Leonard (Len) Max Adleman

2002 Recipient of the ACM Turing Award

Interviewed by Hugh Williams

August 18, 2016

HW: = Hugh Williams (Interviewer)
LA = Len Adelman (ACM Turing Award Recipient)
?? = inaudible (with timestamp) or [ ] for phonetic

HW: My name is Hugh Williams. It is the 18th day of August in 2016 and I'm here in the Lincoln Room of the Law Library at the University of Southern California. I'm here to interview Len Adleman for the Turing Award winners' project.

Hello, Len.

LA: Hugh.

HW: I'm going to ask you a series of questions about your life. They'll be divided up roughly into about three parts – your early life, your accomplishments, and some reminiscing that you might like to do with regard to that.

Let me begin with your early life and ask you to tell me a bit about your ancestors, where they came from, what they did, say up to the time you were born.

LA: Up to the time I was born?

HW: Yes, right.

LA: Okay. What I know about my ancestors is that my father's father was born somewhere in modern-day Belarus, the Minsk area, and was Jewish, came to the United States probably in the 1890s. My father was born in 1919 in New Jersey. He grew up in the Depression, hopped freight trains across the country, and came to California. And my mother is sort of an unknown. The only thing we know about my mother's ancestry is a birth certificate, because my mother was born in 1919 and she was an orphan, and it's not clear that she ever met her parents. But the birth certificate is enough to guess that she also came from modern-day Belarus and also of Jewish origin. She was born in San Francisco. They met, according to the lore of my family, when my father approached her at a dance and asked her to dance and said that if she didn't dance well, he would leave her on the floor. Knowing my father, I suspect that could have happened.

At any rate, I was born in 1945. In particular, December 31st of 1945. It was kind of an interesting time to be born because when I was conceived there were no computers in the world, when I was conceived there were no atomic weapons in the world, and certainly it would be maybe 10 years before there were any satellites in the world. So it was a low-tech, compared to today, era. And if I may go on a little bit about this? Okay.

An interesting thing was that I was born in 1945, and though television had existed before that experimentally and a little bit commercially in New York City, it came to San Francisco in 1948. When it came to San Francisco and it was a new technology, they didn't know where to sell it. That is there was no Best Buy to go to to acquire a television. So they decided they would sell it in appliance stores. Appliance stores were places where they sold toasters and mixers and things like that. My dad worked in an appliance store. So even though we were sort of maybe lower-middle class economically and could never have afforded this high-tech thing called a television, because my dad worked in an appliance store, he was able to get his hands on one. He brought it home when I was probably like three or four. It was a little black-and-white machine and its screen was about the size of our video… you know, our cell phones now. And he also brought home this huge glass magnifying glass that you set in front of this little screen and it made the picture bigger. Did nothing for the resolution, but it deceived us into thinking we were seeing more.

So I consider myself sort of on the very cusp of high tech. Ever since my time, every kid who's born is plunked in front of, at a very young age, some electronic device like a television. Today it's more likely that it's a computer. But I got plunked in front of it when I was like three. So I began to take in this information that was being broadcast and not learning in traditional ways.

HW: Can you tell me some of your earliest memories?

LA: Wow, my earliest memories. It's so strange because I think my earliest memories may never have occurred. They've sort of got lost in time. The earliest thing I can vividly remember was going to Golden Gate Park. I lived like less than a quarter of a mile from Golden Gate Park. When I was at Golden Gate Park, I went to a place called Stow Lake and I remember getting lost at Stow Lake. Stow Lake had a lot of trees and sort of foresty areas around it, and I remember being lost there and being very fearful. I'd lost track I think it was of my brother. So it's a vivid memory I have, but I'm not sure I didn't dream it. But it's probably the earliest recollection of any sort of image of me when I was young. That would be it, I think.

HW: Tell me about your siblings, if you have any.

LA: I have a brother, Ronald. He was three years older than me. He was tall and I was short. I always admired his name, Ronald J. Adleman, and I thought I got stuck with Leonard Max Adleman – it wasn't anywhere near as good. He was a pretty

good athlete. He was a very handsome guy. And I don't know. He took me a lot of places, but I'm not sure… He would take me to Golden Gate Park. We grew up together, we spent a lot of time together, but I always was the tag-along with his friends. Really, Ron has grown to be one of the most important people in my life only probably in the last maybe 15 years, in which case since then he's become invaluable to me as somebody to talk to, somebody to confide in, to learn from. So I love him a bunch.

HW: What education did he have?

LA: Well, his education actually is interesting because he went to high school, graduated. Then he went to what was then called San Francisco State College, which was what we would call… which you now call Cal State. Oh, excuse me. He first went to a junior college for a few years and then he went to San Francisco State College. By then, it was sort of the emerging 1960s, the 1963, mid-'60s, where the social/cultural "sex, drugs, and rock-and-roll" burst onto the scene, and San Francisco was sort of a hotbed of it. So he got a degree in English not because he knew anything about English. In fact, as I recall, the only book he had read perhaps until he graduated was either *The Babe Ruth Story* or *Black Beauty*. But what he could do is he could write this wonderful stream-of-consciousness poetry. That was in vogue and the professors at Cal State San Francisco liked that, so he graduated. Then he later got a degree or a credential in mathematics and became a teacher of mathematics in San Francisco.

HW: Now can you tell me about your mother's education? What did she do?

LA: I think that my mother was largely… she wasn't… I don't even know if she graduated from high school. She was brought up in an orphanage and in foster homes, so her life wasn't very stable. What she did was she mostly was a housewife, a mother to my brother and myself, but she also worked. She worked in retail sales during seasonal kind of work, Christmas sales, and she also worked as a bookkeeper for private companies and then later for Bank of America.

HW: Where there any others in your family that went on to higher education?

LA: No, I think that is my family, as best I know it.

HW: What was your favorite subject in school?

LA: Well, I didn't have a favorite subject in school. Not for a very long time. Math was always easy for me, that was clear. But I was in my own view amazingly naïve and oblivious to myself and my future. I didn't know anything. I just went to class because you had to go to class. I was the kind of kid that would get called into the office with my parents and they'd explain how on the state tests I was doing very well but I wasn't living up to my potential. But I didn't care. So I had no favorite topic.

But a real turning point for me was when I took, as a junior or senior, a Shakespeare class. It was taught by this brilliant and wonderful teacher whose name regrettably I forget. It was the first time in my life that I realize that there could be something beyond the superficial, that there could be a deeper intellectual world to explore. This woman had a huge effect on my life because one day she called me up and said, "Leonard, I'd like to talk to you," and I said, "Yes, miss." She said, "What are you going to do after you graduate from high school?" and I said, "I don't know. I guess I'll go to City College," because my brother went to City College. You know, I never thought about these things. She said, "Why don't you go to Berkeley instead?" and I said, "Okay." That was it.

HW: Just like that.

LA: Just like that, because I was very obedient, but I seemed to lack context. I didn't see a big picture.

HW: Do you remember a subject that you really hated in school?

LA: Yes! Oh, wow. Yeah, I do. German. At that time, in high school you were forced to take several years of German and then later at Berkeley I was forced to take several years of German. So I probably took German for six or seven years, because when I got to college, I'd always have to drop out of the class because I was failing it. And in fact, after six or seven years, I don't think I knew any more German than I knew after the first two weeks. I faked my way through all of the German classes that I managed to pass. Yeah, and I resented it because I thought that "Why am I being forced to do these things which have no purpose in my life? I know I'm not going to become a German scholar. Who cares? There's two or three hundred different languages that are currently spoken, probably more. Why this one? Why does it matter? Why am I forced to suffer through this?" Yeah. So yes, I hated German.

HW: Tell me a bit about growing up. What did you like to do as a kid?

LA: I think I just existed. My parents would work. I'd get on the bus, I'd go to school, I'd come home. I'd go to the television, as I'd been taught a very early age. And I just did what I was told and what was available and life just flowed by me. I was kind of a voyeur in life. I would watch things around me but I wasn't much of a participant. Where other kids in high school were maybe getting cool and socializing with girls and everything, I was still sitting there just sort of looking around, eating my peanut butter sandwich. I wasn't a very interesting kid.

HW: What did people say about you?

LA: Oh, but one thing did go on. Because of that little television, which later became bigger, I started to watch programs like *Mr. Wizard*. Several times in my life,

there's been these very influential people. The Shakespeare teacher. But Mr. Wizard too. I would get up early before school and I would watch Mr. Wizard who would teach us all sorts of things scientific. So I am one of the few people in the world who understands how to take a hardboiled egg and get it inside of a milk bottle, right? I know this because Mr. Wizard taught me. So I was becoming fascinated with science and all these things, and so that was part of my life. I did early on like science.

HW: When precisely was that? I mean when did you realize that you liked science?

LA: I don't think I realized it. I just did. I just started to watch these programs and… I suspect this would have been mid-'50s. Maybe I'm 10 years old or something like that. But I liked science, so I started doing little experiments and things.

HW: You already talked about an English teacher that you liked. Were there any other teachers as well that you liked in school who helped or inspired you?

LA: Well, up to high school, the one stands out is this Shakespeare teacher. But of course after that, there were a lot of teachers that inspired me, not necessarily formal teachers at school. But one of the great inspirations of my life was really Martin Gardner. And I see you acknowledging that, because for mathematicians of our generation, Martin Gardner inspired it's got to be 50% of us. So Martin Gardner wrote a column for *Scientific American* and it was called the "Mathematical Games" column. He did such a brilliant job. He wasn't a mathematician himself, but he could expose us to mathematics in a way that we who weren't mathematicians could understand and intrigue us, and he would ask questions for us to ponder. It was just so inspirational.

There were two Martin Gardner articles by now sort of grown up that came out that had a profound effect on me. One was "The Game of Life"…

HW: Oh yes.

LA: …which virtually every mathematician has encountered. It was this strange sort of dynamic game that consisted of moving tiles along a very large essentially checkerboard according to certain little local rules. But it was fascinating. It later became called "cellular automata" as a theory. I found it fascinating, and by that time I was between my undergraduate and graduate degrees and I was working at the Federal Reserve Bank in San Francisco as a computer guy.

Martin Gardner asked, because he always asked these questions at the end, "What happens to the particular arrangement, constellation of tiles called the R-pentomino?" Not too important, but what happened to it? The way to find out what happened to it was to play the life game starting with that configuration, except that you would die before you ever got to the answer unless you had a really big computer. And no one had really big computers because no one had a personal

computer, right? The only big computers were in large institutions, often government and things like the Federal Reserve Bank, where they were kept in special rooms with air conditioning and all sorts of stuff going on. Not many people had access to them, but I did because I worked there.

I thought it was a good use of the federal tax dollar to find out what happened to the R-pentomino. So I went in and used those computers to find out the destiny of the R-pentomino. I found out what it does, its destiny, and I wrote to Martin Gardner what its destiny was, I think along with a computer printout to show that it wasn't just a guess or something. Then the next *Scientific American* that came out, there listed among the 10 people who had figured out the destiny of the R-pentomino was me. Me. I. And this was the first time my name had ever hit print. You know, I'd made a mark on the world, right? I had meant something in some crazy way. So that was one very influential thing in my life Martin Gardner did.

The other thing he did was he had written an article on Gödel incompleteness. Gödel incompleteness is a mathematical result. It's done by Gödel and it's based on work by Tarski and other great mathematicians like Church and Turing of the 1930s. It's a mathematical result about the nature of truth in mathematics and our ability to apprehend it, to get our hands on it. The answer is, well, we can't get our hands on all of it. In fact, we can get our hands on very little of it. It's extremely profound. It's when mathematics sort of transcends itself and has something grandly philosophical to say.

And I was intrigued by that result. I was still at the Federal Reserve Bank I think when it happened, when he wrote that article. I said to myself, "You know what? If I go back to graduate school, I'm going to learn about one of these great, great things, you know, these mysterious things. I'm going to learn Gödel incompleteness or I'm going to learn about black holes or I'm going to learn about many-worlds in quantum mechanics." Things like that, these bizarre… Or relativity, right? "I'm going to learn about one of these for real, not just as cocktail party discussion. I'm going to learn what it's really doing." I later did that, and it had a profound effect on my life.

HW: Did you have any mentors when you started higher education?

LA: Well, what happened was when Martin Gardner did that "Game of Life" thing and I had found out the mysterious destiny of the R-pentomino, I became interested in the cellular automata. There was a woman who worked at the Federal Reserve Bank who had done some graduate work in mathematics. So I was thinking about these cellular automata and I produced a sort of mathematical result, and she helped me write it up. She said, "Well, this is how you say this is mathematics language." That was the first paper I ever produced. I submitted it to a conference, I think it was FOCS or STOC. Very early. And it got rejected out of hand. You know? But now I was a little bit interested in this stuff and she was friends with Lenore Blum, a mathematician, who was married to Manuel Blum. She said, "Well, maybe what

you should do is go to graduate school at Berkeley and work with Manuel Blum." And just like that Shakespeare teacher – "Go to Berkeley," "Okay" – she said… and I said, "Okay," and that's what I did too. So Martin Gardner had a profound effect and later on he was to have a third profound effect on me.

HW: Yes, we'll get to that. Do you recall any textbooks that might have been important to you when you were in university?

LA: Ooh! Boy, do I ever. Okay. The textbook is a book on theory of computation or automata or something, an early theoretical computer science textbook by I think it was Aho and Ullman.

But here's the story of that. And this doesn't tell short. This story doesn't short, but I'll try to keep it as short as I can.

So I'm struggling. I got my bachelor's degree. I'm thinking, "What am I going to do with my life?" I had tried out chemistry and I was thinking about maybe math, but I said, "Well, I never really tried physics," and after all they had relativity and black holes and all sorts of cool stuff, "so what I'll do is I'll go to Cal State University San Francisco," then called San Francisco State, "and I'll try out physics. Ah." So I did that. I went and signed up for like four or five classes in physics while I'm still working at the Federal Reserve Bank. I sign up for them all and I start taking physics.

Like four or five weeks go by and one day I find myself in this lab and I'm shining light through lenses and I'm measuring where the light falls, and I'm supposed to be rediscovering the refraction laws or whatever it was. I'm sitting there doing that and I stop and I say, "I hate this. I'm not going to spend my life doing this." Now I was naïve because I was seeing just one part of the elephant. Right? There's magnificent parts of physics, but that was what I thought physics was. I said, "I'm out. I'm done with this," and I left. Didn't withdraw from the university, didn't do anything. Just said, "I'm not going anymore."

Then when I reflect more on this stuff about the Game of Life and this interest in Gödel and everything is around, I say, "You know, I think I'll try, as Linda said, to go back to Berkeley and work with Manuel Blum." I decide I'm going to do that, but then I think, "Wow, Berkeley is a state school and San Francisco State is a state school, and I withdrew from all these classes without telling anybody. I probably got four or five F's sitting there." So I thought, "That could harm me. That could keep me out of Berkeley." So I went back to Berkeley [he really means San Francisco State] and I went into the library and I checked out Aho and Ullman, and I stole it. I checked it out with the intent of never returning it, and I never did. I did that because I knew the following. I knew that since when people leave a university there's no conceivable way that they're missing books from the library, their library fines and all these things will ever get paid. There's no leverage

except one. The leverage is they won't release your transcripts. And since my transcripts were four or five F's, that suited me fine, right?

So I stole that book on purpose, but there's a little sort of addendum to this story which I think is kind of charming. But I was troubled by this. I felt guilty for years because I'd stolen this book. I didn't like stealing and I wasn't comfortable. So one day like 20 years later, Gina Kolata, who's a writer for *The New York Times*, is interviewing me and this story comes up about my stealing a book on purpose to keep the transcripts… I discuss it a little informally with her and I said I felt guilty ever since. She said, "Well, why don't you just send them some money to take care of it?" I said, "I've thought of that many times. By god, I'm going to do it."

So I sit down and I write a check for I think a hundred or two hundred dollars and I mail it to the library at San Francisco State. And in those days, checks had all sorts of personal information on them, including phone numbers and things. So some days later, I get a call and it's a representative of the library and she says, "We want to thank you for the generous donation. Is there any particular type of book that you would like to get with this gift?" I said, "Well, yeah. Math books and computer science books would be appropriate. I'd like that." And I should have known, if you just send people a couple of hundred dollars out of the blue, they're likely to want to talk to you more. She said, "Well, why did you send this to us in the first place?" I said, "Well, it's really a strange story, but if you want to know it, by coincidence, there's an article in *The New York Times*" – I think it was the very day she called – "that will explain why I took a book once."

So she thanked me and then later, maybe a couple weeks later, I get a letter from the head of the library at San Francisco State College. And he thanks me for the gift and he explains that he had read *The New York Times* article, and though he had no aspirations to religious life, he hereby absolved me of guilt. I still have the letter. So that's the most important book in my life.

HW: I see. Tell me about your current family, your children, spouse.

LA: I got three children – Jenny, Lindsey, and Stephanie. Jenny is currently working at Harvard, Lindsey works at LinkedIn, and Stephanie lives with me. They're the most important thing in my life. Just that's all I can say about it and wonderful. Beyond that, with women, I've been married twice, divorced twice. I've had maybe three long-term relationships. Women have been great. They were all wonderful women and, yeah, a big part of my life.

Now my personal life beyond that? Yeah. Well, I spend a lot of time doing research still, but I also spend a lot of time with friends. I also exercise quite a lot. I work out maybe four or five times a week. I find that very beneficial for a variety of reasons, not the least of which is psychological. So I work out. I take boxing lessons. I've been doing it for maybe 10-plus years. That's really a wonderful part of my life because I take boxing lessons with a trainer. His name is Shadeed

Suluki. He has trained many world champions, including heavyweight world champions, and he's nice – he's my friend now – nice enough to train me while he's training these champions.

So I get to hang around with these incredible athletes – right? – that all of whom could kill me in a matter of seconds. But they're wonderful people. So I have these two groups of people. My young students, PhD students which I still have or previous students which I do research with, and I get to see them develop intellectually, but also I like to keep track of their lives and give them whatever wisdom I might have. But then there's these young guys who are boxers, and I get to know them and it's much the same process. Though I can't teach them, Shadeed does. So that's been wonderful for me.

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

LA: Let's see. I read. I listen to music. I watch sports on television. I'm not much of an outgoing person. I don't go to plays and the like. Yeah. But those are pretty much the things I do.

HW: Then just one final question in this section. Have you ever changed careers or shift from one major area to another? And if so, why?

LA: Yeah, I've done that several times. I've done it I think for a variety of reasons. I certainly started out as a number theorist, and an algorithmic number theorist in particular. But I shifted at one point into a biological sort of thing. This happened when I was probably in my forties, mid-forties. I guess I thought at that time that these talents that mathematicians have… I mean we're really good at some things. I mean we are the world champions in concentration. Everybody can concentrate, but I can concentrate on the same problem 16 hours a day, when I'm not eating or have other obligations, for years in a row, and I'll be so concentrated that I could be startled by somebody saying my name and stuff. We're good at that. And I thought, "Maybe these are talents that I could apply in other areas."

When I started thinking this, HIV was a big thing. So I started to investigate HIV. I found it really interesting because it taught me something about mathematicians. We're so good at what we do in rigorous, logical thinking and intensity that it hardly matters what we are thinking about, those skills still will serve us well. So I found that if I just got a medical dictionary to understand the words that researchers in biology were using, I could read their literature immediately and think about it, and I could think about it in the way mathematicians think about it. So it led me to a theory of the pathogenesis of HIV, how it becomes… causes us damage. The HIV world never really nurtured my theory. I tried very hard to get them to do it and did some experiments in animals and things as a collaborator to try to get my theory… I still believe in my theory. I think I'm right. But it was a big disappointment in my life when I did that.

But it led to something different. You know, the journey starts in one direction but it ends up someplace else. What happened was in order to be able to speak better and to be heard by the HIV paradigm-setters, I thought it would be good if I learned molecular biology and virology. So one time I went into… I asked a USC-associated molecular biologist and virologist if I could spend a summer in his lab. So I went into his lab and biology was not what I expected it to be. I expected it to be things that smelled bad in refrigerators, and what happened was it was all about A, T, C, and G. You know, "Geez, words over a four-letter alphabet. I got it." You know? So I looked at it that way. Since I was looking at it one way, they were looking at it very differently, so I started doing experiments which were really mathematically based with the tools of molecular biology. There were a couple of experiments, but one of them in particular was I realized one day that…

Well, maybe we should take a break before I go into this, if that works for you.

[A short break was taken]

LA: Now with regard to the DNA thing, I'm in this laboratory and everybody's viewing what's going on from a biological standpoint, the way they learned to view it, and successfully. But I didn't see it that way at all. I saw the cell as doing computations based on these words over a four-letter alphabet. My goal was to learn some molecular biology and I'm reading a well-known book, the… I think it's… Well, it doesn't matter. I'm reading a book one day and there's this wondrous little molecule. It's a protein. It's called polymerase. I'm reading about it and what polymerase does is it jumps onto a strand of DNA and it's like a juggler on a tightrope. It walks down the strand and it reads the A, T, Cs, and Gs. And as it's walked forward onto the next letter, it reads it and it reaches out into the solution around itself and grabs a corresponding letter and then attaches that to a growing strand of DNA that it's building. Then it takes another step forward, grabs another molecule based on what it's standing on, adds it. By this mechanism, this little protein, that's how DNA reproduces. It's sort of the centerpiece of life because if polymerase didn't reproduce DNA, then cells wouldn't reproduce and we wouldn't reproduce. It's where life happens. It's about 2 nanometers in every direction and it does this incredible stuff.

But from my point of view, here was this string of letters, the DNA, and this little machine that was walking along it making new strings of letters. Well, to anybody who grew up with my intellectual background, it was a Turing machine. That's what Turing machines were. That's what Turing… That's what the first conceptual real computers were. So I remember I sat up in bed, because I was reading it in bed, and I said to my wife, I said, "These things can compute." At that moment, I knew that they could compute. So I said, "Well, why don't I run an experiment during the summer where I'll get them to compute something?" So I designed an experiment. It didn't work just like a Turing machine, but I knew that the tools of molecular biology would make… these tools would give me

universality in the sense of Turing. I could compute whatever I wanted with DNA and these proteins. You know, I could balance a checkbook or fly to Mars, but I chose to do something called the Hamiltonian path problem.

So I sat in the lab and I did this experiment with the tools of molecular biology. Basically, in a drop of water, a computation took place, and it took place by interacting molecules. Those were the operations. I did the experiment and I did all the work and I got the answer. I mean, that is it worked. I did find the Hamiltonian path.

It was a small example. But I said, "Well, I'll write it up as a paper. Where should I submit it?" Well, I didn't know anything about the biological world, where you submit these things, so the only thing I knew that would accept papers like this was *Science*. So I sent it off to *Science* and I didn't know… reject it, whatever. It turned out that the reviews came back with words like… just superlatives. I said, "Wow! That's surprising." It became a paper and people liked it, and it launched a field called DNA computing.

That field's still alive and thriving. Two of the students I worked with were attracted to this field. Paul Rothemund and Erik Winfree now are at Caltech and they do this, and they both won MacArthur awards, and they're wonderful and brilliant at it. It's sort of where computer science meets biology. Ideally it gives us a new way of looking at biology and computation.

HW: That's a nice segue into your accomplishments, which is the next part of my selection of questions here. Let me begin with can you describe the computing field? What was it like when you first entered it?

LA: When I first entered it, it was like 1972 or something. We were sort of not widely accepted by mathematicians. Mathematicians who were proving theorems and like viewed us as not doing very good stuff. In fairness to them, I think they were largely right. You don't get accepted into a discipline that's been around for 2,000 years or more – in fact more – just because you played with some numbers or you did a little something here or there, a bunch of ad hoc results. There was no theory there, there was no profound thing there. So when I entered the field, there was sort of a curse or a blessing. One is we were not accepted by our peers. The other thing was we were a hot topic. There were actually positions available in the world. You could get a job, which unlike the mathematicians who couldn't, right? So when I entered the field, it was a blessing because I could get a nice job, but it was also the perfect time to enter the field.

As you know, Hugh, because we worked in the same area, what happened was… And this is true of many disciplines. They burn brightly for a little while at some point in history, and then they don't burn as brightly and they're kept alive by a sort of priesthood or cadre of individuals who keep the ember burning from generation to generation. Then they flare up occasionally, and then they are embers again.

That was true of algorithmic number theory and it was in the ember state. Probably when Gauss was doing it, just because Gauss was doing it, it was in the flare-up state. But there was a new wind blowing that would fan those fires and that new wind was complexity theory.

So there were things going on. Out of Gauss and people who worked on it, there had been this lineage of algorithmic number theory which had passed through the Lehmers, Derrick Lehmer Sr. and Derrick Lehmer Jr., and they had developed all these incredibly good ideas for dealing with numbers and algorithms on numbers. And Derrick Lehmer Jr. was at Berkeley at the time.

At the same time, there was a second trend that really goes back to Gödel and Turing and the like. That was that we could look at sets of numbers and wonder about a new feature they may or may not have, and that was decidability. We could start to wonder whether a computer could know enough about this set of numbers to tell what was in it and what wasn't it. So we can write computer programs that will tell us of a number, if it's even or odd, and we can write ones that can tell us whether it's prime or not prime. And the logicians taught us there are some sets of numbers where no computer program can do it. Those are undecidable.

What had happened is that field, which is very important, had developed, and it had developed sort of along two lines. One line was to get more and more precise, learn the tools to become more and more precise about which problems were on the decidable side and which were on the undecidable side. A particularly rich thread of that was Hilbert's tenth problem. That had just gotten solved when I went back to graduate student by Yuri Matiyasevich. He had built on the work of Julia Robinson and Martin Davis and others, and Julia was also a professor at Berkeley. Julia was wonderful to me and my graduate student colleagues. She would call Matiyasevich, well, late at night her time to transmit our questions and get answers about Matiyasevich's work and tell us.

Then at the same time, real computers got invented, and so people started to care not just whether a set of numbers was decidable or not, whether a computer could know which numbers were in and which numbers were out, but whether they could do it fast. And "fast" became theoretically polynomial time, or "not fast" became not polynomial time. The great people in that field included Manuel Blum, my advisor and an incredibly inventive, wonderful person, who had started to make a theoretical basis for this. And Dick Karp was also at Berkeley, who was starting to put together… These guys were putting together a theory, not just a bunch of ad hoc results, a theory of theoretical computer science.

So I was blessed by having all these three threads come at once. Then one of Manuel Blum's other students was Gary Miller. He was the first one to really pick up this thread and start to bring these two separate developments, the number theoretic and the sort of computational, together. He produced this result on primality testing, which was a wonderful breakthrough result. So I was following

his lead and I became interested in number theory, and I became enamored with number theory and I began to love number theory and I started reading number theory, etc. So that became the direction I took. The wonderful thing about that was that the people in algorithmic number theory didn't have this guidance that polynomial time… "Stay away from subroutines that require non-polynomial time." Didn't have that. But it was gifted to me, so I could go to the Lehmer school and guys like you who had this vast warehouse of great ideas, and I could just sort of piece them together and get great stuff, right?

So it was working great for me. And that together with the fact that people wanted computer scientists all of a sudden. Because there were computers at universities, there were positions and it meant that when I graduated, I could get a position at MIT. So lucky.

HW: What was your first job?

LA: My very first job?

HW: Yeah.

LA: I think the first one I remember… Oh, it was paperboy.

HW: Oh. Oh no. I mean within the context of…

LA: Academic?

HW: …the academy, yes.

LA: Oh yeah. Well, it was getting to be a professor at MIT in mathematics. Which is like, "Wow! What a great first job." So that was my first job, yeah.

HW: What was your first computer?

LA: Ah. Yeah, my first computer. Now this is another interesting…

HW: You always remember your first.

LA: Yes. Very good. But I have a first computer that's… Well, let me just tell the story.

When I was at the Federal Reserve Bank, there were a bunch of very brilliant people there. One of them was a guy named Efrem Lipkin. Efrem was never quite sure whether he was an anarchist or a communist. I asked him one day, "Well, how do you reconcile your political beliefs with working at the Federal Reserve Bank? You know, the Federal Reserve Bank." He said, oh, he didn't have a problem with that because he never planned to finish any project. There would never be a

deliverable. So he and I used to use that big computer for all sorts of things – trying to make music and all sorts of things. But he was a real visionary and he lived in Berkeley. And we would dream as we were using the Federal Reserve computer of actually having a computer of our own. And Efrem to a large extent did it because he was a part of a group of people and he had set up… They had gotten their hands on a big computer, not a personal computer, but that they owned. And they set up the first sort of network where people on Telegraph Avenue in Berkeley could type in "Hey, man. Need a ride to L.A.," and there was another one at like Tower Records. That computer would hook them up. This was really early, early putting together a network. I mean this was really far-out stuff and he was really doing it, he and his friends.

So one day I go over to Efrem's house and sitting on a desk is this thing that's about the size of a modern amplifier or FM thing, maybe they're smaller now, and it's got a row of lights on it. And those lights are blinking, and they're blinking in a way… I walk up to it and I say, "Well, it's clear this thing, these lights are counting in binary." I said, "Efrem, what is this thing?" and he says, "Len, it's a computer." And computers were these big things at the Federal Reserve Banks with special air conditioning, wiring running all around, spinning tape. "It's a computer." I said, "What?!" Turns out it was a computer and it was *the* first personal computer. That is not an example of the first personal computer. It was *the* first individual personal computer. What had happened is this guy who was part of Efrem's network who lived in Texas had started to develop a kit called the Altair and he had built himself a prototype. Being a good guy and "Don't sell the kit unless you put it together yourself," he had made a prototype and he had sent it to Efrem and his buddies in Berkeley, and that thing sitting on that desk was his prototype. And that thing, later he and his buddies took it to show all their buddies at a big meeting this computer. None of them had ever seen such a thing. I had never seen such a thing. Then that group decided they would meet regularly and they called themselves the Homebrew Computer Club. That's when Jobs and Wozniak first saw a computer as well. It was that one. Wish I had that computer, huh?

So that was my first experience with a personal computer. The first one I actually owned was some kind of early Apple thing. Very early Apple.

HW: You've talked about this a little bit, but if you want to say a bit more about it, the projects that you did work on in the early part of your career?

LA: Projects I worked on in the early part of my career. You mean…

HW: What sort of things were you…?

LA: Oh, well…

HW: You mentioned some already.

LA: Okay. Well, in my early career, I was really in love with logic computer science and in particular number theory. Like many mathematicians, when I was young, Gauss was my hero. So I was dedicated to this stuff. So I was working on algorithmic number theory and in particular primality testing, because Gauss had said – and I'll only be able to paraphrase him – "The problem of distinguishing prime numbers from composite numbers and factoring the latter is so famous and celebrated that it would be a waste of time to describe it here, and the dignity of science requires a solution." Now this is written in 1801 in *Disquisitiones Arithmeticae* by the guy who was arguably and I think most people would choose as the greatest mathematician who ever lived. And he'd written "the dignity of science requires a solution to this." Well, that lit me up.

By the way, there's a footnote, because you, Hugh, I think probably have read at least parts of *Disquisitiones*, right? There's a footnote there wherein he says… Oh, he goes on, having described how important this problem is, to then give what he considers a solution. "Lovers of arithmetic" – the word for number theory at the time – "will find these following algorithms wonderful." And indeed they are wonderful, but they don't run in polynomial time. But he has a footnote there, and in that footnote he says, "The reader should be aware that as the numbers get bigger, these computations become more prolix." In that one statement in 1801, he's saying that an algorithm has a complexity function associated with it that's a function of the size of the input. The bigger the number, the more time it takes. I've often thought that if Gauss had a spare weekend sometime and could have paid a little more attention to that, he could have launched computer science and complexity theory 150 years before it did get launched. The guy was off the charts.

HW: Oh yes. The citation for your A.M. Turing Award is the following: "Together with Ronald Rivest and Adi Shamir, for their ingenious contribution to making public-key cryptography useful in practice." In fact, this investigation led to the establishment… This is what I'm saying now. That was the citation. It's quite short. In fact, this investigation led to the establishment of the RSA cryptosystem – and I'll read another quote here – "the most widely used encryption method, with applications throughout the Internet to secure on-line transactions." What is public-key cryptography and why is it so important?

LA: This goes back to Diffie and Hellman and sort of the history of cryptography. So cryptography, secret codes, have been around for thousands of years and they've been very important in world events because people often want to send messages where they fear an enemy will get their hands on the message. So they encrypt it, they scramble it, and it's decrypted on the other end. This has been used for thousands of years and often failed miserably during many periods of time and led to great disasters and failures of nations and of rulers and all sorts of things. It's been an important thing in the history of the world.

But Diffie and Hellman in like ’76-77 were thinking about this, and sort of like Efrem Lipkin, they were thinking about the future of the world and what computers and networks were going to mean to the world. They foresaw a day when all sorts of Internet commerce and medical records and everything would be flying through the air at the speed of light all over the world and all this stuff was going to go on. They said, “That’s going to create security problems, privacy problems.” And one way to try to keep things private was cryptography.

So they investigated cryptography, but they realized the Internet was not like historical uses of cryptography. In the historical use, you had a general and his lieutenants and they met at headquarters and they shared a key. Then when they were dispersed in the field, that key was used as a key to encrypt and decrypt the secret messages that would be transmitted. But they said, “Once this big thing” – which we of course now call the Internet – “happens, people are going to communicate with other people that they didn’t know one minute before. They didn’t share a key at headquarters, because they’re halfway around the world from one another and they never knew each other existed until just now, but they have to send important private information” – classically credit card information, for example. They said, “We can’t do it that old way where they share a key, because they don’t. Can we do it without them sharing a key so that we can transmit the secret information and someone listening on the line won’t be able to read it?”

Well, it seemed impossible to do such a thing. In fact, at that time, the mathematical foundation for cryptography had become information theory. And information theory, due to Shannon, actually you could prove you can’t do such a thing. But they said, “Well, there’s this new stuff about called computational complexity and there’s this P and NP and all these things. Maybe we can exploit that and make a new foundation for cryptography where you won’t share a key and you can still communicate in private.” Very visionary stuff. So they produced a paper on it and that’s how public-key cryptography was born and which is used invisibly to most users all the time anything’s… billions of times a day, I think.

HW: Can you tell us a bit about the work on RSA?

LA: Yeah.

HW: What inspired it? What the individual contributions were.

LA: Well, what inspired it was… Yeah, I’ll just tell the story of RSA and my part in it. So Diffie and Hellman did indeed produce their paper and they were Stanford researchers. And Ron Rivest got a copy of the paper. It could have been… It was before publication I suspect. A manuscript. And Ron, Adi Shamir, and I were all young professors at MIT and we were friends and we used to do everything together. You know, we’d go on trips together, we’d have dinners together, we did everything together, and we were constantly collaborating on our common

discipline, which was computational complexity theory. We saw each other every day.

I remember the following story. Ron I think remembers all this differently, but Ron will be sitting here sometime and maybe you'll be opposite him, Hugh, and you can correct his mistakes on this history.

Okay. What happened was I remember walking in Ron's office and he says, "Len, did you see this new thing from these guys Diffie and Hellman at Stanford. It's all about this, you send this and you scramble that, then out the other end…" I said… And to my ears, I'm trying to save the dignity of science because Gauss told me to do it. And this isn't going to save the dignity of science. So I hear this as some kind of engineering thing about networks and stuff like that. I remember interrupting him and basically saying, "Well, that's nice, Ron, but let's talk about blah-blah-blah." So it meant nothing to me.

Ron did enlist Adi who was interested in it, Adi Shamir, and together they start working on this. But I'm always around these guys and they become obsessed. They're constantly talking about it and they're constantly coming up with possible public-key cryptosystems. See, Diffie and Hellman had said, "This is how you could do it," but they couldn't make an actual incarnation, but they spelled out what you needed to make an incarnation. Rivest and Shamir are trying to make an incarnation and they have numerous theories. Some of them come from graph theory and a variety of places. All sorts of things, combinatorics. They're going to create this public-key cryptosystem. It turns out it's not such an easy thing to get it all to fit together right. So they make these systems and they break them themselves, and I just have to endure their talking about this stuff.

But for reasons we only understand now and we didn't understand then, all these systems are failing and they start to move towards number-theoretic stuff. Number-theoretic algorithms in particular. Of course, nobody cares about algorithmic number theory, as you and I both know, at that time. But there's like – what? – six guys in the world who care, and I happen to be one of them. So I know this, I mean as well as anybody knows it. So when they start to move into number-theoretic kind of approaches to getting a public-key cryptosystem, they're producing them every day and I go in and I look at them and say, "No, I can break that. This, this, this. Boom, done." Mostly it goes that way, and it goes that way for months. Occasionally they produce a really pretty clever system and occasionally… in one instance they produced one so clever that I couldn't see how to break it and I had to go home and really do some research to figure out how to break it, but it was breakable.

Then there's the night of Passover, I think '77, 1977, and one of our students, Anni Bruce, has a Seder party and things for Passover and she invites us all, and Ron and Adi and I and lots of other people are there. And at Passover, very often there is

Manischewitz wine. I didn't drink because I couldn't drink, but Ron had no problem with it, so he drank a lot I think of Manischewitz wine. So the party breaks up around 11 say and we all depart. It was a nice evening. I go back to my house, Ron to his house, and I receive a call at like midnight or maybe one o'clock or two o'clock, and it's Ron. Ron says, "Hey, Len. What about blah-blah-blah?" And the "blah-blah-blah" he said was what we now know as the RSA cryptosystem. Upon hearing it, I said, "Congratulations, Ron. I think you finally did it," because it looked solid to me. This one, wow, I wouldn't know where to begin to break this. Well, I know where to begin, but I couldn't succeed. So I said, "Congratulations, Ron."

So hang up – Ron I think does not remember this call, but at any rate – and I go into MIT I think it's the very next day and Ron has apparently stayed up all night and handwritten a paper. And I go. I run into Ron. He hands me the paper. I look at it briefly and I say, "Oh, it's what you called me about last night, this public-key cryptosystem thing," and the authors on that paper are the default order, "Adleman, Rivest, Shamir." And in one of those quirks of fate, and this stuff happens in life, I say to him, "Take my name off that paper." He says, "Why?" I said, "You thought of the idea." And he says, "No, no. We worked as a team. This is a team. You deserve to be on this paper." We proceed to have an argument about my getting off the paper and he's arguing to keep me on it. So we agree that we'll just think about it for a while. I go home and I think… My first question was sort of moral-ethical – "Do I deserve to be on this paper? Am I going to be comfortable with myself if I'm on this paper?" And I reflect on that evening or two that I spent trying to break one of those cryptosystems that they came up with, and I say, "Well, that was real research. The rest was just casual observation, but that was real research." By the way, that system was discovered later by other researchers, published, but was born dead because it was already broken. So I said, "Yeah, I guess I'm comfortable that I did contribute something." I also said to myself, "Well, no one's ever going to read this paper, but it will be another line on my résumé when tenure time comes. So okay." I go back into Ron and I say, "I'll tell you what. Let's compromise. I'll become last author and you'll be first," and that's how it became "RSA" rather than "ARS."

That's the story of how RSA got born. It still meant nothing to me, but it was soon to mean a lot to me.

HW: In view of Adi's reluctance to grant interviews…

LA: Oh, is he really…?

HW: He is reluctant. He doesn't grant interviews.

LA: Ah, I didn't know that.

HW: So can you tell us what he was like to work with…

LA: Yeah! Adi?

HW: …and how closely the three of you collaborated?

LA: Yeah, we collaborated *really* closely. I mean we'd be doing research in gondolas at ski places in Vermont, because we were *always* together.

But our collaboration mostly was around this public key stuff because, first of all, they were intensely interested in it and, second of all, then it became a big thing and so we thought about a lot of subsequent problems that arose in that area together. Working with them was absolutely great. Working with special people like that is a joy. I mean Adi is like… He's just like a lion. You put a problem in front of him, he'll devour it. He's just really, really, really smart. And Ron is one of these guys who, if Ron decides that he's going to become a rocket designer tomorrow, in five years he's going to be one of the best rocket designers in the world. He can just do anything.

So yeah, it was wonderful because we were first of all friends. What greater joy than to sit around with your friends and try to solve problems? It was wonderful.

HW: The agency that considered itself the guardian of secrecy during this time was the National Security Agency. You must have run afoul of them.

LA: We did run afoul of them. I was still in a mode where I didn't understand that there had been this whole history of cryptography. I didn't understand… What I understood is "It's still ain't going to take care of the dignity of science."

Then one day I'm in a bookstore in Berkeley… Oh! And Martin Gardner arises again. So Ron and Martin somehow got together and it was a wonderful topic for a Martin Gardner article and he wrote it. He said that anybody who was interested in getting a copy of the manuscript could send a self-addressed envelope to us. And I'm in a bookstore one day and I'm about to buy my book, and the guy in front of me has *Scientific American*. He gets up to the cashier in front of me and he says, "Did you see this neat article on cryptography?" and the cashier says, "Yeah, is that cool or what?" So sort of in a burst of immodesty, I said, "Oh wow, that's stuff that I and my friends did." So the guy who's buying the Martin Gardner… I mean turns to the Martin Gardner page where the article is and he says, "Would you sign this for me?"

Now I'm sure everybody listening to this thinks that mathematicians are constantly accosted by autograph seekers and the like, right? I know you're accustomed to this. I certainly was.

No, it had never happened in my life and I never even conceived that it ever would happen in my life. "Who? My autograph?" When that happened, I said, "What's going on here? Maybe there's a bigger context to this thing."

Then I get back to MIT and the room is filled with self-addressed stamped envelopes. I look at some of them and they come from bizarre places like the Bulgarian secret police or something like that. I'm going, "What's going on here?" because I still don't know. But I'm beginning to wake up. Then we hear from a representative or an employee of the NSA that we can't send out these manuscripts in their self-addressed envelopes because it's against the law. And I go, "Law? What law?" You know what I mean? "What is this?" It turns out that it was against the law for us to send out information say about atomic bombs or stuff like that, and among the things it was against the law is cryptographic stuff. So it was against the law.

It was at that moment that I found out there was this agency called the NSA, and no one knew about this agency. At that time, not even people in government knew about it. Only a small number of legislators and presumably executives knew about it. And when they talked about it, they jokingly I heard said… they called it "No Such Agency." But NSA did exist and it was charged with protecting our information from our enemies and breaking the codes of our enemies. Yeah, and that became a whole chapter that continues to this day with Snowden and everything else. It was quite exciting.

HW: So what happened with all of these requests for your manuscript?

LA: Ultimately the powers that be at MIT decided to send out the manuscripts, and the whole thing precipitated a sort of big debate that involved the president's press secretary and the like and all sorts of people. It broke into two camps – the academic freedom–privacy–security camp and the national security camp. Sound familiar? I mean it's going on today still, this very break. And it was very interesting.

Now at that time – this is not my view today – I naturally fell into the academic freedom–privacy–security camp. I was passionate about that. But I have a different view of the world now and I now think… I totally understand the NSA's point of view and I think they acted very admirably in the way they handled it, and it's now become what it probably should become. It's a line that is drawn by the political process and it can be shifted a little this way and a little that way from time to time. When there's more national security needs, less privacy, and when there's less national security needs, more privacy. That's going to shift, I expect, *ad infinitum*. But it's I think the way it should be. So I no longer passionately believe in my side and not the other. I think they're both just a line we have to live with.

But there was one episode which was particularly interesting, and that's that I used to write grants to the National Science Foundation, the leading supporter of pure

science in this country. That's where money for pure science comes from, and mathematics. And I used to write grants and it was sort of a ritual Kabuki dance that we would go through every three years. The dance would consist of I'd write down all of the wonderful things I was going to do in algorithmic number theory, and they were going to be so wonderful that the country would thank me and thank NSF, and that they could acquire this wonderful thing just by supporting my research. So I'd write 20 pages or so on what I was going to do, then I'd get a call from the NSF, "Well, we want to cut your budget on this and blah-blah-blah." I'd say, "Okay, done." And that had happened. I mean that just was routine.

Then in 1980 or thereabouts, I begin this process again and because crypto has taken off, I'm not foolish, I'm not going to fail to mention that this is going to have big, important implications for crypto and privacy and national sec-… you know, whatever. So go through the ritual dance and I get my call from NSF. They say, "Love your stuff, Len. We're going to fund it. Oh, by the way, the National Security Agency is going to fund that part involving cryptography." And we had been at loggerheads for several years, the academic freedom–privacy part versus the national security part. They had tried all sorts of things to put the public-key cryptography genie back in the bottle – legislative action, new crypto standards which we presume they could break. So this war had been going on. But when I heard that particular line, that the NSA was going to fund that part of my research that involved cryptography, I knew I'd won a battle.

So I hung up the phone and I called Gina Kolata again at *The New York Times* and I said, "Here's a story you might be interested in. The NSF, you know the leading sponsor of pure research in our country, and the NSA, you know that secret agency that does intelligence work, very important, and keeps our country safe, they seem to be collaborating now." And she did find that story interesting. Yes.

HW: I'll bet she did.

LA: Yes, she did. So I hang up with Gina and then my phone rings again. It's Bobby Inman, the head of the NSA, and he wants to explain that there's been a little misunderstanding. I said, "Thanks for the call, but I think this is probably something's that going to be worked out in the open as part of the political process. And, you know, thank you. Bye." So the article appeared in *The New York Times*, and that event I think sort of helped draw the lines between mathematics and science and the NSA. Those lines are not drawn clear-… I mean there's slides, but we've reached a point in time now where I'm very satisfied with where we are. NSA is important and protects this country and is vital to our interests. Security and privacy on the Internet and elsewhere are also important. And now the political process decides where we need to draw those lines, and I can't think of a better way things should be.

HW: What is the special property that RSA has that has made it so useful?

LA: One of the things it has is that it was first, so it got adopted. The other thing it has is it's the cleanest of all the systems I think. I always like purity and I like to know what foundation I'm basing actions or theorems on. Even though it's not perfect, with RSA it basically comes down to primality testing, which we know how to do fast, and factoring, which we don't know how to do fast. And it's pretty clear. You and I know that there's additional subtleties here, but it's pretty clear. So I can see the foundation clearly. I know what gamble we're making basically, that factoring's not going to be done in polynomial time, quantum computing aside. And other systems I think have not been given the scrutiny historically on the underlying foundation that RSA has. I mean Gauss tried to find a polynomial-time factoring algorithm. If Gauss couldn't find one, us mortals can't, right? So that's what I like about it, is purity. It's clear to me what's going on.

HW: The words "Squeamish Ossifrage" have a connection to RSA. Why?

LA: Yeah, they do. Oh, this is a good story. Ron won't like this either. Remember that Martin Gardner article and remember how Martin always used to like to give open problems? He wanted to give an encrypted version of some message where if the readers could find out what the message was, that would be the problem they were trying to solve. So Ron did that and the message itself that he encrypted was "Squeamish Ossifrage".

Now an interesting thing happened because Ron kind of messed it up. He did the calculation of how big the key needed to be to make sure that with the rate at which computers were being done and Moore's law and you do all the calculation, he wanted it to last for a billion years I think. And he did all that calculation. But he did it based on a square-root-of-*n* factoring algorithm. We knew better than that because we had inquired among all the factoring guys, including… What was the guy's name who started with S-C-H? He was a factoring guy.

HW: Oh, Schroeppel.

LA: No, not Sch-…

HW: Not Schroeppel?

LA: No.

HW: I thought it was Schroeppel.

LA: Oh. Right, Schroeppel. Yeah, maybe it was… What's Schroeppel's first name?

HW: Rich. Richard.

LA: Rich. Yeah, it was Richard Schroeppel. So we had written to Richard, because that was his specialty, "What's the fastest algorithm?" He had written back, "You can't

prove any of this stuff, but it's E to the square root of *n*, ballpark, what we know it to be." But Ron didn't use that, and if he had used that, he would have used a bigger key and it would have taken, ballpark, a billion years to break. But he used the wrong speed. Therefore it got broken like 10 years later, right? How long did it take Lenstra and…?

HW: 1994.

LA: '94 it got broken, so…

HW: So '77 to '94.

LA: Yeah, but that ain't a billion years.

HW: No.

LA: Another interesting thing about Schroeppel and that letter, which I have a copy of, Schroeppel had read our manuscript, we sent it to him, and Schroeppel had made some comments about how we might improve it. He said, "You're calling the person sending the information 'A' and you're calling the receiver 'B,' but they're really not mathematical symbols. They're not representing mathematical quantities. Maybe you should give them actual names, 'A' and 'B,' right?" And he said, "Call them 'Adolph' and 'Boris.' " And Ron vetoed that, but called them "Alice" and "Bob." That's why "Alice" and "Bob" are all over the place in cryptography. And you know what? It's even contaminated physics, because quantum mechanics guys I think now use "Alice" and "Bob." Okay? So yeah. But it should be "Adolph" and "Boris" due to Schroeppel.

HW: Okay. Of course it was already mentioned that RSA is broken once a quantum computer with enough qubits is constructed. What do you think of this possibility?

LA: Well, I ask all the young quantum guys this question. I've been asking ever since Shor's breakthrough paper in that regard. And you know what? Instead of becoming more and more pessimistic about actually building a quantum computer, they have through time become more and more optimistic. Everybody I talk to today says, "Yeah, it's going to happen. We're going to get actual quantum computers." There's some hedging about when it will happen and there's some hedging about whether we'll ever be able to build one big enough to actually factor a big number, because there's all sorts of error correction and you need a lot of quantum bits. But yes. It's just hearsay to me, but I think it is something. You know, all you kiddies out there in the future are going to have your quantum computers on your desks.

HW: What was your involvement in the setting up of RSA Data Security, Incorporated?

LA: When RSA first came out, everybody said, "Wow, you guys are going to be rich," and I said, "Okay." I wasn't sure how, but it was clear the world was responding. But we couldn't quite figure out how to get rich. So we talked to some companies about commercializing RSA, but we didn't know how to go about it. We weren't businessmen and we didn't have those skills.

So one day in my studio apartment in L.A. – I'd moved to L.A. since then – Ron, Adi, and I got together and it was sort of like Mickey Rooney, "Let's put on a show." We said, "Let's put on a company." We signed papers – we'd done a little footwork before then – and it created the RSA megacorp. We did it and we had to choose roles to play, because the Delaware documents required you filled in various… So Ron became the Chairman of the Board, I became CEO, and Adi became I guess Secretary or something. I don't know. Something, but it didn't matter.

Yeah. So that's when RSA was born. As CEO, I steered that ship right into the gutter. We had raised a little bit of money from a dentist to get us underway and we're written code and stuff, and I was too naïve. I didn't realize what business was all about. Make no mistake, you mathematicians out there, business is hard. Real hard. Business requires very special skills and has its very special challenges, and I was not good at those things. So I'd steered it about into the drink, then I resigned as CEO because there was this new CEO. But he didn't turn out to be very successful. Then it continued to go into the drink, and by now it's been alive, RSA, for a couple years.

Then Ron… Like I say, you set Ron to doing anything, if he decides to do it, he's going to do it super well. He decides to take his role as Chairman of the Board seriously. He takes over the company and he fires everybody but a guy named Jim Bidzos. And Jim has all those skills which I lacked to be a real CEO. You know, lurch forward. No matter what's going on, you just keep moving forward. Also he had the gift of gab. He could paint pictures for people. The work he did in building RSA into what it became, the company, is just astonishing. I sometimes say to him that we made similar contributions to RSA as CEO, Jim and I, except his had the right derivative.

Right? Yeah, so he took RSA from this company… He had to educate the whole country into using it. He had to defend these ideas against the NSA – you know, the whole Clipper chip episode. He was amazing.

And the first thing he did was he… Or I don't know if it was the first, but when he became CEO, he raised more money. And he called me and he said… or, well, he was going to raise more money, and he said, "Look, the company owes you a lot of money," because we never got paid for anything. You know, we were the company. He says, "I'd like to give you 10 cents on the dollar of what we owe you." I said, "Jim, why would I do that?" He says, "Well, here may be a reason. You're on the board of that company, and if this company goes down, the investors

in it might sue you." The last thing I wanted was to be sued and tied up in courts with lawyers and judges, so I said, "Ten cents sounds good." Then I resigned from the board, because I didn't want to get sued, and I had nothing to do with the company for many years while Jim built it into this incredible thing.

HW: Are you happy with what happened to RSA subsequent to your involvement?

LA: Yeah. Yeah. I mean on the business front, Jim had built this up, and every year RSA would have this conference, a crypto conference they'd put on. I'd gone to a few of the early ones and there were all the usual guys. The guy from Sandia and… You know them. It'd be the usual guys, a bunch of us wearing slippers and… "Us guys," right? And there'd be 30 of us.

Years went on, years went on. I didn't want to hear about RSA. Business was too hard for me. Then there was some anniversary at RSA and they said, "Len, will you come up for the RSA Conference? Because it's kind of a big deal." I said, "Okay, I'll go up." So I flew up to San Francisco and I went into the Fairmont hotel and I said, "Where's the RSA conference room?" and they said, "Well, it's ballroom blah-blah-blah." I go down there and I'm about to walk in and I expect it to be guys like you and me. The usual guys in their slippers and beards, right? I open the frickin' door and Jim is on the stage like a quarter of a mile away from me, and there's this big screen behind him showing Jim, and everywhere I look, there's thousands of people wearing suits and everything. And I say to myself, "I'm rich. Damn!" I was thunderstruck. Yeah, so it was really quite amazing.

So Jim took that company to be a huge thing. It spun off Verisign and all this, and it's a centerpiece of privacy and security on the Internet. I mean whatever there is of that stuff. So that's been a wonderful development.

Another wonderful development is what it did to number theory, algorithmic number theory, and more generally to the area of cryptography, which it helped create. Because it hooked number theory to something that people actually wanted and was commercial, it got funded and the like and it became this thriving thing. There's a lot of algorithmic number theorists in the world I think today. Many more than when you and I began. And the cryptography has become a major sub-area of computer science itself. The sun never sets on a crypto conference. If you look at the schedule of crypto conferences, there's one all the time somewhere in the world. It's just amazing. To see that grow out has been wonderful to watch. And of course it's been very nice for me in a variety of ways. So it's been wonderful.

And it's just been a great story to watch. I sometimes occasionally still go to the RSA Conference. I go there and I sit in the office. The last one I went to was like two years ago and there's somewhere between 30 and 50 thousand people there. It takes place in the Moscone Center, you know, in San Francisco. I sit there and I

just wonder at how these little things you do can sometimes snowball. So it's really fun for me to observe it.

But the best part is I get together with… We always have a dinner at the RSA Conference and I get together with Jim Bidzos, Rivest and Shamir, and Hellman and Diffie. For us, it's just sitting around and talking about our children and just going, "Look what happened." That's a joy.

HW: A remarkable thing to happen for a paper of which you wanted your name at the end.

LA: Yeah. Right. Which I thought no one would ever read.

HW: Of course the citation for the award is careful not to say that you discovered it.

LA: Hmm. What do you make of that? I don't know. The award talks about "practical," right?

HW: Yes. Yes, it does.

LA: For me… I didn't write the award. I'm very grateful to receive it. But it was never a practical endeavor for me. Well, it was briefly when I was CEO, but geez, I couldn't…

HW: Were they taking into account the fact that it had been discovered years earlier at GCHQ?

LA: Oh! Maybe so. I don't know the answer to that. Yeah, so okay. At GCHQ in England, which is their NSA, there were Clifford Cocks, a few other… Maybe you remember the names?

HW: Ellis.

LA: Ellis, yes. These guys, we hear… And I have no doubts it's true, because everything's classified so you never quite know. But yeah, they apparently had discovered the notion of public-key cryptography and had come up with RSA I think in like '75-76.

HW: About that. Maybe '74.

LA: Okay. Maybe '74.

HW: But a difference of about three or four years, hardly anything.

LA: Yeah. So those guys probably did it as well. And I admire them mostly for their service to their country, because they didn't receive the accolades that we got. It

was a sacrifice for them to serve their country, and I think that's extremely admirable.

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

LA: Oh, I don't remember it well enough. As I recall, I liked the book, and I certainly like what Steven Levy writes. But I'm sorry, I don't recall it well enough to comment on it.

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

LA: Well, how did my family…? I think they were very proud of me. My children were very proud of me. My, by then, ex-wife was probably pretty proud of me. But yeah, I know my children love me and want the best for me and have joy when I succeed, so that was very good. For me, it had many effects. And if you ask me this question every day, I'll give you different answers. But here's one thing it did that was important to me. And it was a process that began much earlier.

When I got an offer for a job at MIT to be a professor of mathematics, I told my father and he said, "Oh, that's wonderful, Len. Tell me all about it," and I told my dad. He said, "Before you accept the offer, Len, check with Bank of America again, because they have a great retirement fund, plan." I thanked my dad but I accepted the MIT offer anyway. But for my dad, he had been shaped like we all are by our early experiences, and he was a Depression-era guy. And MIT wasn't going to pay me anything. They considered it a privilege to be there and they were right, but no retirement plan for me. So anyway, but for me, it's interesting, it had a very different effect.

When I got this position at MIT, as a young boy once I'd got on the mathematics train, this is my goal, this is what I aspire to, to be a mathematics professor at a great university. I mean that was reaching for the stars. That was the gold medal for me. So I remember walking across campus and saying to myself, "You know what? Now I can be a shoemaker," because I had validated inside myself that I could achieve the things I wanted to achieve, I could achieve what I considered great things. Therefore I had the freedom, the right to do whatever it was I wanted to do. We don't get immortality. We can't figure out how to achieve that. But if you get lucky enough in life to be able to do the things *you* want to do, wow, that's great fortune, right? The Turing Award augmented that.

So when I got the Turing Award, it was not only that I could do the things I wanted to do, but it made it so that people would listen to me and they would provide me resources and they would provide me in some cases the most valuable resources, their intellects, to help me do the things I wanted to do. So just it gave me a bigger

megaphone to go viral with my ideas. Good or bad, people would listen. So I did the things I wanted to do. I would have done them anyway. But I got nurtured in doing them because of the Turing Award. It had that impact. And so it's just part of this blessing that I'm one of those people who got to do what I wanted to do. Wow, what more could you hope for?

So it was that. The Turing Award also… What else does it do? I don't know. For me internally, that's what it did. It gave me this open field, and I'm thankful for it all the time.

HW: Now I want to turn to your achievements subsequent to RSA. In particular, I would like to talk to you about your role in the development of the Adleman, Pomerance, and Rumely primality-testing algorithm. It's a very significant contribution to the area. Before APR, there was no consistent method of attack in proving a number prime. Instead there were a collection of ad hoc methods that were not always applicable in any given case. You produced a truly novel idea. How fast is this technique and what else would you like to say about it?

LA: Not fast enough is the short answer. So remember, Gauss had told me to work on this problem, and I dutifully worked on this problem. I mean I worked on it for *years*. A lot, a lot of time. And in a sort of "ah-ha" moment that occasionally we're lucky enough to experience, I saw something that maybe had never been seen before. I had hoped that this was the breakthrough that would lead to the polynomial-time algorithm and therefore save the dignity of science. But I wasn't a good enough number theorist, especially analytic number theory and some of the algebraic number theory that I didn't know at the time, to carry it out. But Pomerance and Rumely were good in those areas. So we collaborated and pieced together this algorithm, which I really like just because I like this algorithm. I mean I think there's a lot of good ideas in it. It turns out that it runs *almost* polynomial time. It is like so close, but it's not polynomial time.

So very pleased with that achievement. I like it very much. But the AKS algorithm has come along subsequently and they did indeed satisfy the dignity of science and they produced a deterministic polynomial-time algorithm for primality testing.

HW: Where was the APR paper published?

LA: It was published in *Annals of Mathematics*.

HW: Why is that significant?

LA: I'm not sure why it's significant, but I think it was the first time they ever published anything that was algorithmic in nature. Since it is one of the premier mathematical journals in the world, it sort of was a landmark in that…

HW: You finally got respect from the mathematicians.

LA: Oh, you think so? Maybe so, maybe so. There was other work on primality that I did with Ming-Deh Huang that I think…

HW: I'll get to that. I'll get to that.

LA: Oh, okay.

HW: Was the method "practical"?

LA: Was the method practic-…?

HW: The "practical" in quotes.

LA: Yeah. No, as I recall it wasn't. In fact, yeah, no, I don't think anybody's ever done it. You know, implemented it. But that wasn't my concern. It's just beautiful in the sense that we mathematicians have acquired this aesthetic over thousands of years that no one but us understands that lit up my "beauty" light.

HW: What happened in the study of primality testing after APR appeared?

LA: What happened was there were many people who worked on it more and more as I think the crypto thing invited people into the field. And you could go back to Gary Miller's stuff, which I mentioned earlier, and out of Gary Miller's stuff – he was aware of this by the way, but didn't bother to write it down – you could what was called a random polynomial-time algorithm for, well, primality. Later that was made explicit by Rabin and I think Solovay? No, Solovay and Strassen.

HW: Solovay and Strassen, yes.

LA: Then Rabin added some things to that. But that was really, really, really interesting because it brought randomness into the study of computation, and randomness plays this mysterious and wonderful role in computation. As long as you can provide a real source of randomness, whatever exactly that is, you can solve some problems on a computer faster than if you don't have a source of randomness. Now randomness is usually thought of as total garbage. I mean, right? It has no information in it. But you can't trick these machines and give it really good stuff in place of the randomness, like nice, organized sequence like "0101." You got to give it real randomness, then it runs fast and does the right thing. You give it phony randomness, it will fail. So it used to be "garbage in, garbage out." Now it's "garbage in, good stuff out; good stuff in, bad stuff out" with these algorithms. It's paradoxical, it's fascinating, and I don't think we've gotten to the bottom of it yet. And they brought that into the study of many things including primality. Then Goldwasser and…

HW: Kilian. Kilian?

LA: …Kilian, yeah, saw that they could use elliptic curves to give a really cool algorithm that… But they couldn't prove that it actually was a random polynomial-time algorithm for compositeness. A slight difference between a random polynomial-time algorithm for primality and one for compositeness. They couldn't prove that it was. But that stimulated Ming-Deh Huang and myself to try to find a variant of their algorithm which we could prove was random polynomial-time. That was sort of a… And we did. That was another good step in…

HW: That was a very deep paper.

LA: Yeah.

HW: And it also was not practical.

LA: No. Practical has been lower on my radar screen. But it was a very deep paper because it forced Ming and I to get into some deep algebraic geometry to start to exploit that.

Now simultaneously one of the great algorithmic number theorists probably of all time was Hendrik Lenstra, and Hendrik had also gotten into algorithmic geometry. In fact it was his ideas with René Schoof - ideas that sort of gave rise to the Goldwasser–Kilian paper. So we ended up using some pretty deep stuff in this paper that Ming and I had done, and we were invited to give a plenary lecture at the International Conference of Mathematics. And in the audience were the great algebraic-geometric number theorists. Deligne was there. Serre was there. Maybe Andrew Wiles was there, but I didn't know of him till later, where we all know of him. And perhaps that talk additionally added to the acceptance of theoretical computer science as a mathematical discipline worth considering.

HW: Well, you mentioned Lenstra. I guess he in a sense with Henri Cohen did make APR practical.

LA: Did they?

HW: Well, they produced this wonderful stuff on the use of the… Well, they were using various kinds of Jacobi sums, that sort of thing.

LA: Yeah, yeah, yeah.

HW: Yeah. And when they used that, actually it worked pretty well.

LA: Oh, okay. I probably knew this, but I'll appeal to age that I… Yeah.

HW: We can do that at our age, yes.

LA: Yes.

HW: You've talked about your work in primality testing. Did you ever make any contribution to the integer factoring problem?

LA: I made a contribution. There was this result. Who do we attribute it to? This L to L one-third….

HW: Oh, Pollard.

LA: Pollard! Yes.

HW: John Pollard.

LA: So Pollard comes out of nowhere with this new technique for factoring. Caught me totally by surprise. I remember hearing Hendrik Lenstra give a talk on Pollard's method, and even after hearing the talk, I asked Hendrik, I said, "I don't get it. Where's the magic? How does this work?" Why does it work better than anything we had ever tried in the past? And he explained that.

So Hendrik Lenstra and Pollard and I think Arjen Lenstra might have also been involved in this, maybe others, started to pursue Pollard's method and try to make it formal and prove that it had the properties we had good reason to expect it did. And I started doing the same thing. So at some point, I introduced… I don't know. What are they called? Singular numbers. Something. Anyway, and I think that that was a good way to look at a certain part of what they were doing. So I produced a paper on that and I think that the Lenstras and Pollard and those that were working on it produced a book maybe or…

HW: Yes, they did.

LA: And I think they adopted that particular approach to that particular thing. So yeah, I think that was sort of my contribution.

Curiously, I was inhibited in working on factoring by the existence of the RSA. And not because… Because I had agreed with my colleagues… And I took everything so seriously. I agreed with my colleagues that we shouldn't… What was it? For some economic, that we shouldn't try to work again-… I don't know. I don't know. I had some agreement that – it was really a commercial sort of agreement – because we had formed a company that I shouldn't work on… I took that seriously, and I regretted it because it was the natural problem for me to work on, but I didn't do it.

HW: Well, let's talk about how hard do you think the problem is?

LA: I think it's hard. I explored a lot of tools and a lot of methods and thought very hard about them in my life as an algorithmic number theorist, and sort of have a feeling like I know what's out there. Of course it's changing all the time. And while it was enough to prove a number prime or not prime, it just didn't look like the tools were there to make a great breakthrough, a polynomial-time breakthrough. On factoring, I just never could find the crack in the door for that, the little way to try to ease your way in. I never could and I eventually just came to believe that if it was going to happen, if there's a polynomial-time algorithm for it, deterministic polynomial time, then it's a hundred years away. You know, a lot more has to be done. And I suspect… Gauss couldn't do it. Maybe he had a good reason not to be able to do it. Maybe it can't be done. What do you think of that?

HW: I'm not allowed to say.

LA: Oh. Go on.

HW: Do you have any comments on the status of the problem today?

LA: Yeah. The status of the problem itself has not changed theoretically much since the time of Pollard's idea. There's been implementations that are probably better or worse than others, and computers get faster and like that. But I don't think much has changed in that regard. The big change that did happen was the advent of quantum computation, at least theoretically. That was sort of foreshadowed by Feynman and picked up by various guys like, in England… gee, he does a lot of many-worlds stuff. My bad.

HW: Penrose?

LA: Huh?

HW: No, no. It wasn't Penrose?

LA: No, no, no, no. Okay, my bad. I just apologize. And it was picked up by Vazirani and others, and they started to develop this theory of quantum mechanics as a means of computation. Then that went along for a while and then Peter Shor suddenly proved that on a quantum computer, you could factor in polynomial time, and that made the whole field extremely interesting. So if quantum computers come about, factoring may be doable in polynomial time in the real world, which is good enough because cryptography as a practical topic exists in the real world. RSA could go away. Right? Factoring could be settled. That's a threat on the horizon for those who use RSA.

HW: Let's turn to another area. You've worked on Fermat's last theorem. What result did you produce?

LA: So Manuel Blum is my advisor. Linda Kavner at Fed had said, "Go work with Manuel Blum." I said, "Okay," so I did that. Manuel was an incredibly great teacher and an incredibility brilliant and inventive guy. Working outside the box, he was a master at that. He'd come out with ideas that had nothing to do with anything that had preceded them. *Sui generis*.

So I was working on number theory and various other things when I was a graduate student. Because I was such a purist, I remember going into Manuel's office one day and I was saying, "You know, I think I'm going to work on Fermat's last theorem." Most advisors might give me a cautionary sort of "Well, maybe you should try something…" Right? Because Fermat's last theorem was open for 350 years and was the greatest, most famous open problem in all of mathematics, subsequently settled by Andrew Wiles in a great masterwork. But Manuel said, "Oh yeah, that's a good idea." So he gave me license to go work on Fermat's last theorem.

And I think it's very good advice. I'd like to give it to young researchers. "Don't sell yourself short. You don't know how well you can do. Maybe you can do great things, but you'll never find out if you only work on small things. So a certain amount of courage is warranted. And if you try for really hard things, you usually fail. But you learn tremendous amounts in the process and you'll be able to use those tools to prove lots of very worthy results. But just don't settle for less if you don't have to." Yeah. So Manuel sort of taught me that lesson and I seized on it.

So I started working on Fermat's last theorem and at one point produced a really nice result together with Heath-Brown and [Henryk] Iwaniec, and we produced something about the so-called first case of Fermat's last theorem, infinitely many primes. This was sort of the first time I guess you could argue that something had passed the finitely many cases boundary.

So I was very pleased with that result and we published that. That was nice. Of course, Andrew Wiles was to come along and just blow the whole thing out of the water, and just brilliant stuff. So my paper with my colleagues, or two papers actually, is fairly meaningless at this time. But Wiles' result had a lot to do with my sort of considering other things than number theory mathematically, because I realized I had bet on the wrong horse. I had bet on algebraic number theory à la Kummer and stuff, and Wiles had made it clear that it was algebraic geometry. I looked at that and I said, "You know what? I figure it will take me six years of hard study before I can learn those tools adequately to use them, to wield them," and I said, "No, I'm not willing to do it." So yeah.

HW: It's not well known, but you are the prime mover in the establishment in 1994 of the biannual Algorithmic Number Theory Symposium, better known as ANTS. This meeting has become a major conference in algorithmic number theory and has been held all over the world. Can you tell us something about how and why you got involved in this project?

LA: Yeah. It was sometime in the… What year was the first one?

HW: 1994.

LA: '94. Oh. Well, I had always avoided getting the Internet and this thing called email because I wanted to sit in a room and think about these problems. But finally I decided to get them. People were complaining they couldn't reach me, blah-blah-blah, and I thought, "Well, maybe that's not so bad," but anyway. So I got the Internet and I got email, and I went overboard. I start communicating with my colleagues and it's really exciting. Then I think, "Maybe we should all get together and have a conference about our passion for algorithmic number theory." And Ming-Deh Huang is my colleague at USC, so I enlisted his aid. So things get out of hand and this idea of a conference really starts rolling. Now I become engaged in something much like when I was running a company. It's not easy to put on conferences and find a location for them and get them funded and stuff.

But we did that and there was a guy at Cornell. Again, I can't pull up his name right away. He offered to host it there and did a lot of the work for the conference. And his wife was an artist. I wanted this conference to have a catchy sort of acronym, so I chose "Algorithmic Number Theory" – "ANTS" – "Symposium" or something. "ANTS." And his wife was an artist and I asked if she would draw a nice ant that we could put on the things associated with the conference. So that's why there's little ants on the Springer-Verlag thing, announcements of it.

It was just exactly at the time when Peter Shor's quantum factoring algorithm came out, and Peter I don't think had given a talk on it. So I got a hold of Peter and I said, "Would you please come to this first ANTS conference and speak about this new factoring algorithm? Because it will be intensely interesting to this audience." So we held the conference in Cornell. I think it was a great success. Peter came and gave the first public talk I think on quantum and factoring.

And that launched the discipline. So people set it up as a "every two years we'd have this in various parts of the world." As I understand, it's thriving now and it's the central thing that people in algorithmic number theory want to attend. So it's great.

HW: It's also the venue in which they award the Selfridge Prize.

LA: I don't know about the Selfridge…

HW: Yeah, the Selfridge Prize.

LA: I know Selfridge but I don't know there's a prize.

HW: They put a prize….

LA: Excellent.

HW: It's something about the Number Theory Foundation sort of decided to put a prize together for computational number theorists.

LA: Excellent. Great. Who's won it recently?

HW: I do not remember who won it most recently. I wasn't at the most recent meeting. They're given away at the meeting.

LA: Okay. Pleased to hear it.

HW: Oh yes. Oh. As I recall, you contracted a lengthy illness somewhat after the first ANTS meeting. Can you tell us something about that? Because I think I saw you in a wheelchair at one point.

LA: Yeah. Look, life's a struggle. It is for all of us. There's difficult times and there's great times, but it's always a struggle. And I've been very blessed physically. I mean a lot of terrible things happen to people and they haven't happened to me. But I haven't escaped entirely from physical woes. I've had a few that have damaged me. One is that I used to get something called cluster headaches, which was terrible and I had for like 25 years, and they were awful.

Another thing that happened was a stupid thing. I was I think playing racquetball and I hit the wall, and I became black and blue all over the side of my body. I went and had X-rays. Nothing showed up. But soon thereafter, my back failed. I conjecture that I messed something up down there. It got worse and worse and worse, and limited my movement more and more and more, and created more and more chronic pain, and I was reduced to being in a wheelchair for a while. I couldn't do anything, and it contributed to the destruction of my marriage. It was just a very bad time for me.

But there's a big lesson. You know how as professors sometimes, troubled young people come up and maybe ask us about their personal problems. One of the things I always tell them is "In my experience, whatever's horrible in your life right now, whatever you cannot see a way out of, what is going to just destroy your life, make you miserable, in my experience it's very likely than in five years it won't even be on your radar. That's the good news. The bad news is something horrible will come along and replace it. But… So keep the broader picture."

So the headaches went away. For some reason I don't know, but they stopped. And the back problems I was having, this thing that was confining me to a wheelchair, I tried everything. I tried orthopedic guys' shots and this, that, and the other thing. I tried chiropractors and I tried massage therapists and I tried physical therapy and yoga. A zillion things. I learned that this old saying, "When all you

have is a hammer, the whole world looks like nails," every one of those practitioners in all those fields sees you as their nail and the odds that they're all right are vanishingly small. So you just got to go on down the list of things and try them is my experience, and maybe if you're lucky, somewhere down that list something will actually be useful to you. And it happened to me. I found a few things on the list, the most important of which was to start enduring a bit of pain and start building up my body through exercise. It took me… It's taken me 20 years. But right now, I'm always in pain. People our age are quite often always in pain. But I can do everything I want to do. I can walk now, I can go places I want. It's been great. So life's a struggle. I mean I'm very blessed. A lot of people have a lot worse than I do.

HW: You're one of the few people I know who has a Hollywood credit.

LA: Ah! Yes, I do.

HW: Do you want to tell us about *Sneakers*?

LA: Of course. So the *Sneakers*, yeah. There were these guys Lasker and Parkes, and they had made a movie called *WarGames*. It starred Matthew Broderick I think. It was a big success. Based on that success, they were now able to produce Hollywood films. They could get money and stuff. So they called me one day, I'm at USC now, and they say, "We'd like to come over and discuss a movie idea with you." I said, "Okay. Come over and we'll discuss it." They came in and they said, "Well, we have this movie idea that we're pursuing. The idea is there's going to be this secret code and it gets broken and the world is threatened by it and everything like that." I said, "Okay." And Lasker I think it was said, "Ah. And then we have this other idea of a movie, because we're considering a couple others. This other movie would be about these people who have been sort of frozen for a very long time, medically frozen, and there's this new drug" – I think it was probably dopamine – "that you can give to these people and they come out of it. You know, they can dance and everything else, and they've been frozen for years. Sort of Rip Van Winkle stuff." I remember saying to them, "Wow, that sounds a lot more interesting than crypto."

So they disappear. You know, "Thank you. Bye." I don't hear from them again. The next time I encounter them, this movie *Awakenings* comes out, which starred De Niro and the comedian who recently died.

HW: Robin Williams.

LA: Robin Williams. Really good movie. They made that movie, right? After that, I get a call and they say, "Can we come over again?" I say, "Sure," and they say, "Look, we're now making that crypto movie we talked about and we would like it if you would help us and advise us on this movie. In particular, there's going to be a scene where this cryptographer has a breakthrough in factoring, and it's going to

have big implications for crypto." So I said, "Uh, sure. That sounds fun. That sounds nice. I'll do that." They offered to pay me to do this work of creating dialogue for the movie, the mathematical dialogue, and of creating slides and dialogue for the professor who's going to describe this breakthrough in factoring. So they say, "We'll pay you for that," and I say, "No. I don't want to get paid, but I'll do it if you give me Robert Redford," who stars in the movie. I say, "I'll do it if I can introduce my wife to Robert Redford." So they agree to that.

So I go home and I really work hard on my little old-fashioned Apple. This is very early. Things aren't user friendly. Graphics is not easy. And I make these brilliant, dazzling slides. And I write dialogue, and I write dialogue wherein I… the slides and everything are about towers of number fields and Artin maps. They're just some fantasy. I decide that… And I have to write dialogue for the talk that this professor's going to give. So I write, well, probably it's monologue for the talk and I have the professor saying, "It is a breakthrough of Gaussian proportions," because since Gauss had given me so much, I thought I could give him a plug in a major movie. Right? So I really liked that, "Gaussian proportions."

Then I was going to call the name of the new method the "function field sieve," because the current best factoring was the number field sieve and I was working on a paper called "The Function Field Sieve." I don't know why I decided against that. I wish I had called it "The Function Field Sieve" because it would have really helped the function field sieve paper I was writing.

Anyway, there came the day when it was time to actually shoot the scene. We went out to this college in L.A. and there was Robert Redford. So we got introduced and in particular my wife got introduced. Then we chatted for a while. At least I chatted with Redford for a while. He was talking about Stephen Hawking, stuff like that, so he was interested in that kind of stuff. My wife just stopped after "Hello." I think she was starstruck by Robert Redford. Anyway, so we chatted for a while and then they filmed the scene. It's a pretty good scene. But… And I got… I think I was "Mathematical Consultant," in the credits as "Mathematical Consultant." But as I like to say, the Academy snubbed me because apparently the mathematical consulting Oscar went to somebody else that year.

HW: You're associated with the creation of an early computer virus. Can you tell us something about that?

LA: Yeah, that's another interesting episode. I'm at USC, it's 1983, and I'm teaching a course on computer security and privacy, because crypto, right? This kid, Fred Cohen comes up to me after class one day and he says, "Professor Adleman, I have this idea for this new kind of security threat on the computer. I'm going to write this program and then everybody's going to use this program, but it's secretly going to send me all their privileges and access to all their data." I said, "Yeah, that would work, Fred," and Fred said, "I want to try it." I said, "You don't have to try it, Fred, because it's clearly going to work." He said, "No, I want to try it, I want to

try it." So he wears me down and I go to the chairman of the department, because we don't have personal computers at that time. We all use one big computer. I go to the chairman of the department and I say, "Look, this kid in my class wants to try this experiment, blah-blah-blah," and the chairman says, "Sure, why not?"

Fred proceeds to write this malicious software and he proceeds to make it available to everybody on the computer, and everybody or enough people take it so that when they take this program up, it sends Fred access to all their data and all their privileges. So Fred takes over the whole computer. He can see everything, do everything, change all the grades if he wants. And he runs this several times. He comes back to class and I invite him to present his results to the class, and he describes what happened. And it takes over the computer. You know, the only interesting thing is it took 30 minutes this time, and this time it took five minutes, some different variation, and he gets all control of the computer.

So Fred wants to do more experiments, because now he's thinking hard about what you can do with these things. He wants to do more experiments and he's thinking about it, what he could do, and he wants to use more computer time. But by that time, word gets out about what Fred has done and other people are starting to think about what you could do with programs like this. And the chairman decides he'd been a little hasty in letting Fred do this, so no more experiments.

But Fred wanted to do his PhD thesis on this kind of thing. And I wasn't his official advisor. Irving Reed of Reed–Solomon codes fame was his advisor, but in some ways I was a de factor advisor. So he starts writing a paper, a thesis on computer virus. Practical aspects, some theoretical aspects.

Then one day I'm at a crypto conference, the Santa Barbara CRYPTO conference, and I run into a reporter I knew, Lee Dembart of the *L.A. Times*. As a routine matter, he says, "Len, what's new? Anything interesting happening?" I said, "Nothing's really going on. I got this student who's started working on this thing we call a 'computer virus.' " I was naïve. I should have known that you tell a reporter that you're working on something called a "computer virus"… well, yeah. So Lee writes the first public article, as I recall it even had the now familiar computer with a thermometer image on it, and says, "Computer viruses." He describes it and uses the term "computer viruses." That's the first time it appears in the news press. I've subsequently learned that both the term "computer virus" was used in science fiction before me by a guy named Greg Bender, and that other programs in addition to Fred that were happening around the same time also could be claimed to be the first computer viruses. But for me at least, Fred's the father of the computer virus.

HW: Well, you talked earlier about some of your DNA work. Would you like to expand a little bit more on that?

LA: Yeah, a little bit. What happened was that's sort of pushed me into getting an actual molecular biology lab and I started doing experiments in molecular biology and had people in the lab. Erik Winfree and Paul Rothemund who I mentioned, these guys were great at this kind of thing. They were also theoretical computer scientists, so it was computer science meets biology. But there were a lot of people in the lab and it was a big lab, and people were throwing grant money at me. I found myself back in this situation I never wanted to be in of running an endeavor which I wasn't good at. But fortunately Erik and Paul in particular, but others as well, were really good at this stuff and they sort of flipped the whole field on its head.

This gets back to cellular automata, because we knew you could compute with the tools of biology, but there's a million ways to go about computing. One of the most fundamental things that the great logicians like Turing and Gödel taught us was it doesn't take much to compute everything that's computable, to be universal. Just a way to store some data and a way to manipulate it. The ways can be incredibly simple, but you still can compute everything that's computable. So we knew there were a million ways to use these tools to compute. One of the ways goes back to cellular automata, and Erik Winfree started to say, "Well, we can take strands of DNA and they'll self-assemble into structures based on how they interact with each other, and we can do universal computation that way."

So he started to do that. I remember going over to Caltech. This was one of the most exciting things in my life. He had this new device at Caltech. He was a Caltech student in fact, and he had got this atomic force microscope, because DNA molecules can't be seen through a regular microscope, but you could see them now. He had taken DNA strands that he thought, if he threw zillions of these strands in, they would wind around each other and form like these big crystals or brick structures. So I was over at Caltech and Erik's doing his experiments and he's got his atomic force microscope and he's trying to use it and everything. On the screen appear these bricks, just like his theory had said they should appear, and we were looking at them. We were up here in the macroscopic world and these things were down there at the nanometer scale, and Erik was designing them up here and making them appear down there.

This became known as DNA self-assembly. It was really quite an amazing thing. Suddenly we had control of the nano world. I mean we'd been able to draw a plan for a house for a long time and then you'd get engineers and construction people and they'd build it, and they'll build 20 copies if you want. We could do that. But now we could design stuff up here and have it take place at the nano world. That sort of turned DNA computing on its head and self-assembly, "What could you assemble?" started to become a real topic that grew out of it. And they assemble to great things.

I don't know if this will work on camera, but then Paul, my other student… I always carry this with me. You probably can't see it. It's a picture of a *Nature*

cover. On it is a little yellow happy face. Now the thing about that happy face is, one, I'm very proud of Paul. He made it all by himself. Two, it won him the MacArthur award. Because that's not a little diagram. That's an actual physical object and it's about 100 nanometers in diameter. So like 15,000 of them or something could fit across a human hair. And it's made entirely of DNA. Paul designed some strands up here, got them made in tubes, poured them all into a common tube, they came together and wrapped around themselves and formed that happy face. He did it in a little drop of water. In a half-hour they all assembled. There were 50 billion of those. Now these guys who are in this area… Hugh, I think people would like 50 billions statue of you made out of DNA, right?

HW: Not likely.

LA: We can get it done. So it gave rise to all that and it's really quite lovely. People sometimes ask me, "Well, is DNA computing ever going to be practical computing?" The answer to that in one sense is no. Electronic computing just is too advanced for us. We can't keep up. We did okay, but we couldn't beat out electronic computers. Also, there's this line I like. It's not that the bear dances so well, it's that he dances at all.

HW: Dances at all.

LA: Right? So it's not that DNA is going to replace our supercomputers, but it computes, and that tells us biology computes and you can look at biology as computation. Also, DNA computes in places that silicon can't, like inside of a cell. So people are working on trying to use DNA computers to place inside cells to fight disease, deliver medicine, stuff like that. So there will be ramifications of this stuff and they should be exciting. But another really nice, fun chapter here.

HW: Well, our students are like our children when we're professors. Would you like to talk about some of your intellectual children?

LA: Well, I've had a number of really brilliant intellectual children. I've spoken about Erik and Paul. In addition, I've had some really brilliant theoreticians. I have one right now, Joe Bebel. Really for sort of raw intellectual power, he's as good as I've ever seen. I'm currently collaborating still with one of my other students, Rolfe Schmidt. We're writing a paper on digital currency and making a surrogate for the United States' physical currency – dollars and coins. And I collaborate with them and some others on another area that I'm currently working, which is complex analysis. We're writing a book in that…

But I've had a number of them – Dustin Reishus, Henry Yuen… Unfortunately I'll probably leave somebody out. But anyway, I apologize. Brilliant guys. We get to see the best. They're so brilliant and they're so wonderful to work with. To watch them grow and to see their lives and how they evolve, they have all the troubles and difficulties that every human has, but they also have these great gifts that make

their lives much more exciting and I think wondrous than the average person. I get to enjoy that vicariously and maybe give them some guidance. It's a blessing. It's wonderful.

HW: What are you working on now? You said one thing about this project in analysis.

LA: Right. I never liked analysis. I never got it. But I stumbled into it. So for the last like 10-15 years, I and my students have been immersed in complex analysis. We sort of made the decision that we would do complex analysis. We had a choice. We could stand on the shoulders of the giants. We could stand on Gauss's and Cauchy's and Riemann's shoulders, or we could just try it ourselves. Perhaps unwisely, we chose the latter. The value of doing… I mean the bad consequence with doing that is you don't know what they did, very little, or what happened since then. The good thing is you go your own way. So we've gone our own way and we've created something we call "strata theory" and we are polishing a book which we've been polishing for the last seven years. It's about 230 pages. It's really a good book and it's complex analysis. Strata theory, complex analysis.

It fulfills a desire of mine. Since the great mathematicians were always my heroes and they all provided big bricks in the wall that we call mathematics… You know, it's all built on it. But they're at the foundation, right? And I've been blessed. I've put a few little ornaments on that tree. But I always wanted to at least have my little brick in that foundation. This strata book is my sort of legacy to mathematics, because complex analysis of the form we're doing is also in a sort of ember stage. It's not burning very brightly right now. There's brilliant people, just a few, a handful that still do it. And it'll burn brightly again I think. I think when it burns brightly again, maybe people will come back and take my little brick and use it. That's one of the things I want to do.

So I work hard on that. I'm trying to apply what we've learned to some of the Hilbert problems without success. Then I'm also working on this paper with Rolfe Schmidt which we hope will give an alternative to Bitcoin and credit cards and everything for an economic infrastructure as we move more and more into the web. We would like to think that our system will provide a basis on which we can build a better economic future in the world that will improve the lives of lots of people. We think we've got a good system. So we're working on that.

Then the final thing I'm working on is a book, which is about 125 pages and I've been working on it for a long time. It's on memes. Not "memes" as they're currently used on the Internet. Not dancing babies or something. These go back to where the word comes from, which is Richard Dawkins. In the '70s, Richard Dawkins produced this wonderful book called *The Selfish Gene*. It's mostly about genetics, but he mentions these memes. Memes are a generalization of genes and in his hands, as I recall, he's thinking of them largely as sort of cultural ideas that can reproduce by passage to other brains and can evolve because we tend to change

our ideas and interact them with other ideas, and therefore an evolutionary system like genes.

And when I read Richard's description, I said to myself, "Oh, that's how it all works. That's what motivating and moving human beings in the same sense that the genes are moving and motivating biological organisms." I've thought about this stuff for 40 years, and so I'm writing down my thoughts. I wish I could have written a better book, but given time constraints, I have to write down what I got. So I'm enthusiastic about that as well.

HW: Any thoughts on retirement?

LA: No. I'm a "die at the desk" kind of guy. I wouldn't know what to do. I'm better at it now. Maybe I would know what to do. But no, I don't want to retire.

HW: So we finished the accomplishment section, unless there's something that I've left out.

LA: No, I can't think of anything. Can I…

HW: Okay. Let's go into the retrospective section. Actually we're getting close to the end of my questions, believe it or not.

LA: Really? Maybe… Is it a good time to take a break and then we can finish up?

[A short beak was taken]

HW: Oh, okay. So who during your career were your role models?

LA: Oh! My role models. Gauss. I also thought that Newton and Einstein were pretty good. Certainly Manuel Blum, my advisor, certainly a role model. Dick Karp was a role model. Albert Meyer, who is a professor at MIT, was a role model. Who else? Was there anybody else? I thought Darwin was good.

HW: Yeah?

LA: Yeah. Right.

HW: Any more that were closer to you?

LA: Oh, closer to me. Okay, yes. Role models. Umm… No, the three computer scientists I mentioned were certainly role… Oh. I think in many ways… There was a professor of logic. His name was John Addison. He's still with us I think. Quite old. He was sort of inspirational to me. He was a wonderful teacher and was the one that could present to me mathematics in a form that I could see its beauty, that I could fall in love with. "If you don't cross that bridge, get another job,"

right? And John had a lot to do with my crossing it. He showed me wondrous things.

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

LA: Well, I've mentioned that people played a part. Linda Kavner. Martin Gardner certainly. But largely my progress through mathematics was kind of characteristic of my progress through life. That is I was just doing the things that fascinated me all the time. I just found that as time went by, I was in better and better company doing it. At least what was perceived as better company. Originally it might have been colleagues at school or kids in my classes and stuff like that. Then as time went by, I never stopped what I was doing. It's just that I was at better places doing it. At least I was getting paid more. Or like I'm at MIT and I'm doing the same things I always did but now it's with Rivest and Shamir, who are just great. So I don't know. The way it looked to me from the inside was just life going by and I find myself here and was in such fun places. So nothing comes to mind as a big turning point other than those things I mentioned earlier.

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

LA: Ooh! Let me tell you the best decision I made, or one of the best, was to leave MIT. I was unhappy there. It was cold. I had just gotten my first divorce. I brought my beautiful German shepherd with me and she got run over. Socially I felt out of place. I mean with my friends I was okay, but I couldn't acclimate. I'm not a very adventurous person, so I had to leave that place. And it was a regret to leave it and it was a hard decision because it is a mecca of research. It's a *wonderful* place for research. But I traded that off to come back to California where I felt comfortable.

And Erdős. You know Erdős of course. He's the most published author in the history of mathematics I think. We all know our Erdős numbers and stuff like that. When Erdős came to town as a young mathematician, I'd be very excited. But as I watched Erdős through time, I watched that he had sort of sacrificed his life to his discipline, to mathematics. He had no home, he had no family – his mother eventually died – and he just was this itinerant mathematician. And that's fine and he accomplished tremendous amounts, but it made me reflect on whether I wanted a life like that, because I could see it in me to be that person, to always sit in a room and always do the mathematics. But I said, "No, I want to have people in my life, I want to have a family, I want to have children." I thought that I wouldn't be able to do that very well in a place I wasn't comfortable in, Massachusetts. So I made a decision to go back. That was one of the best decisions I ever made.

What were bad decisions I made? Decisions I regret? [pause] I don't like the way I have handled my physical problems, like the headaches or that back problem that

put me in a wheelchair. I don't like the way I handled them but I just didn't know what to do. Made some bad decisions there.

Oh, here's another bad decision I made. I was so dedicated to mathematics that I wouldn't allow myself to leave time for anything else. I didn't want to be encumbered by anything that would interfere with ability to go sit in the room and think. By making that decision, it was a very bad one because it cut me off from social relations, which I need very much in my life, and it cut me off from interaction with people and maybe exploration of things I would have found exciting and would have enriched my life. But I made the decision to try to cut all obligations so that I could study mathematics. It led me to be isolated during certain parts of my life and it led me to be bored during certain parts of my life, because I never had an obligation. So yeah, that didn't work out perfectly well and I've reversed that somewhat in my older age.

HW: What were your most important life lessons?

LA: Hmm. One I mentioned, that whatever seems terrible is likely to be transient. Not all of the time unfortunately, but likely to be transient even though you don't think so.

Another important life lesson for me is the importance of people and interactions and family. In many ways, I'm sort of an on/off person. If I'm around people, if I'm interacting with people, I feel very much alive. If I'm by myself, I don't. And I've struggled with depression and math has been a relief from that, because when I'm alone I do math. But that's been an aspect I've learned about myself.

And some very classical things that everybody's known or people have talked about for thousands of years. It's how you play the cards that life deals to you is going to determine how much joy or sadness or distress or whatever that you get out of life. It's not a free ride. It's very tough. But you can participate in the journey and you can steer to its better or worse things. That's been an important lesson to me.

HW: What was your proudest moment?

LA: Proudest moment? My mind turns to the birth of my children. That's what it comes down to, you know? Yeah.

HW: Right answer.

LA: Oh, yes, yes, yes. As the daughter who lives with me says, we joke about a Nobel Prize and an acceptance speech. She says, "Yeah, when you get up there, you should say, 'The most important two awards are the Nobel Prize… that I've aspired to are the Nobel Prize and Father of the Year.' "

But Father of the Year is maybe the better one.

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

LA: I think the ones that will be remembered are cryptographic, but the ones I'm most proud of is my contribution to algorithmic number theory and the fact that I got to sort of shepherd in this new concept of complexity theory. That should have ramifications for a long time in a field that is very dear to me. So I think that's most important to me.

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

LA: Umm… [pause] No.

HW: Oh. Alright. Good. Then my job is done.

LA: Well, great job, Hugh. That was wonderful. Thanks so much for doing it.

HW: No, not a problem. Not a problem at all.

[end of recording]