms, now Big Four. It would be Deloitte Touche whatever, some Japanese name, "Tohmatsu" I think. She was headed for a partnership. She left her career to work as a full-time volunteer. I was ready to resign my professorship at Stanford to work as a full-time volunteer. I mean this was the culture, and we loved doing what we were doing. And it makes logical sense – if you really believe that the survival of the world depends on taking this seriously, you would do things like that if you could afford to.

I actually ended up taking a year and a half leave without pay to work as a full-time volunteer, but during that time, it became clear that my position at Stanford was critical to the success of Breakthrough. The Soviet Academy of Sciences could not work with an NGO. They could work with a world-famous scientist at Stanford. I hadn't realized that. So I came back to Stanford and I'm really glad I did.

But when I came back from the leave, I started teaching undergraduate courses, which I'd always wanted to do, and there were more black and Latino students in the classes. The racial tension was very thick on campus in those days. Stanford had admitted enough… It was very successful in recruiting minority students, so successful that there were enough of them to become a pain in the rear. Because when there's one or two, they don't want to stand out, but when you have 8 or 10%, they can start to say what the problems are and demand change.

When I came back and I saw this going on, I saw it as very similar to what had gone on between the United States and the Soviet Union. Each side was really good at seeing what the other was doing wrong and pointing out how they needed to change, which produced no change. Just like in my marriage when Dorothie and I each tried to change the other, it didn't work. But neither side was really looking at its own problems. The administration at Stanford talked about how wonderful Stanford was for minority students, and yet I knew from talking with the minority students that they were deeply unhappy and didn't feel fully accepted, didn't fit in. There was more racism on campus than we realized. But I also saw that the minority community had its own part in this. They had their prejudices.

To take an example, I'm Jewish, Dorothie isn't. It was supposed to be… If her parents had been upset that I was Jewish, that would have been antisemitism. The fact that my parents were upset that she wasn't Jewish was supposed to be understandable, and yet it hurt her just as much. The same thing goes on when there's an interracial marriage. The white family's racist if they're upset; the black family is just understandable if they're upset at a white son-in-law, daughter-in-law.

So I started working on these issues, it seemed very similar, and was able to have some really good success. It wasn't just getting past the racial prejudice but helping the students perform better, realize more of their potential. Like there was one student who was unhappy with how he was performing, so he started working harder and harder and harder and harder. He was studying almost 24 hours a day. He was killing himself. I told him he needed to cut back.

With things like that and bringing understanding to the issue and bringing a non-blaming environment, I was very pleased that the SBSE, the Stanford Black Scientists and Engineers, gave me their outstanding professor award twice, and SSCLES, the Stanford Chicano and Latino Engineers and Scientists – both are affiliated with the… like SHPE, I think "shape" or "shep" is the national for the

Latinos – gave me their outstanding professor award and asked me to be their banquet speaker. I was very honored by that.

I'll tell you one other little story. When I'm the banquet speaker at the Latino affair, I talk about how when I met Dorothie on the beach in Catalina, and about 10 minutes into our relationship she asked me if I'm Jewish. As a kid growing up, whenever anything about Jewish came up, it was always "dirty Jew," "Christ killer," that kind of thing. So in the talk, I said, "A minor earthquake went off inside of me." Fortunately I didn't let it get in the way of it, I didn't take it the wrong way, and we have this great relationship. One of the Latino students came up to Dorothie afterward and he says, "Are you sure you didn't mean something by that?" It just shows how powerful these things are and how all of us need to change. It's not just… Racism exists on all sides, black as well as white, brown.

So I learned a lot from that. I developed some wonderful relationships.

HW: You served during the '90s on the National Research Council's Committee to Study National Cryptographic Policy. Can you tell us what this committee achieved?

MH: Miracles. Prior to this committee being formed, it was almost impossible to export even 56-bit DES, as weak as that was, from this country. Most of the commercial encryption, it had to be much weaker. Congress, with some prodding actually from the National Research Council – there was a little back and forth – asked the National Research Council to form a study committee to look at our national cryptographic policies, particularly export restrictions, to see if they were adequate for the Computer Age. Because there's a trade-off. If you make strong encryption very difficult to export, then you preserve law enforcement and national security access to conversations they'd like to listen in on, but you also give the Chinese and a bunch of other countries access to a whole bunch of conversations we don't want them to listen in on.

The National Research Council pulled together a great committee. In addition to privacy advocates like myself, they had a former Deputy Director of NSA, Ann Caracristi, representing NSA's interests; they had a former Attorney General, Benjamin Civiletti, under Jimmy Carter representing the FBI and law enforcement's interest. We were able to put aside our prejudices – in fact I worked very hard at doing this and the others did as well – and we reached unanimous conclusions. We all had to compromise a bit, but we said, "What is possible?" and "What works best for the country?" We came up with some at the time far-ranging recommendations. That's why I say "a miracle." We recommended that 56-bit DES be almost freely exportable, which was unheard of and a great step forward. It's actually created… Now our recommending it doesn't mean it happens, but within a year or two, that in fact happened, and I think it played a key role. It really was this respecting one another and really trying to understand each other's point of views that allowed us to reach unanimous conclusions.

I've tried to do something similar today with the Apple–FBI as an example. I'm working with a man who independently tries to do similar things. He came to me and he said he's trying to do something along those lines. This is a man very prominent in Republican politics. I said, "Oh, I'd love it." I was actually trying to do that and I'd had some emails to a deputy director of the FBI saying, "Hey, can we talk off the record," because when you fight it out in the press, you never get anywhere. You have to try to understand one another as a way to start. Hopefully that will happen.

HW: Very recently, and you've alluded to it several times, you and your wife Dorothie completed a book entitled A New Map for Relationships: Creating True Love At Home & Peace On The Planet. The book has a very unusual premise, which you've told us a little bit about. Was there anything more that you'd like to tell us about?

MH: Yeah. Well, first of all, if anybody wants to get a free copy of the book, I mean obviously using our $500,000 to promote these and related ideas, we're not just trying to make a buck here, but we do have a PDF freely available on the book's website. People can download it. It's "anewmap.com". So those three words "a new map" run together ".com". Go to the "Get The Book" tab and there's a link you can click to get a free copy in PDF. It's the complete book.

I was very gratified. I mean it's an unusual premise that the best thing you can do to bring world peace is to work on personal peace, and that's actually the only thing you can do. I mean if you're president, maybe you can do more, but you and I, that's what we can do. I was very gratified that Bill Perry, a former Secretary of Defense under Bill Clinton, gave us a wonderful endorsement. He called it "a truly unique book" and he said it "should be read by . . . couples seeking peace at home, as well as by diplomats seeking peace in the world." Karl Eikenberry, another colleague of mine, who led the coalition troops as a three-star general in Afghanistan and later was our ambassador to Afghanistan, again made that connection between we need more diplomacy at the interpersonal level and the international, and said some very nice things.

And it's got some stuff on cryptography in it. People ought to read my Turing Lecture write-up, because there I actually go into how Alan Turing was really the guy that created my cognitive dissonance over… it wasn't Gödel's incompleteness theorem, it was actually… but it was too complicated to put in the book. It was Turing's proof that the computable real numbers are not effectively denumerable, which is a mind-blower. I mean it initially looks like it's a proof that the computable real numbers are uncountable. I mean it's very similar to the proof that the reals are uncountable. How subtle are assumptions? I mean there the subtle assumption is that if something exists, we can compute it, whereas the way that they resolve that is "Yes, something exists, but we'll never know it. God knows it, but we don't." I mean what a subtle assumption. What other assumptions might there be?

In fact one thing I'm working on now is looking at trying to convene a major conference that would then reach the public looking at the assumptions that underlie our national security thinking. Because if you have assumptions that you don't recognize as assumptions and any of them are false, you end up with a house of cards. As an example, the United States is the world's sole remaining superpower. That's stated as fact repeatedly. Is it true? Well, what does it even mean to be "a superpower"? We can be destroyed in under an hour. Is that a superpower? Would a superpower have the results we had in Iraq and Afghanistan? Then what happens if we believe we're a superpower, in fact the only superpower, when we're not?

I would argue that maybe we jump off tall buildings thinking we're Superman expecting to fly, and when we crash to the ground, we don't learn our lesson. That happened in 2003 in Iraq. That was the tall building we climbed up and jumped off, and we didn't learn our lesson. 2011 under a different president, different party in power, Democrats instead of Republicans, we climbed up a tall building, jumped off, and crashed to the ground. We're repeating the same thing in Syria. Now maybe Syria's different. But until someone analyzes it and shows me why regime change in Syria is going to work better than regime change in Iraq or Libya, I think we need to be very cautious. The people of those countries are worse off and our national security is worse off. Jihadists who had no power in Iraq under Saddam Hussein, no power in Libya under Gaddafi now control large parts of those countries and threaten us.

HW: I'm going to go now into questions that are more on a retrospective frame. How many graduate students received postgraduate degrees under your supervision, roughly?

MH: Oh, not that many. It'd be about 10. I mean many faculty have a hundred, but I have only about 10, partly because I was only really active from '71 to '81, about 10 years before I moved into these other areas.

HW: Can you tell us something about what some of them have done since leaving Stanford?

MH: Well, Ralph Merkle. Ralph started his work at Berkeley, but no one appreciated him there. In fact a professor, when he proposed public-key cryptography as a term project in a CS class, the professor said he ought to work on the other idea that he proposed instead. Ralph quit the class and worked on public-key cryptography.

So Ralph was a PhD student of mine. I joke that I kidnapped him and brought him to Stanford. He works on nanotechnology and he works on… Very different from me. He works with this group that – I'm trying to remember what it's called… Foresight Institute – that when they die, their heads are going to be cut off and frozen in liquid nitrogen so that… When technology allows you to be cloned from a single cell, that only clones your hardware. What about all the software that's in your brain, your life experience? You don't want to come back to life as an adult

with none of those experiences. The idea is Ralph is working on nanotechnology partly so that nanomachines can go into your frozen brain, read out all the connections, and reprogram them into your cloned brain. Not what I would be working on, but Ralph is brilliant and very different.

Whit Diffie. [laughs] Well, he was technically my student for maybe a year or two. We never finished his PhD because Whit, as I put it, is… In fact in the ACM video that they made for the Turing Award, it starts off, we're sitting in the same couch, Whit and I together, and I say something like, "It's often said that Whit was my student, but Whit can be nobody's student. He's much too independent." Whit then says, "Well, actually it's a very useful talent. I just don't have it," something like that. To the extent that you count Whit as a student, Whit has done wonderful things working on privacy issues, various aspects of security at Sun.

One student was from Brazil. In fact I'll never forget… He taught himself English. I remember him telling me that he couldn't believe, he thought someone was pulling his leg when they told him that "Arkansas" was not pronounced "Are-Kansas." Aydano Carleial. He went to work for the government there in a research center.

Steve Pohlig, who I mentioned, worked at Lincoln Labs on various government projects.

Oh, Justin Reyneri. Justin, he could build anything. He actually was a math major as an undergraduate. In fact when he became my graduate student, he came to see me because he was trying to get some units transferred somewhere. He was trying to do a master's in electrical engineering and he came to me to see what math units could carry over. I said, "By the way, if you want to do a PhD," because he impressed me immediately, "if you want to do a PhD in electrical engineering, you could do that and I have a research assistantship you could have. It doesn't pay a lot, but you could support yourself."

He could build anything. He built a DES board for a PDP-11 computer so we could speed up computations. He was working on the random graphs that I talked to Don Knuth about that I mentioned earlier. He's been at Synopsys and other places. It's interesting, he went into computer-aided design. It turns out information theory actually comes in there.

Abbas El Gamal, who is our current department chairman, was not my PhD student. He was Tom Cover's, so he's my kind of academic brother. He was one of the founders of Actel, a field-programmable gate array company. In fact for a while, it was… oh, there was a whole group of information theorists working on computer-aided design at this one company. They just were doing great things.

Then Susan Langford, my last PhD student, I don't know if she's still at HP. She was at HP Labs. So all over the place.

HW: You elected to take retirement in your early fifties.

MH: It was actually 50.

HW: Hmm? At 50?

MH: Yeah.

HW: That's quite unusual for an academic. Was there any particular reason for **this?**

MH: I didn't know what it was and I'm still not sure what it was. First of all, I started teaching when I was 23, so I had 27 years of teaching. It's hard to qualify for emeritus status at age 50, but because I started teaching so early… I didn't know what it was at the time, but the job that I used to love was becoming burdensome.

It started with committee assignments. Early on, they were never my favorite thing, but I'm a kid from the Bronx and I'm not as refined as most people, so I'd be in these committee meetings and instead of the typical Stanford thing of "Oh yes, oh no," I'd actually sometimes be able to shake things up enough to make it work. I enjoyed that early on. But as I got close to this point where I needed to retire, I'd feel like a caged animal in those committee meetings.

I still love the magic lessons, the classes where you teach things like Fourier analysis where you add up these smooth sine waves and get a square wave. I mean it's magic. But making up exams, which again I used to think of as a nice exercise, "How can I teach them something?" I had to force myself to do it.

So the job was becoming progressively more burdensome. I didn't know what it was, but I'd learned to pay attention to my intuition as well as my head. Something was telling me, "Time to get out," and so I did.

In hindsight, I think it had to do with my wife's health, which was getting worse at the time. It's fortunately better now. But there were several, five years in there, maybe more where really my primary job was being a caregiver to my wife. She was drugged up a lot of the time. So just before I retired, I might come to her and say, "Hey Dorothie, I have to leave now for a meeting with the department chairman. Is there anything you need before I go?" and she wouldn't answer me. Now she might not answer me because she was drugged out and somewhere else, or even without the drugs it was painful to be in her body with migraine headaches, and so she would go elsewhere. And sometimes it was just that… Well, I work on a clock five times as fast as her even now, but back then it was 50 times faster. It may have just been that she was going slowly. If I was working at the pace that I needed to work at to be a Stanford professor, it would have caused problems in our relationship or for the job. So it wasn't a conscious decision, but in hindsight, I think I intuitively knew that I had to slow down.

But then it's wonderful. I don't get paid, that's the negative side of it. But thanks to Jim Bidzos and RSA creating this wonderful market and making money with PayPal and things, it's okay. I can do anything a professor does. I could even have PhD students if I wanted to, if it made sense. I just don't get paid for doing it, so I get to pick and choose. It's wonderful. And I spend most of my time when I'm on… Well, here we are on campus in this house, but when I go to the academic part of campus, I'm mostly at CISAC, the Center for International Security and Cooperation, where Bill Perry and Karl Eikenberry and a number of other people that I've met have been really helpful to me in working on these international security issues.

HW: Who during your career were your most influential role models?

MH: Hmm. I didn't realize at the time, but my father was an influential role model, not just with his being a physics teacher but with his enjoyment of life. As I mentioned, my mother's family had money, my father's family had freedom. That was important, because slave-driving yourself is not good.

My mother was an important role model. My wife and I have joked that if she'd been born a generation later, she would have been running a billion-dollar company. She was a very capable woman. Instead she put all that energy into raising three sons, which is one reason I ran away to California as soon as I could. But she taught me a lot of really important things. She taught me how to save, which is why I am free to do what I'm doing. I mean a number of people make a lot of money in Silicon Valley, but if you live to the fullest extent of what you're earning, you can't afford to do what you really want to do. So my mother.

My Uncle Charlie, Charles Hellman, my physics teacher.

Palócz, the Hungarian refugee professor I mentioned. A true gentleman. I mean aside from technically, just had to be a person.

Harry Rathbun, who I mentioned, and his wife Emilia. Emilia had no advanced degrees, but she was a powerhouse and she knew a lot. She had her blind spots, which I didn't know at the time, because when you're in the group, you had to put the blinders on and pretend everything was perfect. But I learned a lot from her, and I unlearned the things I had to unlearn from her.

Tom Cover, my PhD advisor, wonderful role model. I used to joke that the Stanford approach to research was to skim the cream off the top. If we got to the sixth page of equations, we figured we were on the wrong path, whereas at MIT in the information theory group, when they got to page 7, they were just warming up. Both approaches work, but I do like the approach of looking for the new areas.

And I'm sure there were others, but that's enough for now.

HW: Looking back, what were the turning points or major decisions that led you to where you are today?

MH: Ah, major decisions that led me to where I am today. When I was in third grade at age eight, I wanted to be an explorer – you know, we were studying explorers – and I was very sad because I knew I couldn't be an explorer, I had to be scientist. I don't know how I knew that and I didn't know about engineers. There was something early on in my life that told me I had to do that.

Then coming to Stanford was a key thing. I mean in many ways. Not just in terms of who I met but the culture here being so open, the California culture being much more open than the New York culture, which is much more open than the European culture. I sometimes say that the malcontents from Europe came to New York and the malcontents from New York moved to California. So there's an openness to new ideas.

Then marrying my wife. I didn't know what the hell I was getting into. It's a good thing. I would have run the other way and it was the best thing I ever did.

Then screwing up my marriage enough that I had to change, and Dorothie finding and insisting that we find ways to change. I hadn't realized it, but as we wrote the book, she told me she knew our marriage was in trouble before I did. She had actually contemplated should she leave, as many women in fact do. But she decided no. First of all – I love that she tells me this – she said, she tells me I'm the one. [pause 14 secs] She knew the first day we met that we were going to married. It wasn't like she *wanted* to marry me, but she just knew that. She's very intuitive. So screwing the marriage up enough and having Dorothie there, I describe it as in the *Inferno*, "Dante had his Beatrice. I have my Dorothie." As I say in the book, she's truly lived up to the meaning of her name, "gift of God."

Ah, turning points. Getting involved with Beyond War. Learning from Emilia. Leaving Beyond War so I could unlearn some of the things I had to unlearn.

Then writing this book has been a really powerful experience. We've learned a lot. By the way, we haven't had a single fight in 15 years, including writing the book. Our goal was the same, to make the book as good as possible. Why would you fight if you're trying to make it as good as possible? She has a different perspective from me. She has a perspective that many other readers will bring to it. I need to understand that rather than disrespect it and fight it.

And my children and my grandchildren have been big teachers. They've mentored me.

HW: What's your biggest regret in terms of decisions you've made?

MH: None. I mean take my screwing up the marriage. I could regret that, but if I hadn't screwed it… Dorothie said that if the marriage had been bearable, she probably would have put up with it, but because it was unbearable, she was going to get it right, and I'd much rather have it right. So I do have a view of life somewhat mystical that everything happens for a reason, including like in this case. I'm not going to impose that on other people – I mean someone gets cancer, I'm not going to say, "There's a reason you got cancer." But everything that's happened to me, I wouldn't change. Including getting beat up as a "Christ killer" as a kid. That taught me some very important things, because I then had to see the prejudices that we had against the kids who beat me up. I mean they hated me but I hated them back. It was a very similar things.

HW: What were your most important life lessons?

MH: I could be 100% certain that I'm right and 100% wrong. That happened in the room right over there. There's a story in the book about that. There was this video that I would not use. It was a horrible piece of propaganda and Dorothie kept saying, "But everyone else is using it so successfully." Finally she pulls the ace that she always has up her sleeve out. She says, "Why don't you try this as an experiment?" Any women listening out there who have husbands or vice versa who use logic, what scientist, what engineer can refuse to try the experiment, be that close-minded?

So we show this video that I hated to the then-Dean of Engineering who's given me permission to tell you what happened. It was Bill Kays. I'm dying a thousand deaths as we're watching this video because it's worse than I remembered it. At the end, there's this silence. And I was so certain that everyone hated the video that I nearly broke the silence to say, "I know it has its problems, but it has some good points too." But fortunately I kept my silence. Bill Kays is the first one to break the silence, the then-Dean of Engineering. He says, "We've got to do something even if it's unilateral. This is too dangerous." And I go like that. Everybody had been impacted by it.

It turns out the reason I hated the video so much was my shadow side appeared in it. We all have shadow sides. They're parts of our psyches that are so repugnant to us that we can't admit they're there. And when we can't admit they're there, that gives them free reign to blossom all over the place, which is why we make the mistakes we make. My shadow side in that film was an arrogant Jewish professor from New York. I didn't even realize that's why I hated the film. It took me time to realize that. And I don't even know that he was arrogant, but he impressed me as an arrogant Jewish professor from New York, and that was my dark side.

And – this is also explained in the book – I had to embrace my dark side. When I took NSA on in the mid-to-late '70s singlehandedly, when I worked on cryptography when my colleagues all told me I was crazy, it took a certain amount of arrogance or courage to do that. Today people tell me I was courageous. Back then, they would have said I was arrogant.

HW: What was your proudest moment?

MH: I might get teary again. Dorothie saying that we had built the relationship she'd always dreamed of. That I could change that much, that I could go from being that self-satisfied, smug, arrogant Jewish professor from New York and become open enough to have "the Princess and the Pea of relationship conflict" tell me that.

HW: What contributions to computing are you proudest of or you think are the most significant?

MH: Mine or in general?

HW: No, yours.

MH: Well, public-key cryptography very clearly. But also I would say, it's different, but establishing the right of researchers who have not had access to classified literature to publish their results, that was very important. And creating an environment where even the then-Director of NSA would now say that that was the right thing to do, I'm very proud of that. And proud that we can be friends about that and instead of saying, "See, I told you so," we both celebrate the fact that we each had blinders on in different ways.

HW: Are there any other interesting things that you worked on that we should talk about?

MH: Yeah. I was inducted as a Stanford Engineering Hero. They have this program where they induct about five or six faculty or alumni every year, and I was part of the first two dozen inducted. Given that Hewlett and Packard were a little before me, when they called and told me this, my first reaction was "Why me?" and my second reaction is "Keep your mouth shut."

But in that talk… And it's online. If people do a web search on "Hellman Stanford Engineering Hero" and look for the video, it's there. It's "The Wisdom of Foolishness." There's a TV in the other room that we bought about 10 years ago, and we barely use it. It's rarely on, but we use it occasionally. So I made sure… I'm very energy conscious and I made sure it was ENERGY STAR compliant, and Sony said that it used less than a tenth of a watt in standby mode.

But I did what I do with all new appliances. I put my power meter on the thing and let it run for a couple of days. The damn thing was using 15 watts average, not a tenth of a watt. It was off all that time. So I did a little more looking. Sony was no help, and in fact somewhat resistant. They're very nice in other ways, but in this they were not very good. But all the manufacturers were resistant on this.

I eventually learned what the problem was. The TV doesn't just have two modes for ENERGY STAR, on and off. It also had something called "Download

Acquisition Mode" where it downloads a free program guide over a subcarrier from a PBS station, and that is default on. It was using a tenth of a watt in standby mode 25% of the time when I thought it was in standby. 75% of the time it was using 20 watts in Download Acquisition Mode trying to download this stupid program guide that I didn't even use because we have cable.

I then did something very foolish. Well, the first thing foolish is to measure all your appliances. The second thing was I called the EPA and I found the woman at the EPA who was in charge of the ENERGY STAR standards for television, and she was stunned. She said, "Oh my God. Download Acquisition Mode was a new thing and we didn't put any limits on it, but we didn't think it was going to be anywhere near that bad." So I participated in two teleconferences with TV manufacturers and the company that put the program guide on there and made money from advertising, and they all said, "This is crazy," that I was crazy, that they were happy they got it down from 80 watts to 20 watts. And I said, "Look, I'm not a hardware type, but I'm sure you can get that down to five watts and maybe a watt." I later checked with a person who really understood this. He said, "Five watts, definitely. A watt would take a couple of more years," which has now happened.

Anyway, she rewrote the ENERGY STAR guidelines so that there's a limit on energy in Download Acquisition Mode. I've estimated that I've saved the world about a billion dollars' worth of electricity, and all the CO_2 that goes with that. That's something that people wouldn't have known about me and it's covered in that video, the Stanford Engineering Hero talk. There are some notes online and it tells you where to find them, or I ought to put that up somewhere. And it's order of magnitude – it might be $10 billion or it much be $100 million, but it's a lot of electricity. I unfortunately didn't make any money on that either, but that's okay. I'm a lot better off than I was in the Bronx.

HW: [laughs] Are you working on or considering any current or future projects?

MH: Well, this book that my wife and I wrote is our current project. And it's not just the book. It's really this idea that we have a huge problem that we're facing, nuclear weapons. The problem didn't evaporate at the end of the Cold War. I'll give you a 30-second pitch.

Even if nuclear deterrence – that's threatening to destroy civilization to avoid war – even if that could be expected to work for 500 years before it failed and we destroyed ourselves, which seems optimistic to most people on our current path, that's like playing Russian Roulette with a child born today. Why's that? Because one-sixth, which is the risk in Russian Roulette, one-sixth of 500 years is roughly that child's expected lifetime. It's 83 years. If the time horizon is significantly shorter than 500 years – my research indicates it's probably closer to 100 or 200 years – then that child probably has worse than even odds of surviving.

So we have this huge problem, but a huge opportunity. If we look at it the right way, we actually have to… We can't just get rid of the weapons. We have to become a lot more peaceful. We have to become a lot more rational in our foreign policy and in our military policy. We have to stop jumping off tall buildings, like Iraq in 2003 and expecting to fly. That would be a much better world.

But the other key thing is that the best contribution that any typical individual like myself can make is to work at bringing the same objectivity to our personal conflicts that are needed at the international level. Now when Dorothie does something that seems crazy to me, instead of treating her like she's crazy, which drove her crazy, I now go to her and say… There's a story in there about how we bought a new car two and a half years ago, and it made no sense to me that this woman was looking at new cars, because our older car was six years old and we keep cars for a minimum of 10 years. And I went to her and I said, "I can't get over feeling that what you're doing is crazy. But you're not crazy. What am I missing?"

She explained that the new car she was looking at had safety features that would give her more independence with both our age and the meds that she's on – she still has meds for her migraines, although not as bad as 20 years ago. It would give her more independence. I also realized it would make my life better. Suddenly what had been a crazy idea was brilliant, not just in terms of making her life better, which I would have wanted, but in making my life better.

So that's the project we're working on, is getting people to entertain those possibilities. And I'm working on a possible summit at Stanford involving… We don't have commitments from any of them yet. And I dream. This probably won't happen. The wisdom of foolishness that I talk about, you have to swing at 20 wild pitches to hit one fool home run, and this may be one of the 19 that goes nowhere. But I'm hoping it'll happen, and that actually could make the world wake up not only to the risk but to the possibility. Stay tuned. We'll see if it happens.

HW: We've covered a lot of ground, but I wonder if there's something further that you'd like to mention. Last chance.

MH: [pause 5 secs] Well, since the people watching this are likely to be ACM members, computer scientists, very logical people, read what I have in my… it's not yet out, but the CACM will have my write-up of my Turing Lecture about illogical logic, how illogical we can be about applying logic. So when you have a partner, a child, a co-worker who sees things differently from you, you don't do what I did, used to do, which is misuse logic to win the argument and lose the war.

HW: Thank you very much.

MH: Thank you.

[end of interview]