Martin Hellman:
2011 Fellows Interview

Public-Key cryptography

Interviewer: Jon Plutte

Recorded: March 11, 2011
Mountain View, California

CHM Reference number: X6076.2011

Jon Plutte: Okay. We're here today. It's March 11th, 2011. We're interviewing Professor Martin Hellman at the Computer History Museum. Thank you for joining us. I'm going to start off with a series of short questions and as we discussed, please keep an eye on the camera and answer, try and answer my question as you are answering; I mean state my question as you are answering. My first question is what is cryptography?

Martin Hellman: Cryptography is the study of codes and ciphers for two purposes, privacy and authentication; privacy to prevent prying eyes from seeing what two people are saying and authentication to prevent a third party from injecting messages and making them look like they're coming from someone else.

Plutte: Next question; what is public-key cryptography and how does it differ or how is it the same?

Hellman: Public-key cryptography differs from conventional cryptography in the following way: In conventional cryptography, you have to exchange a key securely ahead of time. The same secret key is used by the sender of the message and the receiver of the message, transmitter and receiver. And since the same secret key is used to encipher and to decipher, clearly it's got to be protected in transit. In public-key cryptography, we broke the key into pieces, a public-key and a secret key. And so there are other variations, but one way to think of it is the public-key could be used for enciphering; so I could put that out in a directory and everyone could encipher messages and send them to me, no courier needed because it's public. I keep the secret key, which is its inverse, secret obviously, and only I can decipher the messages.

Plutte: Okay. Sorry.

Hellman: That's okay.

Plutte: I've got a little mess here. That was a great answer and I'm wondering if you can possibly, since this is sort of the core to our whole discussion for the movie, is there a way that you can do a really, really condensed version of a public-key cryptography?

Hellman: Sure, not contrasting it, just public-key by itself.

Plutte: Yeah.

Hellman: Yeah, that would be short.

Plutte: Yeah, okay.

Hellman: Ready?

Plutte: Are you ready? Okay.

Hellman: Okay. In public-key cryptography, you break the key into two pieces. And so, one piece, the public-key, can be public and the other piece, the secret key I would keep secret. Everyone can encipher messages and send them to me using my public-key, but only I can decipher them. That's how it works.

Plutte: Okay. When did you first think of doing public-key cryptography? Maybe give us just a little hit on the history of where you started and how you came up with the idea or your process for developing the idea.

Hellman: I've lost track of the exact date when we came up with it, but it was in 1975 and there were a couple of things that led to it. One is we saw commercial use of encryption becoming widespread and in commercial encryption, there's a lot more of a key distribution problem. In the military, there's a chain of command that limits the number of connections whereas any two people outside the military might want to talk to one another. So, that was part of it. The other thing; Whit [Diffie] and I were working independently of Ralph [Merkle] at that point. We were looking at things like trapdoor ciphers, how you could make a cipher that would protect your communications. Like if you're a general, you could give it to your troops and know it's inviolate against your opponent, but if the opponent captures it and uses it, then you could break it easily because you have the trapdoor information that went into its design. It's a very small step in hindsight from a trapdoor cipher to public-key cryptography. Now, Ralph came to it independently of us in a slightly different way.

<Crew talk>

Hellman: Oh, okay. Good. Yeah, to me, time goes very fast and I will do that. You can always cut. Thank you.

Plutte: That gives us a little insight into the history of it. So, what specifically motivated you to work in that? I know that it sounded like almost three independent folks working together and then you ended up working together. Can you give a little bit of story of how that full process of working together went?

Hellman: Do you want how we came to work together, or do you want first how I came to work in this individually?

Plutte: First, how you came to work on it individually and "then I worked with and then I"--

Hellman: Okay. There are three key events that I can pinpoint that led to my interest in cryptography. One was David Khan's book, *The Codebreakers;* I think it was 1967 that it came out. He spoke at the 1969 Information Theory Symposium that I went to and that year, '68 to '69, I was working at IBM Research and they had just started their cryptographic effort that led to the Data Encryption Standard (DES). The guy they hired in to start that, Horst Feistel, was in the same department as me. So, I'd have lunch with him. He'd explain to me how a lot of things worked and I could see IBM was spending good money and so, it reinforced in my mind that there was a growing commercial need. The third key event was when I was at MIT, I taught at MIT from 1969 to 1971, and Peter Elias, one of the original contributors to Information Theory, gave me a paper by Claude Shannon, the father of Information Theory, that made it clear that cryptography was a branch of information theory and that what I had been studying in my Ph.D. and soon afterwards was applicable. So, it was those three events.

Plutte: So, how did you start connecting with the other folks who worked on this?

Hellman: So, for several years, I was really working in a vacuum and more than a vacuum. My colleagues uniformly told me I was crazy to work in cryptography. They had some good reasons: NSA had a huge budget, how could I hope to discover something they didn't already know? They'd been working on it for decades and if I did anything good, they would classify it. Those two arguments were almost-- it was amazing how frequently they came up. However, that did not deter me. I'm a bit of a fool that way and in fact, I view this as part of the wisdom of foolishness. When I was at Yorktown Heights visiting Feistel and the IBM crew working on cryptography, Whit Diffie came through a few months later saying roughly similar things and it turned out they weren't very interested. They were being moved away from cryptography toward operating systems security by management, but they said, "When you get back to Stanford, look up Hellman." And so, Whit did and I set up a half hour meeting with him that ended up ending at 11:00 or 11:30 that night. He stayed for dinner. I mean it was really a meeting of the minds and so that's how Whit and I came together. And then, a mutual friend of Whit's and Ralph's heard the two of them talking about cryptography. Ralph was at Berkeley at the time and suggested we get together and when we met Ralph, it was the same thing. I mean clearly another fool, another person crazy enough to work in this area with lots of good ideas and by the time we met him, we each had been working on trying to develop public-key cryptography.

Plutte: So, was there a first product that you and Whit Diffie did, then you collaborated with him more with Ralph, or did you work together to develop the whole process?

Hellman: Jim Massey was the editor of the IEEE Information Theory Transactions and he came around, he saw that my work in cryptography was going in good directions. This is prior to public-key cryptography. He invited me to write a paper; we call it an invited paper, for the *IEEE Transactions on Information Theory*. Since I was working closely with Whit, I brought Whit in on that and Jim Massey agreed that it could be a joint invited paper. When we came up with our approach to public-key cryptography independently of Ralph, we, of course, started to put that into the paper and then when we developed what is now usually called Diffie-Hellman Key Exchange, although I've argued it should be called Diffie-Hellman-Merkle Key Exchange if you put names on it, we, of course, incorporated that. But, Ralph has a separate paper he had already submitted to the Communications of the ACM and so, the first two key papers were published separately because he had done his work independently of us and we had a lot of other things in our paper.

Plutte: And so, after those, you started collaborating on more development of the process?

Hellman: Well, once I met Ralph, I really wanted to have him work more with me and I wanted to work more with him, and he was finishing up his Masters at Berkeley. When he did that, I kidnapped him and brought him down to Stanford. He finished his Ph.D. at Stanford under my supervision, although to say you supervise Ralph is not quite right. I mean that's technically the situation, but he was very much an independent contributor.

Plutte: Three strong personalities; how was it for the three of you to work together?

Hellman: How was it for the three of us to work together? Initially, just the two of us, Whit and myself, it was fantastic. I mean as I mentioned before, he came down for a half hour meeting that I had set up and ended up staying for, I think, eight hours because both of us really enjoyed having someone else to talk to and not say, “You’re crazy to do this.” Over time, we grew apart too. I mean Whit really needed to have his own position and place. I was a tenured professor. He was technically a graduate student. We’re about the same age and so he went I think initially to BNR, Bell Northern Research. Ralph, of course, when he finished his Ph.D. went to work at a company, Elxsi, Electronics X-Silicon is what it stood for, the computer manufacturer of the future as Ralph will tell you. Then, he went to Xerox PARC and a few other places. He also moved into nanotechnology out of cryptography, so we saw each other, but didn’t work as closely.

Plutte: Okay. Do you have any good anecdotes, stories about--

Hellman: About them?

Plutte: Yeah.

Hellman: I mean that first meeting with Whit, Ralph. I mean they’re both unique individuals. If I tried describing them, it could come across as making fun of them and it’s not. It’s just their personalities. They could do the same with me.

Plutte: Backing up a little bit, people gave you lots of reasons not to work on cryptography and they seemed to all revolve around the NSA and government security. Do you feel that the NSA was hindering you or helping you, or did they have any opinion on the work you were doing? Did they communicate with you?

Hellman: NSA never really helped us in our work. I mean that’s not their job. Their job is to work on classified research. Early on, they were very unhappy with us doing our work because we were publishing things that I’m sure they would have classified very highly and, in fact, there were some threats that we could be thrown in jail for publishing our papers. These were never official threats coming from NSA, but there was a man who worked at NSA, we determined later, who wrote a threatening letter from his home address in Maryland to the IEEE. I’ll never forget the conversation I had with Stanford’s general counsel over that letter. Should I describe it?

Plutte: Yes, please.

Hellman: John Schwartz was Stanford’s general counsel and so, when I got this letter that Meyer had written from his home address in Maryland to the IEEE, pointing out that you could be thrown in jail for five or ten years and I forget the fine, in the thousands, in many thousands of dollars. But publishing papers in cryptography and exporting them as in fact the IEEE Transactions were exported, I, of course, took the letter to Stanford’s general counsel, John Schwartz. He studied it and at our second meeting said it was his legal opinion that if the law was construed that broadly then it was unconstitutional, but he warned me that that was just his legal opinion and it would have to be decided in a court of law. He told me that if I was prosecuted, Stanford would defend me, they would appeal, but if all appeals were exhausted, he warned me, and this is the part I'll never forget, "We obviously can't go to jail for you and we can't even pay a fine because now you've been adjudged a criminal. We can't aid and abet criminal conduct."

Plutte: How did that make you feel?

Hellman: How did that make me feel? Well, that made me feel actually quite good because, I mean I knew they couldn't go to jail for me and I knew that-- I mean the fact they couldn't pay a fine was minor compared to the jail time, but knowing that knowing Stanford would defend me gave me the confidence that we could go ahead and deliver the papers that were scheduled for our conference just a couple of months later, October 1977, at an IEEE Information Theory Symposium at Cornell in New York, although there was an interesting little hitch. The two papers were joint papers. One was a joint paper with Ralph Merkle and me and the other was with another graduate student, Stephen Pohlig, and myself. In both cases, I was going to have the students deliver the papers, get more of the attention for them, help create their reputations. John Schwartz, Stanford's general counsel, strongly suggested that the students not deliver the papers, but that I deliver them instead because it wasn't clear Stanford could defend the students legally if they were prosecuted, but also he pointed out that as a tenured professor, my career could withstand a multiyear court case whereas theirs could not. So, I went to the students and I told them what John Schwartz told me and I said, "Whatever you want to do is fine with me. I'm not worried about giving the papers. I'm quite confident that, you know, if there's a case, Stanford, we will prevail and we do have Stanford behind us." The students wanted to deliver the papers anyway and initially said they would and after about a week though, they came back; their parents were really worried and so, their parents prevailed on them. So, I gave the papers, but I had each student stand right next to me, everybody knew what was going on and I said, "On the advice of Stanford's counsel, even though the student would normally give the paper, I will be giving it for him, but I want him to get the credit he deserves. So, please consider it in every other way as if he's giving the paper." So, the students actually got just as much, even more attention than they would have if they had given the papers, and we were not prosecuted.

Plutte: That's a great story.

Hellman: There's a little more there too.

Plutte: Please, yes, yes.

Hellman: Now, NSA did try officially to get some laws passed. Admiral [Bobby] Inman, who was the Director of NSA at this time in the late-'70s, was trying to get Congress to pass laws that would make it clear that certain areas, and cryptography was right at the top of the list, were born classified, meaning even though people like Whit and Ralph and myself had not had any exposure to classified literature, whatever came up with was still potentially classifiable. But, Inman is a very thinking individual and we got to know each other. He actually initiated the contact against the better advice of everyone else at NSA he told me, and we came to really respect one another. I pointed out to him that the wall wouldn't really serve their purposes because it would alienate the authors. They needed the authors on their side. They were going to use the editor of the Transactions as the gatekeeper and so, the authors, if they were really PO'd, would just go give a hundred talks before they published and that can't be covered by the law. And so, he came to see that they really need the authors' cooperation and to his credit, he changed the program into a voluntary one.

Plutte: That's great. Today-- I'm sorry; I lost my notes here. Today, there's a little lock in the corner of all of our browsers, which is related to work, but back when you invented this, there was-- what was it used for? What was the reason that you developed this?

Hellman: Well, of course, the Internet did not exist in 1975-'76 when we were developing this work, but I could see either then or very soon after that there was a growing-- well, even then, I could see that there was a growing marriage of computers and communications and this was going to be very important, like electronic funds transfer, which was bank-to-bank at that point in time. I remember saying right around that time I could foresee the day when you might use an electronic funds transfer to buy a loaf of bread, and I couldn't think in terms of a debit card because we didn't have them, but that's basically what I was describing. So, we did have a vision of how the world was headed, and we were at the forefront of that. The ARPANET, which preceded the Internet, we had access to that by the late-'70s/early '80s and we already had networked computers in our laboratory in '75-'76 time frame. So, we could see the future a little bit more easily than most people.

Plutte: Okay.

Hellman: In fact, we could see the future so clearly that we saw it wrong. Whit and I thought when we published *New Directions in Cryptography*, this key paper of ours in 1976, we thought that commercial encryption would be a big business within five, at most ten years. In reality, it actually took double that. It was 10 years before it really became of any significance and 20 years, 1996 is when the Internet really started to explode. So, when you can see the future that clearly, sometimes it looks closer than it is.

Plutte: Okay. Today, the technology you developed enables of billions of dollars of, you say, commerce on the Internet, yet in an interview, you once said that you made almost no money off of this development. Why not, and how does that make you feel about it, and the creation of it, has that been enough? Let's talk about how you feel about all that.

Hellman: Well, it's true that the Stanford patents made almost no money either for Stanford or for the inventors. The inventors were supposed to split a third of the money and there was very little. The MIT patents became much more valuable, but partly because they built a company, RSA Data Security, around it and part of the problem was, while in their paper, RSA, Rivest, Shamir, and Adelman credit us with inventing public-key cryptography, when it came time to pay royalties, they said, the company said your patents are invalid; sue us. Now, in their defense, there's a difference between academic credit and patent credit. Stanford had a summer intern, a law student write the first patent. It wasn't as well written as it should have been. And so, there was a time when I was unhappy with RSA, both the individuals and the company, over this, but I've done better in life-- I grew up in the Bronx, okay? I live on the Stanford campus. I flew a motor glider. I've done things that I didn't think I'd ever- that were incomprehensible to me as a kid growing up in that relatively not impoverished, but relatively poor environment by Peninsula standards. In more recent years, meaning the last 10 or 20, I really looked at it and while I could be unhappy with RSA, they really created, and Jim Bidzos, who was the business guy at RSA, really created an industry for public-key cryptography, which has brought economic benefit to me. So, I could be unhappy that we didn't make more money and that they, you know, took a tough stance with us, or I could be grateful, which is where I've ended up being, that they helped create this business that has actually done good by me economically.

Plutte: I have about two more questions on this subject. Do you need a drink of water, or are you okay?

Hellman: I'm good.

Plutte: Okay, good. Can you paint a picture--

Hellman: Is this a problem like this by the way?

<Crew talk>

Plutte: Just a few more questions.

Hellman: Okay, go ahead.

Plutte: Can you paint a picture of how the world would be different today without public-key cryptography?

Hellman: Well, the world would clearly be different today without public-key cryptography. It's hard to say exactly how because there are other ways to distribute keys other than public-key cryptography. There's something called the Key Distribution Center, which was an idea before we came up with this. There would be one trusted center and everybody would share one secret key with that center and then when two people wanted to talk, the center would generate a key for that session and send it to each of them protected by their individual keys after which they could use that session key to talk. It's not as elegant and it's not as secure as public-key cryptography, but it would have worked. Digital signatures would have been much trickier, the authentication part of public-key cryptography.

Plutte: And then, I'm going to move on then unless you have any other subjects you want to cover.

<Crew talk>

Hellman: I didn't say anything about it. But there's another thing we could do; I could describe how public-key-- a rough idea of how public-key cryptography works in a way that people could understand, not mathematical.

Plutte: That would be prefect. That would be great.

Hellman: Okay. Public-key cryptography involves fairly complex mathematics, but there is a way to get a hold of the basic idea in terms of physical exchange of strongboxes and of course, we're going to mathematize that for public-key cryptography. Imagine you have a strongbox that can have not just one lock on it, but two and you and I want to exchange a message. I want to send a message to you. I put the message in the box. I lock it up with my combination lock that only I can unlock. I hand it to a dishonest person who hands it to you. The dishonest person can't open it, right, because my lock's on it. You can't open it either. You put your lock on it, hand it back with the two locks to the dishonest person in the middle, the eavesdropper, who gives it to me. What do I do? I take off my lock. Now, there's just your lock on the strongbox. I hand it to the dishonest person, the eavesdropper in the middle. He still can't open it. When it gets to you, you can open it, and that's an example of a physical system that's very similar to public-key cryptography. What's critical there is that it doesn't matter the order in which you put on the lock. You can put on lock one, put on lock two, take off lock one, take off lock two. You don't have to put on lock one and take it off before you put on lock two and take it off. It's something in mathematics that's called commutative and that's a key element of making public-key cryptography work, at least the Diffie-Hellman-Merkle Key Exchange uses a commutative function.

Plutte: Okay. About 15 years ago, Sun co-founder Scott McNealy claimed privacy is dead. Is privacy dead?

Hellman: Privacy is far from dead. You don't want your medical records publicly available, especially with some of the healthcare initiatives. Medical records are being computerized and shipped around. You don't want your banking transactions known. It depends on what he meant by "privacy is dead." I mean Facebook, sure. People put out all kinds of information on Facebook, but you don't put your medical records, you don't put your bank account on Facebook.

Plutte: Is there anything else you'd like to add about the subject?

Hellman: No, I think we've covered a lot. Was the description in terms of the strongbox, was that too long or was that useful?

Plutte: It would be good if we could do one more shot at that because that's key and try and make it as concise as you can, but what you said was great.

Hellman: Okay.

Plutte: So, try it again.

Hellman: Try it again. Public-key cryptography is a concept that confounds most people when they first hear about it, and so there is a physical analogy that helps get it across. Imagine we have a strongbox and I want to send you a message locked up in the strongbox, but we don't have a courier for exchanging the combination. So, I put the message in the strongbox. I put my combination lock on it and pass it through a bunch of people who might want to look at it to you. You can't open it, nor can they because they don't know my combination. When you get it, you put your combination lock on. So now, there are two locks on the box. It's now passed back. They doubly can't open it. When I get it, I can remove my lock, only your lock is now on. I pass the strongbox back. When you get it, you can take the lock off because it's only yours and you can read the message. That's basically how public-key cryptography works.

Plutte: Okay. I'm going to move over to now-- I'm going to ask you probably two questions just for our exit theater. In the exhibit when we walk out, there's people just giving short little thoughts about what the future might be or some other thoughts and I'll ask you a couple of questions that would be used in that exit theater at some point. Okay, what advice would you give to a young person just starting out in their career today?

Hellman: The best advice I can give a young person starting out today is to not be afraid of doing things that seem crazy. When I started work in cryptography, my colleagues all told me I was crazy and they had a valid point, but in hindsight, you'd have to say it was very wise to be foolish.

Plutte: Okay. Why do you think understanding computing history is important?

Hellman: It's important to understand history in all lights, computer history, political history, history of war because it helps you to see how to avoid mistakes in the future, how to reinforce approaches that have worked in the past, like not being afraid to do things that seem crazy.

Plutte: Okay. What do you see as the next big challenge for technology?

Hellman: The next big challenge that I see for technology is really a challenge for humanity. Technology has given human beings what previously was thought of as godlike power. The ability to create new life forms - historically only the gods or God is supposed to be able to do that. Human beings do it today. The ability to destroy a civilization and who knows, it's possible if we hit the singularity, as some people call it, that even computer crime could destroy civilization. Humanity's maturity level as a species, not individually is at best adolescent and so you have a bunch of 16-year-olds basically playing, having godlike power and that chasm between our physical power through technology and our maturity level as a species is a recipe for disaster. The thing that I actually focus on these days is nuclear weapons and how we really need to wake up to the fact that it's very dangerous to have fallible human beings with that kind of destructive power. So, I think that's the challenge.

Plutte: My last question is what do you think will be the next big thing?

Hellman: The next big thing is something that we're not even thinking about right now, that no one can envision right now. It's kind of like with public-key cryptography or cryptography as a commercial or academic research area. People thought it was crazy and so the next big thing is something that if someone described it to me right now, I'd probably say, "That's crazy." As just one small example, when

Google started, it started at Stanford. I knew about it as a great search engine, but I and one of my colleagues in computer science both agreed it's a great search engine, but how are you ever going to make money from free search? Well, we should have thought of our question as a question instead of a statement. If we had, we might be a lot richer today.

Plutte: That's all my questions. That's great. Thank you very much.

Hellman: Okay.

END OF INTERVIEW