

An Interview with
MARTIN HELLMAN
OH 375

Conducted by Jeffrey R. Yost

on

22 November 2004

Palo Alto, California

Charles Babbage Institute
Center for the History of Information Technology
University of Minnesota, Minneapolis
Copyright 2004, Charles Babbage Institute

Martin Hellman Interview

22 November 2004

Oral History 375

Abstract

Leading cryptography scholar Martin Hellman begins by discussing his developing interest in cryptography, factors underlying his decision to do academic research in this area, and the circumstances and fundamental insights of his invention of public key cryptography with collaborators Whitfield Diffie and Ralph Merkle at Stanford University in the mid-1970s. He also relates his subsequent work in cryptography with Steve Pohlig (the Pohlig-Hellman system) and others. Hellman addresses his involvement with and the broader context of the debate about the federal government's cryptography policy—regarding to the National Security Agency's (NSA) early efforts to contain and discourage academic work in the field, the Department of Commerce's encryption export restrictions (under the International Traffic of Arms Regulation, or ITAR), and key escrow (the so-called Clipper chip). He also touches on the commercialization of cryptography with RSA Data Security and VeriSign, as well as indicates some important individuals in academe and industry who have not received proper credit for their accomplishments in the field of cryptography.

TAPE 1 (Side A)

Yost: My name is Jeffrey Yost. I am from the Charles Babbage Institute and am here today with Martin Hellman in his home in Stanford, California. It's November 22nd 2004.

Yost: Martin could you begin by giving a brief biographical background of yourself—of where you were born and where you grew up?

Hellman: I was born October 2nd 1945 in New York City. I grew up in New York in the Bronx, until age 20, almost 21 when I finished college and came out to California, initially to work for the summer and then to attend Stanford University for graduate school. I did my Master's and Ph.D. All three degrees were in electrical engineering. The Master's and Ph.D. were at Stanford, the Bachelor's degree was at NYU. I graduated in 1962 from high school, from Bronx High School of Science. I completed my Bachelor's in 1966, and then in 1967 I got my Master's here at Stanford. Technically in 1969, but *de facto* in 1968, I finished my Ph.D.

Yost: Was there any point in your childhood years that you became interested in code and ciphers or was that later on?

Hellman: Later on. As a kid, no more so than the usual secret decoder ring kind of thing. Actually, I don't think I even had one of those. But I was always interested in science as a kid. My father was a high school physics teacher. I'm second generation born here—but because I grew up in the city, unlike my cousins, a lot of whom grew up in the suburbs, I

grew up much more in an immigrant type of culture and mentality. For example, I was free to roam New York City at a very early age using public transportation. I think I was six and my older brother nine when we would take the subway down to Manhattan to the Museum of Natural History and things like that. Maybe a year older, but we were very young. I look at my grandkids today and think, ‘Would I let them do this? No way!’ And in the same way, while my father was certainly an influence, there was a view that kids are fine by themselves. They would play by themselves. There was no Little League or anything like that. We would play stickball in the street or other games. And similarly, when it came to academics, there was very little interference or help—depending how you look at it—from the parents. And so it was more that my father had books on the bookshelf that I would pull down and read about things. Including one I remember, Ganot’s *Physics*, an old physics text from the 1890s that he bought. Obviously it was an antique even for him. And my seventh grade science fair project came out of that. So I was interested in science, but not particularly cryptography, and I loved math too.

Yost: Was it the breadth of electrical engineering, combining physics and mathematics that brought about your interest in this discipline?

Hellman: Well, in my later years, meaning starting my thirties and forties, I’ve developed a somewhat mystical view of life and a belief that our decisions are somewhat guided or pulled. But, looking at it totally from rational causes that got me into electrical engineering... My father was a ham radio operator in the 1920s, as was his younger brother by two years, who was my physics teacher incidentally at Bronx Science. Well,

my father was out of ham radio at that point in time. In high school, I think it was my senior year, I had become very interested in ham radio and I got my ham radio license. I think it was that more than anything that pulled me toward electrical engineering. I knew about science and math as a kid but no one had mentioned engineering. And so I think it was that that pulled me into electrical engineering.

Yost: In 1969 you took a job at IBM Research in Yorktown?

Hellman: 1968.

Yost: Oh, it was in 1968. Can you describe what type of research you were involved in at IBM?

Hellman: I'll answer the question first and then fill in some background. I worked in the Pattern Recognition Methodology Department. That covered a whole host of things, but there was some direct pattern recognition. For instance, we had a Post Office contract and we were doing Optical Character Recognition (OCR), trying to read zip codes. But I also was pretty much free to work on whatever I wanted to. That was in some sense my one ivory tower year because, well at MIT and even more so Stanford, there was just tremendous pressure, certainly you have to think of contracts and funding. Whereas at IBM there was pretty much this infinite budget to do what you wanted to do. And so I had a lot of time to work on whatever research I wanted. I did some work on the Bhattacharya Bound for example, which is in statistics. But I also got involved in

cryptography. When I look at the key factors that got into cryptography, you want me to go there?

Yost: Yes, please do.

Hellman: Sure, let me mention several of the key things that got me into cryptography. But before I do, let me tell you, the funny thing about going to IBM. With my father having been a high school teacher, my two brothers and I said the one thing we were never going to be were teachers, because you didn't make a lot of money. Although in hindsight it was a good living for the time. We wanted something different. When I was going for my Ph.D. I had a research breakthrough very early, in just my second year of graduate study. I really just had two years of graduate study when I finished and left here. My advisor asked me if I'd thought about teaching and I said—the short version is—'No thanks, I don't want to be poor.' He explained to me—and especially in 1968, which was kind of the peak of academic salaries relative to industrial—you didn't have to be poor as a college professor or university professor, particularly in a place like Stanford. You had consulting and other options. He turned out to be right. I made a good living as a professor, a lot of it on the side—consulting and things like that. So I actually had no interest in teaching. I was going to go into management and I saw the Ph.D. as a way to counter my youth, because I was ahead of myself. If I had the Ph.D. it would be a way to help quell questions like 'what can this kid do?' So it was a combination of two things that sent me to IBM. First, that was the way I'd been thinking. And second, I went from thinking who am I to try to do a thesis—an original contribution to research—to having it

being done in such a short period of time, literally six months total. And it essentially took a few hours. In hindsight, there was this one critical breakthrough. Given how fast things changed, there was no time to look for an academic position even if I had wanted to. I went to IBM Research and told them I might be looking into academic positions, and when MIT offered me one for September 1969, I went there. Coming back to the other part of the question is what got me into cryptography. When I was at IBM that was one of the key things, because IBM had just started its own cryptographic research effort that led to the Data Encryption Standard or DES, and had hired Horst Feistel. He was in the same department that I was, I mean you can see what a whole host of sins that department covered. And while I didn't work in cryptography, I'd have lunch with Horst and he taught me some of the early things about classical systems and helped me to see that some of these problems that sounded unsolvable could actually be solved very quickly. And it certainly increased my interest. So, that was one of the three key things that got me into cryptography.

Yost: Was it just Feistel or was it a team of researchers at IBM working on cryptography at the time?

Hellman: Well, Feistel was beginning to develop a team, Alan Konheim, and others. I certainly had contact with them later, but I don't know that I had contact with them that year. That year my main remembrance is of Feistel himself.

Yost: It was 1970 when you left IBM?

Hellman: No it was in 1969. I left Stanford in September 1968 to go to Yorktown IBM. I left Yorktown in September 1969 after just one year to go to MIT. And I taught at MIT from 1969 through 1971, two years, leaving in July of 1971 to come back to Stanford.

Yost: What led to your decision to leave IBM?

Hellman: Are you going to come back to the other things that led me to cryptography, or do you want me to tell about them now....

Yost: Please go ahead with the other factors that led you to cryptography first.

Hellman: The first one was in January 1969, so I had just been at IBM for a few months. I went to my first IEEE International Symposium on Information Theory, ISIT, as we abbreviate it. Information theory is the area that I worked in and cryptography is a branch of information theory, although I didn't know it at the time. In fact information theory owes its existence in many ways to cryptography, which I also didn't know at the time and many people still don't know today. There is still even a dispute about this. Anyway, at the January 1969 symposium on information theory, which was the first one I attended, I gave a paper on my thesis research. And the banquet speaker was David Kahn the author of *Codebreakers*, which at that time was a best selling book, a history of cryptography up through the 1950s basically, maybe into the early 1960s. It came out in 1968, I think. While it was not highly technical, there was a buzz surrounding the

book—cryptography catches people’s attention—and that caught my attention. So David Kahn’s book and his being the speaker at the symposium, working at IBM and having discussions with Feistel, and then the third key thing occurred at MIT, where I was from 1969 to 1971. Peter Elias was one of the grand old men of information theory—he wasn’t that old in those days, but in this work people did things at a fairly early age. Peter had been department chair of electrical engineering at MIT just before I came and he was head of the group that I worked on in communications and information theory. Peter gave me a paper that Claude Shannon had written, that he had published. He published it in 1949 in the *Bell System Technical Journal*, or *BSTJ*. I was aware, as any information theorist would be, of Shannon’s very famous 1948 papers that had two parts that introduced information theory, which was also in the *BSTJ*. When I saw how closely connected information theory and cryptography were, in fact cryptography was clearly a branch of information theory, and even though the paper on cryptography and information theory appeared a year after his more famous papers, there was a footnote that the paper had originally appeared in classified form in 1945. So actually, the work on cryptography preceded the work on reliable communications, which is what most people think of when they think of information theory. A lot of the arguments in Shannon’s work that are so beautiful, but counter-intuitive, that led to his results on reliable communication, make perfect sense when you think in terms of ciphers. And so that was the third key element.

Yost: What prompted your decision to leave MIT and return to Stanford?

Hellman: I had always had the intention and had hoped to come back to Stanford. There was something about California that intrigued me. It wasn't just the Beach Boys singing 'California Girls', although that was part of it. Again the mystical aspect, it was critical that I come to California for my own growth. My model is that European immigrants who came to New York broke a lot of the strictures and rules that existed in Europe. So the malcontents in some sense left Europe for New York, and the malcontents of the malcontents left New York for the West Coast. And there were fewer strictures and fewer rules. And I really needed for many reasons to break the ethnic consciousness of New York City. While it gave me a wonderful start in life and I'm grateful for it, it was important to move on. So, I'd always wanted to come back to California, and Stanford in particular, which I fell in love with. But when I got my Ph.D. my advisor, my Ph.D. advisor, Tom Cover, who still teaches here, said he'd love to have me back here. We both wanted me back here because we'd done some very good work together and work extremely well together. But he said, 'You know, Stanford has a major concern about inbreeding,' where you are hiring your own Ph.D.'s. It was believed that hiring your own resulted in people who thought like your faculty. And it was important for me to go away for several years and then hopefully come back. At the time it seemed like a stupid exercise that I had to meet; I had to jump through this hoop before I could come back. But it's one of those things where in hindsight it's a darn good thing that I left because two of the key things that led me to cryptography were Feistel at IBM and Peter Elias giving me a copy of Shannon's paper at MIT. And when I came back to Stanford, Cover was on sabbatical at MIT. In fact, I helped him locate a house, because just as I was coming back here, he was going out there. So my first year back here we didn't get to

work together. Our work grew apart, where the inbreeding concern actually evaporated. Which I think is a good thing for Stanford because while we did great things together, it was good that we went our separate ways. And if I had just kind of followed in his footsteps I never would have gotten involved in cryptography.

Yost: So in leaving IBM to go to MIT were you actually thinking about getting academic experience at another university with hopes of returning to Stanford?

Hellman: What happened was I realized you didn't have to be poor if you're going to be a University professor. And also I had formulated my goals in life...let's see...when I was an undergraduate, 1962 to 1966, I wanted to travel the world. I remember when we went traveling as a family as a kid our vacations were typically two weeks of camping in a tent at a state park. It was wonderful; it was something affordable. But the idea of staying in nice hotels and being able to go to restaurants and order a steak if I wanted, instead of a hamburger, sounded pretty good. My model was if you work in industry you get sent on business trips and they'd actually pay you to do these things. It sounded pretty good to me. I wasn't going to get married until I was thirty-five. I'd made that rule up in my head as a young man. But when Tom brought up the question of going into teaching... At this point in time I was married, I got married in March 1967 when I was twenty-one, and instead of waiting five years to have kids, as we initially thought, we ended up having our first child two years later in 1969. So when I was thinking about what to do in the summer of 1968 my wife was already pregnant. I said, 'Wait a second I have this model of traveling the world, that's when I wasn't going to get married until

thirty-five.’ I said, ‘Do I really want to be traveling the world or do I want to have more time with my family?’ Although, as it turned out later, you do just as much traveling as a professor at a world-class institution as you do in business. A lot of things had changed so the idea of teaching became more palatable, much more palatable to me. And when MIT came through with a good offer, though I guess an offer at MIT is a good offer by definition...I did think about it though because I took a cut in salary, on paper, of fifty percent. It wasn’t quite that bad but the guaranteed salary was about half of what I was making at IBM. I remember thinking, not just financially, but, ‘Why am I doing this? Am I interested in taking this job just because all of my colleagues would give their eyeteeth for this? Or is this really the best thing for me?’ And I decided it was the best thing for me, and it was, but I did have to go through that thought process. So, going to MIT that was kind of a thought process, but I always had in mind that I wanted to come back to Stanford, if possible.

Yost: And at Stanford, was a fair amount of your research in cryptography in your first few years there?

Hellman: No, my thesis was on learning with finite memory and was published in the *Annals of Mathematical Statistics*, which was subsequently broken into the *Annals of Probability* and the *Annals of Statistics*. Anyway, in my thesis topic, you have two probability distributions and you have an unlimited number of observations, independent and identically distributed according to either distribution one or distribution two. And it’s well known—it was well known at that time—that without memory limitations the

error probability went to zero exponentially, in fact the Bhattacharya Bound that I mentioned before was related to that, how fast it goes to zero. As you get more and more information you can distinguish between the two hypotheses. For example, if I have a coin, this is the very simplest example, a coin that is biased seventy-five percent toward heads and only twenty-five percent toward tails or vice versa...It's kind of like you made a trick coin and then forget which way it was stamped and now you're trying to decide which way to bet. So, you do some tosses before you go bet with people. And I think you can see that after tossing it a hundred times the chances are very, very small that you'd make the wrong decision because you'd expect seventy-five of one and twenty-five of the other. It might be as bad as sixty/forty, but the chance of it reversing itself is extremely small. With a thousand tosses the probability of error is even smaller. But the problem that I treated and worked on in my thesis was what happens if you have a finite state memory. For example let's say you have a two-bit memory. That's four states. You have states one, two, three, and four. And so you can't remember the last hundred or thousand tosses, you can only remember, in some sense, the last two tosses—if you just use one bit per toss. But there were better things to do than that, and I was able to come up with a lower bound on the error probability as a function of the number of states and the distributions. And then actually come up with a machine that could epsilon-achieve it. You can only achieve the lower bound arbitrarily closely. But you could get as close to it as you want. So I was working more on learning with finite memory, a little bit on Bhattacharya Bound, which was not finite memory but related to the same problem of how hypothesis testing goes with observations. And I started to move into cryptography very slowly initially. Well, to fully answer that question, I think I gave my first talk on

cryptography in about 1973. And looking back on it and looking back on the report that I had at the time, it wasn't a published paper but it was a technical report, my ideas were very naïve in hindsight. But when you're developing a whole new area, and even though a lot was known within the classified literature, that's understandable. Well another thing IBM did for me... The fact that IBM was spending a huge amount of money on cryptography told me there were commercial applications for it. I could also see the growing use of computers in communications. When people discouraged me from working in the area, which almost everybody did, my response was, 'Well, what's known in classified literature is not available.' Because that was one of their arguments, and the other was 'How can you hope to discover anything new?' I said, 'It doesn't matter what's known there, it's not available for commercial use, and commercial needs are growing.' And also from a point of view of credit, there's no problem because the rules are clear: the person who gets credit is the first to publish, not the first to discover and keep things secret.

Yost: Was the ARPANET a factor in your view of the growth of computing and communications. Were you aware of it and an early user of the ARPANET?

Hellman: Well, the ARPANET, the first communication—I think from BNN to SRI—I think was probably 1969. But we did have access to the ARPANET early on. Now whether it was the mid-1970s or early-1970s or late 1970s is hard to remember. In fact, I was just going through something recently where—you've got to be very careful because it's so hard to remember how things really were. I saw a Groucho Marx TV show from

1962 and it was in black and white and it looked like it was from the early 1950s to me, but that's what TV was in 1962. So it's hard to date things precisely that far back. But I was certainly using the ARPANET for email to communicate. For instance, a student from Israel went back to Israel while we were working on a paper. It was just fantastic to be able to, instead of using mail or try calling him with the time difference problem, you could just send an email where I could just say, 'Let's rewrite the paper this way' and have him respond back and have it cost us nothing. So certainly it was much before the Internet became the Internet when I was aware of the promise of computer communications networks. I was seeing communications and computations coming together. But it was obviously in a lot of other places too, I think. Super computers were being made available, maybe over the ARPANET, to researchers. And ATMs came in the 1980s. We were using communications to do financial transactions.

Yost: During the first half of the 1970s did the National Security Agency (NSA) ever try and formally recruit you?

Hellman: Sure. It's interesting, early on when my work was, I now say in hindsight, naïve, but still I think it showed promise. At the conference where I'd given a talk, someone from the NSA—and the person always identified themselves as Department of Defense, they had a simple substitution cipher. The CIA was always 'US Government' and NSA was always 'Department of Defense.' So you knew who was in the CIA and who was in the NSA, they just couldn't say it. Individuals in the NSA asked me if I'd want to do some consulting for them and I said, 'I'd be interested, the only problem is I

want to be free to publish whatever I came up with, and from what I understand that would not be the case if I consult for you, even if I do things separately.’ I had had normal security clearance but I knew crypto-clearances were much worse in terms of the strictures. With the normal security clearance that I had for my consulting for example, if I did work in a related area but did not build on anything classified, I didn’t need to get permission to publish it. On the other hand, in cryptography, my understanding was, and the NSA people who approached me agreed, that once I had a crypto-clearance I would have to get permission to publish anything I’d worked on.

Yost: Can you describe your first meeting with Whitfield Diffie and what it meant for your evolving ideas on cryptography?

Hellman: Sure, actually a lot of that first meeting was in this very room. First of all it seems we need a little background. I would go back to Yorktown, IBM Research in Yorktown Heights, and especially as I got interested in cryptography. I would meet with Horst and other people in the department. And I went back and I gave a talk—informal not a big thing, but just to that little group—on my growing thoughts on cryptography and the need for a theory of cryptography. And it’s interesting, my remembrance of the meeting was that they were somewhat discouraging. Because what had happened is, we didn’t know this, but they had developed DES and they’d tried to break it and weren’t able to break it. And the thing is about to be published, maybe a year later in the Federal Register as a proposed standard. And so IBM management was telling them, ‘Hey look, you’ve done everything you need to do in cryptography. What more is there to do? The

big problem is operating systems security. There we've got a million holes. I mean cryptography's a simple problem and we've solved it. We've got a secure system for commercial use.' And so they were somewhat, you know, maybe a little depressed about doing research in cryptography or discouraging to me, some combination of the two. And also a secrecy order had descended on them. Anyway Whit, I believe within a month or two after this, he was traveling around the country trying to learn about cryptography. He left his job at the AI lab here at Stanford because he wanted to learn about cryptography. I think he'd come into a small inheritance that allowed him to do this. And the way the AI community works, it doesn't take much money to travel around the country because you can find a place to bunk with almost any other AI person. I mean there's this community of AI types. So, Whit also stopped at Yorktown where he knew some people and gave probably a somewhat similar talk to mine and they gave him a somewhat similar discouraging response. But Alan Konheim, who was at that time the head of the group and now is a professor at UC Santa Barbara, said kind of an offhand comment at the end from what Whit's told me. 'Well when you get back... Hellman's been here and said kind of similar things. When you get back to Stanford you might look him up.' So, I believe it was the fall of 1974, although Whit is much better at identifying the timing, he probably has a record of these things and if you have his interview I would go by that. I get this call that says something like, 'Alan Konheim suggested that I should look you up when I'm back in the Bay area.' He was up in Berkeley. In those days he and Mary, now wife then girlfriend, couldn't stand Stanford. It was too clean and not urban enough. They needed something grittier, so Berkeley was their base of operation. He said he was coming down and I said, 'Sure, I have half an hour available.' We met and as I

mentioned, almost all of my colleagues including my former advisor Tom Cover discouraged me from doing work in cryptography with two simple arguments: Basically you'd be crazy to work in cryptography because NSA has a huge budget, how can you hope to discover anything they don't already know. And I've already answered why I thought that wasn't an issue. And the other was if you do anything good they'll classify it. So I was working in a vacuum, with discouragement from all my colleagues. And in spite of my maverick approach to life, I think it was probably getting me down a little bit. Whit shows up and in the first half hour it's clear that he and I are thinking along very similar lines and are excited about possibilities and not discouraged like the IBM group. So that 'half hour meeting,' which probably started about two in the afternoon ... at about five o'clock or four-thirty I say, 'Look I promised my wife I'd be home to watch the kids. But if you don't mind coming back I'd love to continue the conversation.' He called Mary and had her meet him here and we had dinner together and then we talked until probably eleven o'clock at night. So, yes, I remember my first meeting with Whit. It was a mild epiphany, finding an intellectual soul mate in this.

Yost: And soon afterward he became a graduate student of yours?

Hellman: I don't know about soon after. Whit had a Bachelor's degree from MIT, I believe in mathematics, but no advanced degrees. He was traveling around the country. As I said, I wanted to keep him here. I had a small amount of money that I could pay him as a research programmer with a Bachelor's degree. That's all that I could give him, but it was a little bit of income and it kept him in the area. After I don't know, maybe three to

six months of this, or maybe shortly thereafter or maybe longer I don't know exactly, I said to him, 'Look,' ... We hadn't yet done public key cryptography but there were other things. The work was progressing much faster with the two of us working together. In fact, in that first meeting we had some similar ideas where one of us would say something and the other would respond, 'Yes, I'd thought of that too' and then we'd reverse roles on the next topic. And then there were other things that I said that he hadn't thought of and vice versa. So I said to him, 'Look, you've done the hard part of a Ph.D.—you're well along the way on a thesis. What I'm paying you is about what I'd pay you as a research assistant.' I didn't have a lot of spare money. I forget how his undergraduate grades were but with what he'd done, it was clear my recommendation would get him into the program. And so I said, 'Let's get you a Ph.D.' Unfortunately, that didn't work, but not for the usual reason. Many people who start but don't finish a Ph.D. are ABD (all but dissertation) since that's the hard part for most people. Whit, on the other hand, was ABC (all but courses). We never actually filed the dissertation, but with 'New Directions in Cryptography' and the other papers we published, clearly he had the basis for a first rate, first magnitude Ph.D. What happened? Whit is very independent and doesn't like people telling him what to do. At the time it seemed a little strange to me, but you know, I couldn't go back and do a Ph.D. now. I couldn't go jump through all the hoops I jumped through. Taking a stupid language exam that really served no purpose because it wasn't strenuous enough to make sure you could read papers in the language, but I had to take several days of my time to review my French from high school. It was a hoop that you had to jump through. One thing I'm proud of when I was on the faculty here is that I got rid of that exam. I said, 'Either we need to strengthen it and make it really mean

something or we need to get rid of it. Right now it's just a waste of time.' Whit was unwilling to do that kind of crap, but at that point in my life, I was. So he was ABC, all but courses. I was very glad when Jim Massey, a mutual colleague of ours, who was at ETH (the Swiss Federal Technical Institute), got him an honorary Ph.D. And he deserved a doctorate.

Yost: When the Federal Register announced in March 1975 a request for proposals for a data encryption standard, what was your initial response?

Hellman: Actually, the RFP was before March 1975. March 1975 is when the DES was proposed as the standard, so the request for proposals was in 1974. Because they had to make it look like they were requested. And who knows they might have actually considered another algorithm if there had been a reasonable alternative proposal. But since the selection process was not open, we'll never know. DES was far ahead of its time in the commercial world and, other than the key size issue, it was very strong. In fact no one's broken the thing other than by exhaustive search. There have been minor cracks in it, but over an almost thirty year time period no one has found a real weakness in it other than its key size, and that's amazing. What was the question again?

Yost: Well, I misspoke. I'm interested in your initial reaction to DES as the proposed NBS standard.

Hellman: Whit and I took a very close look at it. We were familiar with IBM's earlier work, which appeared in technical reports out of IBM. And *Scientific American* had a 1973 article by Horst Feistel describing what IBM called Lucifer, which was the predecessor to DES. Lucifer, from what I now understand, really covered several different systems. DES was very much related to these earlier IBM systems with a few changes, which were actually quite smart. But the one thing that became clear pretty quickly was that the key size was at best marginally adequate and, at worst, inadequate. We were glad to see the DES proposal, but we also had a major concern about the key size.

Yost: At what point did you think the NSA was involved in manipulating or setting the key size?

Hellman: Well, I think the request for comments on the Data Encryption Standard proposal said it had thirty or sixty days for comments, maybe ninety days at most. Whit and I talked about it a lot and essentially he wrote it up, I think, the initial version, which I forwarded on. Later on it was hard to get him to write things up, but he did write that. Initially he did that and I forwarded it on. This initial thing that we put in had a few questions in general. There were three major concerns that we had. One was the key size, the other was the fact that the design principles were not made public. The design was public, which was a great step forward. But how they came up with the design, why they thought those were good structures, and why they had huge tables of numbers. How did they select those tables of numbers or could there be a hidden trap door in the tables that

allowed them to break it? Because one thing we were very aware of was that, NSA was on our mind here, we knew they were advising NBS. In fact, the two people at NBS who I was dealing with the most closely on this whole thing, who were taking the comments, had both come over from NSA very recently. In fact, I called an uncle of mine who had been in government service and he said, 'Oh they've colonized NBS.' Whenever one agency has a problem with work going on in another agency, the best way to control it is to move some of your people over there who really have your interest at heart. So the design principles concerned us. The double bind NSA was in was they had to put out a standard that was very strong, because if it was broken not only would NBS, now NIST, get a black eye, but NSA would get a black eye because they'd been advising NBS. They can't put out something that's easy to break. Plus all the commercial American data would be at risk. And yet the other side of the problem was it was pretty clear they didn't want a standard they couldn't break. Or they would be in danger with a standard they couldn't break because it could be used by third world countries. We weren't so much worried about the Soviets. The Soviets were very good in mathematics and were therefore presumably very good in cryptography. The general belief and consensus of the community was that we couldn't break the Soviet codes and they couldn't break ours. But third world countries were the real gold mines of information and often we could get information on Soviet intentions, or they on ours, by information going through some third world nation that was an ally. And this problem actually predated the data encryption standard. In the military you have the same problem. You want to give your soldier in the field a very secure cipher for use in getting orders, yet if the cipher is captured by the enemy, you don't want the enemy to be able to use it. One idea that had

started to develop, which led to public key cryptography, was the idea of a trap door cipher. A trap door cipher is one that appears very secure, in fact no one can break it except the designer and the designer can break it only because he's built in trap doors. We came up with the idea of trap doors from the Hardy Boys or other mystery books I'd read as a kid. There was some tomb I think they were stuck in, with a million bricks. And if you pressed on the right brick a door opens and you'll survive, otherwise you die of thirst in this tomb. The designer knows which brick to push and can survive. But anyone else, except maybe the Hardy Boys, who miraculously figured it out I'm sure, will die because they don't know which brick to push. The fact that the design principles of DES were secret was a concern to us. Now I'm not sure whether the trap door cipher idea preceded our concern with DES or followed, or the two developed at the same time. But you can see how those would come about and how even in the military prior to DES we saw that they had this problem. I've said many times that a trap door cipher is a General's dream. This is because you can give your forces absolute security, and yet, if it is used by the other side, they get absolute insecurity.

Yost: So the trap door is one critical factor leading to the concept of public key, what are others?

Hellman: I have a talk I've given recently on the evolution of public key cryptography, and I start off by saying that public key cryptography is seen as revolutionary and of course it is a revolutionary concept. I remember when I first described it to Feistel... Let me just back up a little bit. Even today many people will develop cryptographic systems.

They will come to me and say, 'I've got a great system, it's totally unbreakable, you just have to keep the design secret. You can't tell people how it works except the people who are using it.' Because systems can be captured they can be compromised, so a general rule in cryptography is that the general system even if it is kept secret or there is an attempt to keep it secret, it must be considered public information. So when you try to break it to assess its security you have to assume its design is known. All security must reside in the secrecy of the secret key. That was a great step forward in cryptography when it was enunciated by Kerckhoffs in the late nineteenth century. Why, then say 'public key cryptography,' and just the name sounds like we're going backward. So, when I first described it to Feistel, in kind of a hurried way because he had a doctor's appointment, he said, 'You can't do that.' So what were some of the other things that led to public key cryptography other than the trap door cipher? Oh, I should point out that the reason a trap door cipher can be made into a type of public key cryptographic system. If you can generate trap door ciphers fairly easily, if you have a kind of a meta trap door cipher where you can just churn out trap door ciphers as frequently as you want, every time you and I want to exchange a key I generate a trap door cipher. I tell you what it is and because we're using a public channel everyone hears what it is. You encipher a message with a secret key that you picked and send it. I can break it because I'm the designer and know the trap door, so I get the secret key that you picked. You and I now share a secret key. Everyone else, even though they know the cipher system, they weren't the designers; so they can't break it. We now have public key exchange with a trap door cipher. So trap door ciphers are very closely connected to public key cryptography. Some of the other things, even Kerckhoffs' rule that the key must be kept

secret and everything else must be public, well it sounds, as I just explained, counter to the idea of a public key. Of course we get around that because only half the key is public. There are two keys and one's public and one's secret. The development of public key cryptography is, in hindsight, part of the same revolution because it is taking what was previously thought needed to be secret and making it public. Kerckhoffs demanded that the design of the system be public. And we went even further and said the enciphering key should be made public, with only the deciphering key staying secret. Other things in hindsight, you see, so again I don't know, it's hard to say what led us to public key cryptography. But you can see that, in some sense, we were almost being channeled in that direction, and what I say when I give this talk on the evolution of public key cryptography, I say, 'Well, initially your reaction may be *how did they come up with something so earth shattering, so ground breaking, so different from what was before?*' But after I describe all the threads that were leading us there consciously or subconsciously, 'I hope your reaction will be, *why did it take them so long?*' And one other thing is the idea of a simple substitution cipher. If you look at a simple substitution cipher there are really two keys because when you want to encipher it helps to have the plaintext in alphabetical order and the ciphertext alphabet in scrambled order. When you're trying to decipher it's better to have the ciphertext in alphabetical order so you can quickly find the letter you're looking for and see what its plaintext equivalent is. So there is again the idea of two keys, one for enciphering and one for deciphering. Of course with a simple substitution going from one key to the other is very simple so you can't make one key public and keep the other secret. But, there again is the idea that there could be an enciphering key and a deciphering key that are different. And then there's

one other key thing, not that led us to the concept, but in terms of coming up with what's now called Diffie-Hellman key exchange. And as I explained to Simon Singh and he explains in his book, *The Code Book*, if you're going to put names on it, it should be called Diffie-Hellman-Merkle key exchange, since it's actually based on a concept of Merkle's. We give him credit for that in the paper, but it was in a paper by Diffie and Hellman, so it's called Diffie-Hellman key exchange. John Gill, Professor John Gill here at Stanford, had just done a Ph.D. in mathematics at Berkeley and came here—I was hired in 1971 here, he came on in 1972 or 1973. I went to John because he worked in areas that were more related to this kind of a thing in a way, complexity of the computation. And I said, 'John we're looking for functions that are easy to compute but hard to invert.' That's called a one-way function. But that was the simplest cryptographic entity in some sense and I was using the approach that is usually a good approach although not always, of trying to simplify the problem down. So I didn't go to him and say, 'Can you come up with a public key cryptographic system?' Instead, I said 'Let's start with the simplest thing.' And John suggested exponentiation in modular arithmetic. And exponentiation in modular arithmetic is the basis of the Diffie-Hellman-Merkle key exchange, it's the basis of the RSA public cryptosystem, and it is at the foundation of the Digital Signature Standard or Digital Signature Algorithm. So John Gill is one of the unsung heroes of public key cryptography because it was his suggestion that really is at the basis of all the current systems.

Yost: Did Don Knuth suggest to you factoring the product of large primes?

Hellman: Oh, no one had to suggest that to us, I mean factoring was such an obvious one-way function, I think anyone who knew anything about number theory would look at that almost immediately, although of course, it took some time before Rivest, Shamir and Adleman figured out how to use the difficulty of factoring as the basis for a public key system. But Don Knuth was a very helpful person to talk to, and not just in cryptography. In a Ph.D thesis of one of my students, a simple phone conversation with Don was the key thing that led to solving that problem. He was just a fabulous resource in many areas.

Yost: You spoke of Merkle's work as having a fundamental impact. Can you describe the dynamic between you Diffie and Merkle, of how you worked together?

Hellman: I smile when you say Merkle, I mean Merkle is just someone who makes you smile. He's a comic. He comes and plops down in your office—have you met Ralph?

Yost: No, I haven't, but I hope to interview him in the future.

Hellman: He plops down in your chair and says, 'Hi!' I remember, this was after the discovery of public key cryptography, maybe fifteen years ago, he comes into my office and plops down and says, 'Hi, I'm building a human brain.' He's one of the stars in nanotechnology. Building human brains and repairing human brains on dead people so you can bring them back to life some time in the distant future is one of his passions.

Whit had a friend in Berkeley who knew of Ralph's work. Ralph had a Bachelor's degree in computer science at Berkeley and was then working, this was 1975 probably because I

met Whit in 1974. It was probably a year later, in 1975. I'm pretty sure it was Whit who told me about a Master's student at Berkeley, Ralph Merkle, who's also interested in cryptography and we exchanged some letters and I went up to Berkeley, sometimes with Whit, sometimes without, and met Ralph. And it was clear it was a meeting of the minds, again an intellectual soul mate. He was very interested in cryptography and, I believe, by the time we had met him he had already developed his puzzle method for public key distribution. Public key cryptography encompasses public key distribution, public key cryptosystems, and digital signatures. The idea of a public key cryptosystem is one that Whit and I developed here at Stanford. Public key distribution systems, which are closely related but different, Ralph had developed independently at Berkeley, and even a little before us I believe. Digital signatures all by themselves, it wasn't until El Gamal's thesis, he was a student of mine, that you could have a signature algorithm but it couldn't do privacy for you. And that was later, that was in the eighties. So Ralph had this idea for key exchange and he even had a method for doing it that wasn't practical, but that was on a very firm theoretical ground. I was very taken with him, as I believe was Whit. And it was a little after 1975. It was the summer of 1976 that I kidnapped him down here and had him work. I forget whether I hired him at Stanford as a summer student or whether I gave him some consulting projects—or if he worked on some combination of the two. But he came down here in the summer of 1976 and worked with me. Now what's called Diffie-Hellman key exchange is a public distribution system which is Merkle's concept, not ours, and that's why I feel the names on it should be Diffie-Hellman-Merkle. I encouraged him to come here to do his Ph.D. under my direction. Nobody at Berkeley was working on cryptography. Ralph is fond of pointing out that he put in two proposals

for a term project at Berkeley, one was to develop public key distribution and the other was something much more mundane. But it wasn't clearly stated and you have to give Lance Hoffman a break, who was the professor who liked the second idea better. Lance is a very good guy, he's got fifty or sixty or eighty proposals to read through and Ralph hadn't described it very well. But Ralph in typical fashion went with the first idea. Ralph, from a theoretical point of view, is probably one of the most brilliant persons I've met. Also he did come down and do his Ph.D. under my direction. Oh, one other short thing that is fun. He said, 'I can't afford to go to Stanford.' I explained to him that, with a research assistantship, he would get as much of a salary here as he would be getting at Berkeley as a TA, and tuition's paid for by the RA.

Yost: Can you discuss the initial reception to your development of public key cryptography and the impact that you saw it had on the computer security area as well as computer science more generally?

Hellman: Well you're probably talking about the "New Directions in Cryptography" paper, which appeared in November 1976. We had the concept of public key cryptography for about a year at that point would be my guess, I'd have to go back and check. And one night I came up with this alpha to the $x_1 x_2$ thing $[a^{(x_1 x_2)}]$ that was clearly joint work with Whit because we'd been talking back and forth and, just like the actual first enunciation of public key cryptosystem was from Whit, but that too was joint work. Somebody might say something first but we were interacting like that. We built so much on each other's ideas. Whit and I had been working on a paper called "New

Directions in Cryptography” for the *Information Theory Transactions of the IEEE* and Jim Massey, who I mentioned before got his honorary doctorate from ETH, was the editor of the *Transactions*. Let’s see the short version. There was another ISIT, International Symposium on Information Theory, in Ronneby, Sweden in June 1976. I’d come up with the alpha to the $x_1 x_2$ scheme I think in May 1976 so it wasn’t in anything that was in the published proceedings because the papers are submitted nine months in advance or something but you can always add new ideas, so in the oral presentation I included this alpha to the $x_1 x_2$ scheme that’s now called Diffie-Hellman.

TAPE 1 (Side B)

So I went to Ronneby and gave the talk. Jim Massey was there and Whit and I had actually become discouraged about the paper because we were trying to not just do public key cryptography, we were trying to lay the foundation for a whole theory of cryptography. Much as he and I had talked at IBM Research and been discouraged on, like I mentioned earlier. We’d been working on the paper for probably a year and we said that we felt that it wasn’t coming together well so we sent it off, we felt that the reviewers would give us criticism that would get it back on track. Well the reviews came back quite positive. And when Jim Massey heard my talk at Ronneby with the alpha to the $x_1 x_2$ scheme, we actually had a workable system. Or what appeared to be a workable system because you never know, it’s got to be out there for a while and someone has to try to break it, a lot of good people have to try and break it and fail. Jim Massey said to me, ‘If you can get this in the paper and get it back to me in July I will have it in the November

Transactions,’ which is unheard of speed in publication. So we in fact put it in, but because the paper was much more than that, Merkle wasn’t a co-author. Although we credit him with the public key distribution concepts. And we called it alpha to the x1 x2, not Diffie-Hellman. And so that’s how the paper came to be. You asked what was the reception of the paper? Well the reception of the paper? There were two aspects. I mean the editor was ecstatic—oh and by the way the RSA paper that appeared a year and a half later roughly had the same thing. I was one of the reviewers on that paper, the editor took a very unusual tack. The letter he sends out with the paper, instead of saying ‘please send me your review’ and being very objective, he says, ‘This could well be the most important paper *Communications of the ACM* will ever publish, please get your review in quickly.’ And again it was like a three-month publication delay instead of a one and half or two and a half year delay. Unfortunately Ralph’s paper that appeared in the *CACM*, for various reasons, took the normal two years. So, even though it appeared after our paper, if you look at the submission dates, I’m pretty sure it was before. Ralph really has never gotten the credit he deserves. In fact one thing I hope to do in this conversation today is mention some of the people who deserve credit that haven’t gotten as much as they should. Ralph’s gotten some, but not as much as he should. John Gill’s gotten almost none, although we credit him in our paper. And John’s an interesting guy in many ways. He’s one of the first black graduates of Georgia Tech. You may be a little young to remember how fiercely integration was resisted in the South. So the reception. The reception from the open community, you know the non-military community, was ecstatic. The reception from NSA was apoplectic and it wasn’t just that paper, we also had the DES key size issue that I mentioned briefly before. Those two issues in hindsight, those

two together, really gave them apoplexy. A fifty-six bit key size, which is what DES has, that's roughly ten to the seventeenth keys, a hundred thousand million million. We had had a paper around the same time we were arguing that the key size was inadequate. And, if I put myself in the shoes that I had put myself in, which was the self appointed security officer for the public, a fifty-six bit key size was inadequate. The short version is we had estimated you could build an exhaustive search machine that could search all two to the fifty-six keys in a matter of a day at a cost of approximately ten thousand dollars. We may have been a little bit optimistic, but Moore's Law was involved, so as we pointed out, even if we're off by a factor of ten and it's a hundred thousand dollars a solution, that difference would be erased in five years time because computer costs were coming down so rapidly. So a fifty-six bit key size is totally inadequate if you're going to be a security officer for the public, as I self-appointed myself. On the other hand, I tried doing the opposite thing, not at the time, but as I become more mature, I've thought about 'What if I was someone at NSA concerned with communications intelligence?' I would be going, well... I would be having apoplexy. You can fill in the blanks. Because, even without public key cryptography, fifty-six bits is a lot. Because at ten thousand dollars per solution, that's a lot. Before DES, and actually even after, most stuff was going in the clear, unencrypted. And when it is in computer readable form they could search, today, billions of words for a dollar, and even back then, millions of words for a dollar. All of a sudden DES is going to cost them ten thousand dollars per key. And, with public key cryptography, people using DES can change keys frequently and it is going to cost them ten thousand dollars per key. That's a huge change. And when you look at the kind of vacuum cleaner intelligence operations that they were using, even a fifty-six bit key size

was a major, major give on their part. And now you have public key cryptography coming into it where people can change keys as often as they want. Because prior to public key cryptography you'd need to send a courier or registered letter for a new key and people wouldn't do that but once a year if that often. Once a month maybe if they're very security conscious. Now you can do it every few minutes. So the two papers together I'm sure gave them apoplexy.

Yost: When you gave that paper at Ronneby, Sweden was there any concern, did anything cross your mind about giving that information abroad, that it might pose problems with the export law?

Hellman: In 1976 it hadn't yet gotten into the legalities. But it was clear by January 1976 we'd hit a hornet's nest within NSA. And the basic thing we were told by people at NSA was, 'You're wrong,' this was initially on the key size issue, 'fifty-six bits is really secure, you can't build an exhaustive search machine.' And they had argued this in writing to us that we were off by many orders of magnitude. But what they were saying by January 1976 was, 'you're wrong about the key size.' We didn't even have the public key cryptography really worked out. 'You're wrong but please shut up. What you're doing will cause great harm to national security.' Now you have to put this in context. Right now we're at war with Iraq. There are terrorists. But 1976 was a few years after Watergate. There's a movie, a great movie called "Hopscotch" with Walter Matthau in which there's a real S.O.B., CIA guy. Walter Matthau was a good CIA guy, but his boss was a real S.O.B. He's trying to cover up CIA mistakes and, when someone asked him

why he's doing something, he says, 'Matters of national security. Strictly on a need to know basis.' And the guy says to him, 'You know, that phrase has lost a certain amount of meaning.' And this was in those same post-Watergate years. So I wasn't too worried that I was doing harm. I did think about it, but we concluded, or I concluded, that the United States was the most computerized nation in the world. So we had the most to lose by insecure commercial encryption. The Soviet Union was the least developed in computing, it was so far behind us in computerization that they had so much less to lose. Our conclusion, at least my conclusion, was that NSA was not concerned with National Security. They were concerned with job security. I have a different view now, but that was the simple version back then. So at Ronneby, no I didn't have any concern about giving the paper. But the next year I had some concerns from a legal point of view.

Yost: You presented papers of a couple of your graduate students?

Hellman: What happened was, you'd have to check when Martin Gardner's column on RSA and our work on public key cryptography was in *Scientific American*. I think it was the summer of 1977. The MIT guys, Rivest, Shamir, and Adleman, said anyone who sends a self-addressed stamped envelope to them they'll send a copy of the report. I get a letter from the IEEE, which is the main electrical engineering professional society. I was on the Board of Governors of the IEEE's Information Theory Group, now the Information Theory Society. And it's interesting. I get a letter as a member of the Board of Governors, but not everybody on the Board of Governors gets it. It is from the IEEE saying, 'We received a letter from a concerned member' –who happened to live in

Maryland, and who we later determined happened to work at NSA. It was from his home address saying that he was concerned that the IEEE was breaking the law by publishing certain papers that were in violation of the ITAR, the International Traffic of Arms Regulation, of which he sent a copy, including penalties—which I believe were a ten thousand or fifty thousand dollar fine and up to five or ten years in prison. The basic idea is we don't want American companies exporting weapons to nations without a license and we don't want them exporting the technical details on how to make weapons without a license because that's tantamount to exporting the weapon. But the ITAR defines, and this guy pointed out, any papers related to cryptography are defined as weapons of war. So he claimed we were in violation of the ITAR and the IEEE was in violation of the ITAR by publishing certain papers. He never mentioned me by name, but he quoted about six issues, not papers, but six issues of IEEE publications that violated the ITAR. He never said which papers, but I had a paper in every single one of them, or all but one.

Yost: And that includes the 1976 “New Directions”?

Hellman: Yes, certainly. And the paper on the key size issue, yes that was in the Computer magazine of the IEEE. So my take on it, he's saying Hellman's a troublemaker, shut him up. He never mentioned me by name. It's interesting the IEEE, although they clearly knew that that's what he was saying since they sent it to me but not everyone else on the Board. It's funny how this works when people deal with cryptography everyone gets very weird. They talk in code. It's really really funny. I sent a copy of the letter to Ron Rivest because he and I were in close communication for some

time prior to this. We were exchanging papers and anything relevant. So I sent it to Ron, he took it to MIT's attorneys and I took it to Stanford's attorneys because I was concerned both in terms of protecting myself and also my institution. Oh, what the IEEE said in their response was, 'We're well aware of the ITAR but it is impractical for the IEEE to be the arbiter. It's always been our view that it is the author and his or her institution (actually in 1977 it probably said his institution) who have the responsibility to ensure they are not in violation.' So I took it to Stanford both because Stanford might be in violation and also because I was kind of afraid to defend myself if I were prosecuted. MIT's attorneys told Rivest to stop sending out copies of the paper for a while. Stanford's attorney, General Counsel John Schwartz was very supportive and I remember the conversation very well. He said it was his opinion after reviewing it that, if the ITAR was construed broadly enough to cover our work, it was unconstitutional. But the only way to determine that is in a court case. You can't go get things predetermined. So he said if I were prosecuted the University would defend me. But he had to warn me, if I were found guilty, they could clearly not go to jail for me if that was part of the sentence. And they couldn't pay a fine. Because it's an interesting thing, they can defend my right to do my research but once it's determined, if it's determined, that I'm a criminal, you can no longer aid and abet criminal activity by paying fines or anything else. That's assuming they could not appeal. And Schwartz also said ... We had two papers in October 1977 at the Cornell ISIT. Ralph Merkle had a paper and Steve Pohlig had a paper with me, joint papers, both students of mine. He recommended against the students giving the papers for two reasons. He said if there is a prosecution, it was questionable whether the University could defend a student. I was an employee. I was an agent. I brought contract money into

the University. He also said from a separate, a practical point of view, I was a tenured professor and my career could withstand a multi-year court case, whereas the students were starting out in their careers and it could be much more detrimental for them. I left it up to the students. I left it up to Steve Pohlig and Ralph Merkle, and initially they said, 'We need to give the papers, the hell with this.' It's interesting people have asked me and sometimes talked about how courageous I was to do this. And it's one of those things where it's not courage. You're confronted with a situation where it's so clearly right to do it and you find the courage in yourself. It's just no question and the same with the students, their initial reaction was unquestioning, 'No we'll give the papers.' Their families had other ideas however, and eventually they deferred to their families' concerns. So, at the ISIT, I gave the talks, but had the students stand next to me and explained the situation to call attention to and credit their work even though they were not giving the talks.

Yost: Were there civil liberties groups or other key individuals that came to support the public key encryption issue? Certain journalists?

Hellman: Oh the press. With the freedom of publication issue, the press was all on our side. There were editorials in the *New York Times* and a number of other publications. *Science* I remember had covered our work, and was very helpful. David Kahn had been helpful early on in the key size issue. We were unknown at that point, he was the big name. And when we realized that we had a political problem on our hands, with the key size, not a technical problem, no amount of technical arguing was going to make any

difference. We eventually decided to go with a political fight, so we went to David Kahn who had more stature than we did in 1975. He first had to check us out. And when he checked us out he wrote an op-ed in the *New York Times* in support of our position. We had plenty of support; it was just a ground swell of support from within the press. As you would imagine with the freedom of publication, the whole idea of ideas being “born classified” was not very appealing to them.

Yost: At the NSA’s request, the American Council on Education formed a committee in 1980. Can you describe the nature of the discussion of the committee.

Hellman: Oh, the ACE committee. I’m not sure I was a part of that. [Note added in proof: I was.] But I do remember the ACE thing and I remember some key things about it. This is the one where Admiral Inman came in and was trying to get them to recommend that certain areas, including cryptography, had “born classified” aspects. The whole approach that he was taking and NSA was taking was one of, ‘If we have a law then it’s going to work.’ And an interesting thing happened around this time. In 1980 I began to get involved, and in 1981, I became deeply involved with a group that then was called Creative Initiative Foundation, but it morphed into a group called Beyond War in about the 1982-1983 timeframe. And one of the key things in this group was to get out of your own perspective and try to see the perspective of other people including your opponents. Inman came in as Director of NSA and in my opinion was very smart. And he was also a bit of a maverick. When he came in as director of NSA, my take is he was smart enough to see that all of their threatening us was getting them nowhere. In fact it was

actually, if anything, causing us to be more determined—we hated their threatening us. I did. When someone threatens you, you don't like them, and you may go out and do things you wouldn't have done otherwise. They want you to do one thing, and they're threatening you, so you go even further the other way. So I think Inman realized that and basically made a peace overture. As that relationship developed, I pointed out to him, I said, 'Look'—and over time I came to really like him and some of the others who I met at NSA—and I pointed out to him that, even if they got the legislation they wanted, and even if it was deemed constitutional, because I think there would be a lot of court challenges, I said, 'It wouldn't work.' The whole focus of what he wanted the ACE study to recommend, at least initially, was for the editors of the journals to act as the gatekeepers. And I said, 'You need the authors on your side in this because if you threaten, if you control the authors, they will find ways around it. They might meet the letter of the law, but they will give a hundred talks before they send the paper in for publication. You need to get us on your side, it can't be this authoritarian approach.' And to Inman's credit, he backed off on that and went for a voluntary approach. And that's what ACE recommended.

Yost: So there was a voluntary approach for scholars to send in their papers for the NSA to review before sending them to publications. Did most of the researchers in the cryptography field send them papers?

Hellman: I don't think so. I sent them some things and there were a few cases where they asked me to remove things and I did if it really didn't hurt the academic impact of the

paper, but I could see that it had some negative political or intelligence aspect, then I would remove a few things. But there were other reasons. First I started to get out of my own frame of reference. Also I was working with this group Beyond War in 1982 to 1988 and including a year and a half full-time leave from the University to work as a volunteer from mid-1984 to the end of 1985. We were very concerned. The founders had been a little bit suspect in the McCarthy era. Somehow, calling for world peace can be seen as a—‘Communist Plot’ or something like that—so we were very careful to make it clear that we were loyal Americans—which we were. I had helped Beyond War start a dialog between the American and Soviet scientific communities and, when we had Soviet scientists visit us here, we always alerted the FBI. We said, ‘Look we think they’re legitimate, but they could be good actors and we want to make your job easier.’ Similarly, I bent over backwards in that timeframe to try to cooperate with the NSA so as not to lend any credence to latter day McCarthy-like concerns.

Yost: Was non-proliferation one of the key issues of Beyond War?

Hellman: Yes, Ted Taylor who’s credited with miniaturizing nuclear weapons, so they can fit in artillery shells for example, was a contributor to the book we published, and he pointed out that any nation with a commercial nuclear power reactor was in a state of latent proliferation, meaning they could develop a crude nuclear device within six months to a year’s time once they got rid of international controls.

Yost: Were there public key cryptography applications involved? I think I remember reading something...

Hellman: Oh you're thinking of the Comprehensive Test Ban Treaty.

Yost: Yes.

Hellman: Gus Simmons, who worked at Sandia National Laboratory in Albuquerque, was into cryptography. When we published in public key cryptography he pointed out that because public key cryptography can provide authentication without privacy, it could solve a thorny problem that had been plaguing negotiations on a Comprehensive Test Ban Treaty. Normally it's a little bit of a problem that's easily solved, but public key cryptography can provide authentication without privacy. Normally you want both privacy and authentication. You want to know that the message is authentic, and you want to keep prying eyes from seeing it, for privacy, for confidentiality. But we can do authentication without any privacy, in fact that's what you get if you do it the simple way. And so we always had to work extra to get the privacy. He pointed out that one of the big problems in negotiating the Comprehensive Test Ban Treaty circa 1980 was that the United States was insisting on strong encryption because the proposal was that we would be able to plant seismic sensors in the Soviet Union and they would do the same here. But how do we know that the data coming out of each country to the other, to make sure that there are no underground blasts, how do we know that the data's authentic and not being substituted because it's going over the other country's communication network.

And so we were arguing for strong encryption and the Soviets were objecting, worried that we would have radar sensors, for example, hidden with the seismic sensors and be sending that out in encrypted form. What public key did for you, since you could do the authentication without confidentiality or privacy, we could ensure the data we were getting was authentic and the Soviets could make sure we're not sending anything out that we're not suppose to, and vice versa. Of course Reagan came to office and basically shut down those negotiations. But I don't think, even prior to that, that we really wanted a Comprehensive Test Ban Treaty—there was a lot of posturing going on. Our posture always was verifiability and intrusive inspections. And the Soviets who were very wary were always saying, 'No, no, no.' But about the time that Gus pointed out this elegant solution to that problem, the US stopped putting any real effort into a CTBT and it became clear that we really didn't want it—that the real problem was not technical, but political. So yes public key cryptography could have had a role with the Comprehensive Test Ban Treaty.

Yost: When did Stanford file for the Diffie-Hellman-Merkle patent and were you glad to see this patent filed?

Hellman: Well let's see, the paper came out in 1976. We probably filed—I mean it's a matter of public record, but we'd have to check. It was very close to a year after that, so it would have been in probably the spring of 1977. Was I glad that the patents were filed? Yes, I'm human. I mean I like material things and the idea of making some money didn't sound so bad. I already touched upon the fact that I didn't want to be poor. So I was glad

to see the patent filed, but the reality is we've made almost no money off our public key patents. There were a number of reasons for this, but one of the most significant was because RSA, while they credited us in their paper with inventing public key cryptography, took exactly the opposite stance when it came to patents. They said our patents were invalid and, when we asked their company to take a license, they said that we should sue them. RSA Data Security, the company they formed and that got an exclusive license to MIT's patent, was sold for two hundred and fifty million dollars, while we made almost nothing. So I was happy the patents were filed, but I haven't been happy with the results.

Yost: Did Jim Bidzos offer you some stock, RSA Data Security?

Hellman: Not to my remembrance, no. Whit had stock in RSA, I believe for some consulting he had done. Unfortunately Jim and I had a period when we were in an adversarial relation over the patents. Initially Jim, along with Rivest, Shamir and Adleman took the position that our patents were invalid and that we needed to sue them if we wanted any royalties. But later, during the Public Key Partners period, we worked together. Public Key Partners was a little bit of a shotgun wedding Cylink initiated with RSA. Cylink got an exclusive license to Stanford's patents in return for taking on RSA on the legal front, which was quite an expensive proposition. Initially that produced a period when there was a partnership with the patents—Public Key Partners was the name of the entity, or PKP for short. The patents were to some extent pooled, which is what I'd always hoped for. But, as with many shotgun weddings, PKP fell apart and there was a

big patent fight. Jim as CEO and President of RSA Data Security was on the other side of that. So, that said, I didn't like him too much at first, then we were friends for a while, then we had a big patent fight and I didn't like him so much. And more recently, in the last few years I've tried to adopt a different view of things. My old view used to be Jim Bidzos hurt me financially. But I tried adopting a new attitude, re-framing it. Jim did more than almost anybody, maybe anybody, for commercializing public key cryptography. He's a great entrepreneur, salesman, and innovator and he got public key cryptography out there in a very difficult environment. And while we made almost no money on the patents and we can blame, to some extent, RSA Data Security for that, I re-framed it. I've made a lot of money from cryptography—being on advisory boards of startups, things like that. And, in some sense, I owe that to Jim Bidzos because the industry wouldn't be as big as it was without his efforts. So we've developed a friendship again, which I much prefer.

Yost: Were you surprised by how quickly RSA's work followed upon your work with Diffie?

Hellman: I don't think we were surprised. Although we were a little bit chagrined because Steve Pohlig and I had a paper that appeared after the RSA paper but was submitted before it that was very close to the RSA paper even though it was concerned with a conventional, not a public-key system. But all you had to do was change the arithmetic to modulo n instead of modulo p , where n is a composite number and p is prime, to get RSA. Now we had missed that. We had actually looked at doing arithmetic

modulo n and were looking for public key systems, but we didn't see that that gave you public key cryptosystems. So they deserve credit for the RSA system. But I do feel the Pohlig-Hellman paper, the Pohlig-Hellman system, should have been credited more clearly in terms of its priority and how it forms a basis for the RSA system. So we were excited by the RSA paper, and a little chagrined that we'd missed it.

Yost: You started a firm called Hellman Associates was this in the late 1970s or early 1980s?

Hellman: Well mid-70s I was cofounder, with another guy, of Binary Corporation, which lasted about two years. And they used to ask us who was zero and who was one. That was Stan Fraclick. Then came Hellman Associates...When we closed down Binary Corporation I worked in an unincorporated form as Hellman Associates because I was just trying to get more typical consulting. I tried to take on projects where, on a fixed priced basis, I could do it ten times as efficiently as anybody else. I could charge them a third of what they'd normally pay and still make three times my normal rate, that kind of thing. Hellman Associates moved heavily toward, in the late seventies, heavily into short courses, including a course on cryptography and data security.

Yost: And did you continue with this for a number of years?

Hellman: Well Hellman Associates, let's see, I closed it down probably about 1985. When, in the early eighties, I got involved with Creative Initiative and then Beyond War,

when I took a year and a half leave of absence the consulting business was providing some of the income that let me work as a full time volunteer without getting any money from Stanford. I had some investments also. When Beyond War became a big time commitment, it created a time problem. I could do Stanford and I could do the company but I couldn't do Stanford, Beyond War and Hellman Associates. We tried building the company up because it was at this awkward stage. In terms of today's dollars it was probably running near two or three million dollars a year. Big enough you can't neglect it, but small enough that you can't hire full time management to run it. I had to watch it on a day-to-day basis. I had to be watching it fairly constantly. So the idea was to build it up to maybe five or six times that size where you could have full time management and I could provide high-level direction. But with my main focus, especially that year and a half, being Beyond War it became clear fairly quickly we couldn't hire the people we wanted to, and if I was going to build the company up, I had to do it. And I was too committed to Beyond War, so we decided to close the company. And we did that in a controlled fashion, which actually worked out fairly well.

Yost: How long was one of your main focuses Beyond War?

Hellman: I'd say from beginning in 1982, ending in 1988, and with a year and a half full-time from July 1984 through December 1985. And even after I left Beyond War my prime focus in my later years at Stanford University was ethnic conflict, trying to resolve ethnic conflict and create an environment in which minority students could achieve more of their potential, which was also very much related to my work at Beyond War. I saw

that the two problems were very much connected. So Beyond War 1982 to 1988, but Beyond War and University ethnic conflict issues up until 1995.

Yost: Can you explain your view on key escrow or the so-called Clipper Chip?

Hellman: Well, by this time I had matured some, and as I said I tried to understand the other perspective, and there's value in having two points of view. Sometimes you can avoid a war but even if you're going to go to war over these things, understanding the other guy's viewpoint makes you a much more formidable combatant. When they came out with key escrow, while I didn't like it...At first I tried doing an exercise—in fact I ran a seminar at Stanford trying to get students to understand opposing points of view and break out of their own frames of reference and blinders—in which you pretend you're an actor in a play and you have to take the other side. Like, let's say you're Jewish and you see the Israeli cause as right and the Arabs as these no good S.O.B.s who just want to push them into the sea. In this exercise, what you have to do is research the Arab point of view enough that you could convincingly be an actor in a play, argue that it's all the Israeli's fault and the Jews' fault, and the Arabs are the victims. At the end of this it's not that you would end up in that position but then you could synthesize out of these two extreme viewpoints something closer to the truth. And so when Clipper chip came out I tried looking at it and I said, 'Wait a minute. Let's see. I don't like this, but let me put myself in their shoes.' And what I saw was, at that point, NSA had been very effective in preventing commercial encryption from being adopted. So, with Clipper chip, we'd have protection from everyone except the government, and without Clipper, we'd largely have

protection from absolutely no one. And so, in some ways it was a better deal, right? But eventually, as I studied the thing, it was clear it was an unworkable proposal thrown together much too rapidly. The government was encouraging us to put all our eggs in the Clipper chip basket when it hadn't yet been woven. I served on the National Research Council Committee that studied national cryptographic policy. It was put together at congressional request and had people from NSA and a former Attorney General on it; so all views were represented. We concluded, among us all, that that was the case because key escrow was still a major issue. And what we recommended in our report was that the government experiment with key escrow and, if it could work out the problems that we saw—particularly the international issues of who gets to escrow the keys for a device that's in France. Is it the French government? Can we trust the French, or do we get to keep the keys and the French trust us? There were just things that seemed to be insurmountable problems, that if they could solve those seemingly insurmountable problems then we could entertain it, but we were wasting too much time in our committee on dealing with key escrow and that's the way we dealt with it—that they were putting all their eggs in that basket and the basket had yet to be woven. Let them weave the basket then bring it to us.

Yost: The recommendations of the Committee's report are fairly unified. Was there a lot of dissent and conflict among participants along the way to achieve a consensus?

Hellman: No. Initially I thought I could take credit for that. But it turns out the NRC tends to run that way in general. But when I came in there, one thing I did was, I said,

look my wife and I, in family counseling, had brought up an issue with the family counselor. ‘Why is it when you have a teenage kid and you have to debate whether to be tough with them or easy with them—because you’re worried about pushing them over the edge if you’re too tough and yet you’re worried, if you bail them out, about them not learning the realities of life... If one of us takes one position the other one almost automatically plays devils advocate and goes to the other side, which drove us crazy.’ And what this guy pointed out in very simple terms: ‘That’s why you have two parents.’ Because both viewpoints are needed and he made the really important point that the one who’s taking the one position allows the other person the freedom to explore the other. This comes up in other cases too. It’s easier to see with respect to whether or not to take an expensive vacation. If my wife were to say, ‘let’s take this expensive vacation’, as soon as I take the point of view that we can’t afford it, she can begin to think about how wonderful it would be, not worrying that we’re actually going to spend all that money and possibly jeopardize our financial future. By my anchoring the financial responsibility position it’s freeing her up to think that way and vice versa. Sometimes it will go the other way. What I remember thinking when this committee came about is, in some ways NSA and the FBI, by anchoring the position of controlling export, controlling cryptography, were allowing me the freedom to explore to think why that was bad. Because I knew that my arguing for freedom of export was not going to actually make it happen. I said, ‘Let me pretend for the moment that I am absolute czar of export control and whatever I say goes. Would I really go for free export?’ And I felt some nervousness. We hadn’t yet had September 11th happen but I knew there were terrorists and we had had the first World Trade Center attack and we’d had other things like that. And I knew

about the Mafia and I even had some personal concerns there. I had some rental property in New York State and garbage was mob controlled and whether you actually go out and get free bids was a major question. So I appreciated the fact that law enforcement and the military are protecting me and allowing me the freedom to explore why free export of crypto would be a good thing. So I remember saying, if I were export czar, would I really allow free export? Now I eventually decided I would do most of it. But I went into the committee very early on and did a little speech and I said, 'Looking back, I realize that some of the arguments I made back in the mid-1970s were not solid. At the time, I thought they were honest arguments. But, in thinking about it, I realize I did what most people do. I argued to win and when the other side had valid points I tried knocking them down.' Now NSA was doing this to me too so I'm not uniquely tarring myself. This is how people fight; they fight to win instead of fighting to get at the truth, even when supposedly that's what they're seeking. But I made a commitment in 1981 to try and never do that again. So in the committee I said I am going to work very hard to call them on it when the privacy advocates make a fallacious argument. For example, there was this argument, 'You can buy DES on the streets of Moscow, the software. So what's the point in controlling it? It's stupid to control it.' But as I've said, I've re-examined that, and we're not dealing with stupid people here. NSA is not stupid. And what I concluded was that both the value and the threat in cryptography was not in stand-alone encryption, because most people will not go to the trouble of buying a stand-alone encryption program, even me, and integrating it with their email program. But it's integrated cryptography that is valuable, and also therefore the danger to intelligence operations. And so the fact that you could buy DES on the streets of Moscow was not a threat, but if

you could buy an email program that had encryption incorporated into it—integral and automatic—that was both of tremendous value in protecting against criminal activity and also a threat to law enforcement and national intelligence when used by terrorists or criminals. Because Microsoft and other American companies largely control those businesses, controlling export actually did an awful lot of good. And how much encryption did we have? Very little. So, in spite of the being able to buy DES on the streets of Moscow, export controls were largely achieving their goals. So I said, in the same way that I will try to call the privacy advocates when they make fallacious arguments, and it's not to say they are bad people, I made those same arguments twenty years before in my youth when I didn't realize what I was doing, I would hope that those on the committee who represented law enforcement and national security would call the people that make fallacious arguments on the other side. So, while I may deserve some credit for how well we worked, the NRC tends to work that way in general. It's very good at creating unity.

Yost: What was your reaction at the end of 1997 or beginning of 1998 when James Ellis' paper was declassified about the work at GCHQ?

Hellman: It's calmed down a little, but I wasn't very happy. I wasn't happy with a number of things. First of all this was kind of like a nightmare come to life. Because you remember one of the arguments that my colleagues had made, why I was stupid or crazy to work in cryptography is 'How can you hope to discover anything new?' And I'd argued back that the classified literature was not available for commercial exploitation—

and cryptography was needed commercially. Also the credit goes to the first to publish, not the first to discover and keep it secret. How can you even verify claimed priority based on secret publications? What I would have liked is if they had pointed out, 'Look we're making these claims. We understand there's no way for you to verify these claims. We also understand that the credit in the open literature goes to the first to publish.' It would have been nice if he'd said all those things and also if he'd pointed out that even if all their claims are absolutely correct, that they never did anything on digital signatures, which is at least half the invention, and they never pointed that out. I wasn't real happy with that. And also I have to admit my ego was bruised. I try not to be ego involved, but I'm human, so my ego's involved here. Some of my colleagues annoyed me even more. One sent out an email saying when that came out, 'For the true story on the invention of public key cryptography go to this web site.' Now here's a guy who's a professor at a major university and should know better than that. And I thought about what to do because I was actually pretty mad at him at first. It was very disturbing to me. And I even debated whether or not to say anything here today because I have an interest here. I have an ego involved. So everything I'm saying has to be taken within that context. Just like I argued before, when you get people who really want to try to figure out what's going on, try to be an actor on both sides. First, be me and just get as angry as I possibly could. If I let myself go I can say, first they go after me—and it's not GCHQ, it's taking the whole classified community together. They lie to me about the DES key size for example, 'Fifty-six bits is plenty good don't worry. You're wrong, we can't do exhaustive search.' Putting out specific numbers that are absolutely bogus. So first they lie to me. This is the part of the exaggeration, this is the actor, I'm not saying this is the truth, okay? But it's

one of the extreme viewpoints. First they lie to me, and then they threaten to throw me in jail. Some of my friends who had worked in the intelligence community even told me that my life could be in danger, though other friends, equally knowledgeable, told me that was crazy. Then they steal money from my pocket, and that's where, by holding back the development of public key cryptography, the patents were less useful, so Stanford was less active in defending the patents. So it wasn't just RSA Data Security claiming they were invalid that caused us to make almost nothing off our patents. And now they're trying to steal the credit. Now that's one viewpoint. The other viewpoint and maybe somebody else needs to come up with it, but I can try. Look, these guys toil in anonymity. And while I or any other American doesn't agree with everything that the military has done, overall we have to be grateful to them for giving us the safety in which we can have these debates. Sure we can't verify their claims, but how could they put out a full version of the report that was absolute bogus. There's too much chance that someone would rat on them from within the community. People in that community can get incensed over ethical lapses, especially since this is no longer classified; it's in the open. So somewhere between those two extreme views is the truth. I hope that answers the question.

Yost: Yes. When friends in the intelligence community told you that your life might have been at risk did you ever consider getting out of this and focusing your research and energy elsewhere?

Hellman: Oh no. If anything, as I said earlier, if somebody threatens you, it may not be in everyone, but in many people, the normal human reaction is, 'I'll be damned if I'll let them bully me this way.' My wife was very relieved when the fact that this fight was going on became public knowledge and was in the *New York Times* and *Science* magazine. Because, prior to that point, she was worried if something happened, if some suspicious accident happened, who would question it. Of course once I had some notoriety, that way it would spark a question. I doubt my life was in danger, although you know there are mavericks within every group and who knows?

Yost: What do you see as the most important technological and public policy issues involving cryptography moving forward?

Hellman: Well I think it has to do with integration. What I said before is that the real value in encryption and the real threat to intelligence operations, both law enforcement and national security, is integrated, automatic encryption. I think another important issue is striking a better balance within the government, which I think did happen. Almost all of the NRC recommendations have been met. We argued in the NRC report that DES should be almost freely exported for western countries, for friendly countries. Iran and North Korea are another matter... And that came about soon after we argued for it. I think the other thing is user awareness. I mean it was about twenty-five years ago that *IEEE Spectrum*, the general magazine for the IEEE called me and said, 'What is the greatest unsolved problem in cryptography today?' And I said, 'Lack of user awareness.' And I think it's still a problem. People just aren't as concerned as they ought to be—with the

viruses and the spam and everything else. Now again, I may be thinking as a theoretician. I have argued that the Internet should have had security built into it from the very beginning, where every email message was authenticated with a signature, and that there was an adequate public key infrastructure in place. But there was a predisposition within that community, the open source community, almost toward a lack of security. The open source community has a lot of good things going for it. But it doesn't like secrecy. Like in UNIX, the UNIX operating system, the password directory was all publicly readable because they used what they thought were one-way functions to protect them. But they can't really be one-way functions because the passwords are too short. There was not just a lack of concern for security, but such a strong dogmatism of openness that it got in the way. And what I've argued all along is that building security from day one is much easier than adding it on as an afterthought. So there has been a lack of concern at a user level and at a development level. I've argued that when a company goes to develop a product, that has only two options, secure or insecure, they should, from day one, define the product as either secure or insecure. For example take the cellular telephone system. There are only two options here, secure or insecure. And as we saw with Prince Charles' conversations, the system was insecure. What I would have liked is the people at Motorola, or whoever first developed this, when they sat down would have said, 'Look we only have two options. We are either going to develop a secure cellular telephone system and have that in all the advertising: 'Buy your secure cellular telephone here!' Or, and this is the fun part, 'If we make it insecure we're not going to hide that. We're going to put that in the name and when you go to Radio Shack it will say, buy your insecure cellular telephone here.' Now that's a little bit utopian that companies would actually do

that, but I think that's what should be done. And there needs to be more pressure maybe from the public, maybe even from regulation. Since the Internet developed with little or no concern for security, we have a system that's grown almost impossible to use. I mean ninety-five percent of my email is spam. I have a spam filter, but occasionally a legitimate message will be misclassified as spam. When I get back from a week long trip I have to delete huge volumes of that spam without even looking at it, so I cannot count on email as being reliable any more. I'd like to see more concern for security at the user level, at the corporate level when they purchase, and at the corporate level when they develop these things.

Yost: Is there anything that I have not touched upon that you wanted to talk about? You mentioned some individuals that have not received proper credit for their contributions that you wanted to recognize.

Hellman: Unsung heroes, yes, let's see... First of all certificates. I think for most people VeriSign is basically a certificate company. I don't know what their market capitalization is now, but at the peak of the bubble I believe it was tens of billions of dollars. All that goes back to a Bachelor's thesis at MIT by Loren Kohnfelder, He's the guy who thought up certificates. I mean, in hindsight they're obvious, but prior to his Bachelor's thesis no one had really put forth the idea of certificates. He had a tree structure. Another guy is Richard Schroepel. He has a Master's degree from MIT, I think. And Richard has made major contributions in many areas, particularly in cryptography, that have not been fully recognized. Part of it is that Richard doesn't like to

publish. With the few papers he has, I think what happened is someone else wrote the paper and then they realized that he developed it before them. Unlike the GCHQ things where they were secret, Richard did circulate them. Because people have asked, and that was a good point someone brought up. Here I'm saying Richard deserves credit and yet I take issue with GCHQ's claims. I'm not saying GCHQ doesn't deserve any credit. I'm just saying it needs to be modified. But there was also a difference. I realize that GCHQ could not publish. And while Richard did not publish he circulated his papers.

TAPE 2 (Side A)

So I was saying about Schroepel, while he's made a number of contributions, the one that is most overlooked is factoring, because he again did not publish, he just circulated it. And factoring is critical to the RSA system. In particular Schroepel was the first to develop arguments that show the subexponential work factor for factoring numbers. If you have a number that's a hundred digits long the obvious way to try to factor it is to try to divide it by all primes that are fifty digits or less because you couldn't have more than two prime factors, if there are two prime factors they couldn't be bigger than fifty digits each. As the size of the number grows from ten digits to twenty to thirty to a hundred the number of primes grows exponentially. So the obvious factoring method is exponential. Now the continued fraction method of factoring that Morrison and Brillhart developed in 1971 is subexponential, but they hadn't analyzed it and shown that. Richard did some calculations that while not rigorous, pretty convincingly demonstrated that the continued fractions method was subexponential. And the Quadratic Sieve Method that is Carl Pomerance's, he deserves credit for the Quadratic Sieve. But it is a variant of the

factoring method that Richard had proposed and was circulating. While Pomerance gives Schroepfel credit in his paper, people are not as aware of Richard's contribution as they should be. There are probably others but I think...Gill, Schroepfel, Kohnfelder, Pohlig...are the ones that come to mind right now and I apologize to any others. I should have made some notes before today. Oh, another is Paul Baran. In the sixties, mid-sixties, Paul had a very farsighted report at the RAND Corporation where he was working on the need for encryption and some very interesting ideas. Oh and then there's one other, he's not unsung, of course, Paul Baran's not totally unsung either, but Paul Kocher who runs Cryptography Research, Inc. out in San Francisco. Very interesting character. He has only a Bachelor's degree in Biology from Stanford but knows more about cryptography than most Ph.D.s or professors in the area. The Deep Crack machine that has been publicized—for many years the whole issue of whether you could do exhaustive search or DES was up in the air because we didn't have the ten million dollars or whatever it took to build it. Paul Kocher actually designed that machine and doesn't get as much credit as he deserves for the design and implementation of that machine. He's received a lot of attention in other places, like differential power analysis was covered by the *New York Times*...

Yost: Great. Anything else you'd like to add?

Hellman: Thank you for doing this. I hope at some point people go back and try to figure out all of what happened. This is the first opportunity... I'm too lazy to sit down and write all of this down, this had been a nice way to record everything.

Yost: Well, thank you very much for taking the time to do the interview, it's been fascinating and will be very useful for research.