Whitfield Diffie Interview

Interviewer:
Jon Plutte

Recorded: March 28, 2011
Mountain View, California

CHM Reference number: X6075.2011

Jon Plutte: So what is public-key cryptography? Public-key cryptography, I can't even say, but I'm sure you can say it. And whenever you're ready to roll.

Whitfield Diffie: Okay.

Plutte: Okay.

Diffie: You're rolling, so I have my opening statement, this interview is given in terms of Copyleft. If you're hearing it and seeing it, you're entitled to record it. If you have a recording, you're entitled to redistribute it under the same terms.

Plutte: Okay, thank you. Today it is March 28, 2011. This is John Plutte interviewing Whit Diffie at the Computer History Museum for the Fellow Awards. Thank you for joining us.

Diffie: So now we have a technicality. You asked if I liked to be called Whit, that's fine, but I like [it] to be written as "Whitfield."

Plutte: My words will never be on camera.

Diffie: I understand that, but you may have influence over copy or something.

Plutte: Okay, all right. That's great, okay, so we'll make sure that that gets done, and I'm pretty sure that that is the way it is written out in the paper here. I'm going to start off with some basic questions for us people who aren't that familiar with the field, and the first one is, what is cryptography?

Diffie: Cryptography is any technique for transforming information from a usable, comprehensible form into a scrambled, useless form from which it can only be recovered by people who know what are called "secret keys."

Plutte: How did you get interested in cryptography? I understand this is a long story. I'd love to hear it.

Diffie: Well, I got interested in cryptography in many stages over a quite number of years. The first even occurred when I was ten. I was in fifth grade and my teacher, Nancy [later corrected to Mary] Collins, spent an afternoon discussing cryptography. And I got interested in it and got my father to bring me all the books from the City College library. And I managed to read several of them. I was never able to read Helen Gaines' "Cryptanalysis," haven't read it yet. But that interest lasted for a few weeks, and I sort of concluded that a transposed Vigenère system was the perfect thing, and set the matter aside for quite some time. And then, while I was at MIT and afterwards while I was working at Mitre, every now and then, I'd hear some tidbit on the subject, but I never did anything much with it myself. But in the late '60s, I decided it was important and I began trying to talk other people into working on cryptography. And they all wish they'd been talked now, but they didn't. They thought they were doing more important things also. So in 1969, I moved here to California to work at the laboratory of John McCarthy at Stanford University on what is called the proof of correctness of programs, formal mathematical proofs that programs do what the specifications said they ought to do. And I was going along, not making any huge amount of progress on that problem, for which I can perhaps be forgiven since nobody's made a huge amount of progress on it yet, some progress. And in 1972, something happened in Washington. Larry Roberts, whom I'm sure you know, who lives here in Woodside, and who was funding the Arpanet, went up to NSA to see Howard Rosenblum, who was the Deputy Director for Communication Security, and roughly speaking said to him, "I have $100 million a year research project on communications, with an interest in military applications, and we think we ought to give some thought to security." And they probably agreed on that, but one step further, they couldn't agree because Roberts didn't want to fund any secret research, and Rosenblum didn't want to do anything else. So Robert drives back to his office in Roslyn, [Maryland], and Robert's job is one where his principal investigators come by with their hats in their hands, and they have to listen to whatever he wants to talk about. So in comes John McCarthy, and that week, he wants to talk about network security. And at that time, all of us thought of network security as meaning cryptography, probably NSA did, too. We would now see the two fields as different, and one is just a minor part of the tools for the other. But as it was then, John came back and he talked to his research staff about this, and we talked about cryptography and most people stayed interested in [it] for a week or two. Other than I, the person who did the most work on it is the one who's now head of the robotics lab at CMU.

W1: Hans Moravec.

Diffie: Hans Moravec.

W1: The teacher was Mary Collins, not Nancy Collins.

Diffie: You're right, I apologize. That needs to be corrected. Let me run that little bit again. So I'm ten years old, I was in the fifth grade, and my teacher, Mary Collins, taught us about an afternoon on cryptography. And I got interested enough, I got my father to get me all the books in the City College library, and I was able to read several of the children's books, but I never got through Helen Gaines' "Cryptanalysis," and concluded in a week or two that a transposed Vigenère system was optimal, and didn't revisit the matter for several years. The problem with that is Nancy Collins was the personal assistant to Paul Baran, who died a couple of days ago, so I don't want to make that mistake.

So the other person who did serious work on cryptography in this, after John McCarthy introduced the topic at the AI lab, was Hans Moravac, and he wrote a program for John. John had an idea based on the [Soviet] BESM-6 computer. And the BESM-6 computer had two instructions in it called "spread" and "gather" that had been put there for cryptanalytic purposes. And John McCarthy may not have understood that but he saw them and he saw how to make what was later called a shrinking generator, one sequence that picks bits out of another sequence. And Hans Moravec coded this for him and Hans Moravec [thought] that John McCarthy might want to encrypt something that Hans might want to know. So as far as I know, Hans Moravec is the first person to put in what is now called "key escrow." He stashed the key somewhere in the message, so that he would know where to find it in case he ever wanted to read any of John's traffic. So I started thinking about cryptography and unlike Moravec and everyone else, I didn't stop after two weeks. And six months later, I was working on nothing else, and this was kind of an embarrassment to John because I wasn't working on what I had come to work on. And since I was being funded by under-the-table money from NSA, that might be a bit awkward if it came to light.

So it was spring of 1973, we negotiated a friendly parting of the ways, and I took an indefinite leave of absence and departed, and began driving around the country, thinking about these problems, digging up rare manuscripts in libraries, talking to anyone that wanted to talk about it. And over the next, oh, I don't know, that summer, I met Mary in New Jersey, and then we traveled together for another year and a half before we really settled in California. And I called that my first discovery. Without finding Mary, I don't think I would've found anything else.

But in the summer of 1974, we went to the only non-governmental cryptographic laboratory that I know about of any significance in the U.S. at that time. And that was in the mathematics department at IBM Watson Laboratory in Yorktown Heights. And the mechanism was that a man named David Silver, who was the son of my first boss at Mitre, took me to introduce me to a man named Alan Trider [ph?]. Now, Alan Trider considered himself the biggest man in computer science. He weighed 500 pounds. And Trider introduced us to his boss, Alan Konheim. Konheim's very secretive, he only told us one thing, and since then, he wished he [had] never said that. He said, "You know, I can't tell you anything. We're under a secrecy order here. But my old friend, Marty Hellman was around here a few months ago asking about this, and I couldn't tell him anything either. But you know, two people can work on a problem better than one, so when you get back out to Stanford, you should look up Marty Hellman to help see if you can work together on the subject." So we got back out to California and we were staying up in Oakland with another computer scientist named Leslie Lamport. And I called Marty and he graciously granted me half an hour of his time on some afternoon, probably a Wednesday or a Thursday, I don't think it was a Friday. And Mary and I drove down there and I got off at Stanford and she went off to do something or other. And Marty, five o'clock past, and five-thirty, Mary called and said, "What's up?" And Marty invited us to dinner. And we found not only as individuals, but as family, as we got along wonderfully. Marty's mother-in-law raises dogs, Mary can recognize 300 breeds of dog at a glance. It was a multiple-marriage made in Heaven, you know how California is. And Marty and I then worked together for four years, and during that, we basically did two things. One, we invented public-key cryptography, and the other was that we became critics of the system developed by Alan Konheim's group and others at IBM, which became the US Data Encryption Standard (DES). So the two fundamental seeds of my career, cryptography and crypto-politics, were planted that spring.

Plutte: Why don't you tell me what you think was not correct, what did you like about that?

Diffie: About DES?

Plutte: Yeah.

Diffie: Oh, the problem with DES was that the key was too small. So DES had a billion billion keys, roughly speaking, not quite, and that's a large number, but it's not a large enough number in our view. And a key point of this is the fact that having a large number of keys isn't in itself expensive. If you know how to make a strong algorithm with 56 bits of key the way it had, you could make it with 66 or 76 or 86 or 96. So many people criticized the structure of the algorithm itself, and suggested that trap doors had been built into it and things like that. I believe I was too discreet ever to suggest anything of that sort, and that proves to have been prudent. In my view, no serious fault has been found with it. Although, it's a kind of a cluttered, unattractive design. But it was, I believe, designed to be a compromise between what was seen as the security needs of civilian government. Remember, it was a federal information processing standard, that set of standards for the acquisition of equipment by the federal government. And compromise between the security needs of civilian government and the intelligence community's desire not to be putting out an algorithm that it couldn't possibly break if it suddenly felt it really needed to. So possibly getting ahead of you, I'm just going to go on with this story a little bit.

Plutte: Okay, go ahead.

Diffie: And that was 1975, despite our criticism, the algorithm was adopted in August of 1977 and was in there with some amendments, remained the standard until a few years ago. I don't know exactly, but into the 21st century. But by the '90s, it was becoming clear that this standard needed to be replaced. And by then, NSA had changed its mind. So in early 1997, maybe as a matter of fact, January 2, National Institute of Standards and Technology put out a new call for selecting a successor algorithm. And this was the beginning of a worldwide contest in which ultimately 15 submissions were accepted. And it ran for nearly five years. It's, I think, 2nd of January 1997, for the call for comments on the specification against which the algorithm was to be designed. And then, I believe it's October 26, 2001, it's finally signed by the Secretary of Commerce. And in an unprecedented action in an area that's a chauvinistic and nationalistic as cryptography is, the US selected a Belgian-designed algorithm as its national standard. And unlike DES, it wasn't designed to be a compromise. It, it supports three different key lengths, none of them, in my view, likely to be accessible in this century, though it has keys of 128 or 192 or 256 bits. And two years later, something called "The Committee on National Security Systems," part of the Department of Defense, put out a memo saying, "This algorithm is adequate for the protection of all levels of classified traffic." Secret and below, any of the modes are all right, top secret, you have to use one of the two larger modes. And that was capped off, another two years later, with the publication by NSA of what are called the "Sweet B" algorithms. That and several others, most of them public standards and all of them public, that are a complete set of algorithms for using for cryptography in national security.

Plutte: Great. So we're going to go back closer to the beginning of this story and talk about public-key cryptography. The first thing I'd like to get is what is public-key cryptography?

Diffie: All right. public-key cryptography is a set of cryptographic techniques, in which you can make some of the information that forms the keys public and keep other parts secret. And if you know the public parts, you can't figure out the private parts. So let me give it to you in two different forms. One possibility, and the one which I originally envisioned it, is that you have two keys that are inverses of each other. Anything you encrypt with one, you can decrypt with the other and vice versa. And if you had that, and you had the property that given one, you couldn't figure out the other one, then there are two things you could do with it. In the first place, if you wanted to send me a message, you could just look my key up in the phone book. All right. Since you can't figure out my secret key from my public key, it's all right to publish my public key in the phone book and you can look it up and you can encrypt a message and you can send it to me. At least as remarkable is the fact that it goes the other way around. Suppose I want to send you a message, and I want it to be signed. I want you to have evidence that it came from me. And then, if I encrypt it with my secret key, then you're able to look me up in the phone book and decrypt it with my public key, and now you can go to somebody and say, "Here, look, see this message? If you decrypt it with this public key that's in the phone book under Diffie's name, it comes out and it makes sense, so Diffie must've sent it." It turns out there's a whole other way of doing this, and curiously, I proposed the form I just described to you, and ultimately the only solution song so far was found by other people -- by Rivest and Edelman. Ralph Merkle, who was working independently of Marty and me, initially formulated the problem another way. He didn't see the signatures and said, "Suppose we're talking to each other over an insecure channel. We've never met before. Is there any way we could communicate with each other in such a way as to end up with secure communications?"

And that is the problem that is solved. He had a solution to it called the Merkle Puzzles, but that isn't by and large in most circumstances a very workable solution. And Marty came up and I came up with a much better way of doing it, which is now called Diffie-Helman [key exchange] or Diffie-Helman-Merkle, or if you stretch it even further, Diffie-Helman-Merkle-Williams, maybe we'll get to that at some point. And that one is a little like perfect bridge bidding. So you imagine you and I are north and south, and we're sitting here, playing bridge against the evil east and west, and we're in the contract phase of the game. Now, when each of us comes to understand the other's bids just a little bit better than they understand them, because I can see my hand and you can see your hand, and they can't see either hand. Now, suppose that we're sort of much better. Suppose we could sit here and negotiate in public, and I speak and you speak and I speak and you speak, and after a while, we know something's secret and common that none of the observers know. So the difference, the important thing is being active. So these two things, both are now widely in use. And I didn't do myself any good by liking the RSA formulation better because it solved the problem as I had proposed it. It turns out that that, in retrospect, has two very serious problems, though it is widely in use now and will be for a long time. One, the conceptual problem, is that I give you a secret key and I say to you, "Here, this is a great secret key. Send me a good secret." And I'm expecting you to encrypt something you think is secret in this key that I provided, and there's nothing you can do to tell whether it's good or not. The very fact, the same things that make it secure, make it inscrutable. On the other hand, the other thing that's bad about RSA is the only way that anybody's ever found of doing that. I mean, there are variations, but none of them are as good as that system. So new discoveries in cryptography can't very readily be applied to it. The virtue of Diffie-Helman, it isn't quite as neat, particularly in the signature formulation. But it is very good in the none [sp?] of the secret things, it's complicated. So we proposed a thing called the modulus and the generator, but they're public. You can tell everybody all about those. And then, you have to generate secret exponents, but those are just random numbers, and they'd better not be zero or one, but other than that, pretty much any number will do. And you can do Diffie-Helman with many kinds of arithmetic, and the one that's currently popular is part of the Sweet B I was mentioning to you, is what are called elliptic curve groups. Now, I noticed that you're asleep, but if you wake up, you can ask me another question.

Plutte: I was just trying to figure it out. I'm not a cryptographer. So you worked with Hellman and you worked with Merkle. Can you talk about just the sequence of events of how you all ended up working together?

Diffie: Okay. So how did Marty and Ralph and I come to be working together? There's a key ingredient here, who's name is Peter Blackman, who had been a childhood friend of David Kahn, who's the historian of cryptography. And he was a graduate student of computer science at this point at Berkeley, and he knew Ralph Merkle. And I had been introduced to him by one of their professors. So when Marty and I wrote our first paper on public-key cryptography, for the National Computer Conference, this conference no longer exists, but it was the biggest conference in the world at that time. And in about Christmas 1975, we submitted a paper to the National Computer Conference, which was going to be in June of 1976. And I gave a copy of the paper to Blackman, and Blackman gave a copy to Merkle. And Merkle had been taking a course with a man named Lance Hoffman, who was big on term papers, and you had to submit a proposal for your term paper, and then you write your term paper and so forth. And Merkle submitted a proposal for public-key cryptography, and Hoffman didn't understand it and he sent it back to be re-written. And Merkle submitted it again, and Hoffman still didn't understand it, and Merkle dropped the course, but he kept working on the problem. There's a wonderful remark about DNA, that is Rosalind Franklin had gotten along with the head of her laboratory, that Watson and Crick would be just a minor footnote in the history of DNA. If Hoffman had understood Merkle's proposal, it would all be Merkle and Hoffman, and Diffie and Helman would be a minor footnote. But somehow he didn't, and Merkle went on working on this stuff. And then, when he got our paper, he realized there was somebody else in the world who would understand him, because he'd sent a long paper on it to the ACM, which was not accepted at that stage. And eventually, it was refined into a paper called "Secure Communication Over Insecure Channels." So he called me and sent his paper to Marty, and Marty's nothing, if not a very good talent scout. And he immediately perceived Merkle's problems as a graduate student at Berkeley, and got him to transfer to Stanford and found funds for him. And so from, I guess it's approximately the summer of 1976, the three of us, but particularly the two of them, worked together.

Plutte: So had you and Hellman been working together, doing this?

Diffie: Yes.

Plutte: Yeah, trying to figure that out.

Diffie: So I met Hellman in September of 1974. We worked together from then on for several years, but we met Merkle about January 1976. So there's about a year and a half when we were working together, and don't know about Merkle. Okay, and then another period of time after that, certainly about' 78, Merkle graduated in '78, and the alumni register at Stanford politely shows me as having "graduated" in 1978. That is to say, they lost track of me.

Plutte: Okay. So did the three of you actually work together, or did you work in teams of two?

Diffie: We worked loosely. Marty and I worked closely together. And Marty and Ralph later worked closely together. But the form of the discovery of Diffie-Helman, Diffie-Helman-Merkle is that he, in effect, what we got from him at that stage was the problem, the formulation of the problem, and ungraciously wrote it up. I don't remember if we cite him in "New Directions", but we certainly didn't include him as an author at that point. But the key, that insight into how to formulate the problem, later came to be clear as a very important ingredient.

Plutte: So you wrote your "New Directions," he was involved in your work before that time?

Diffie: He had proposed, he had communicated that formulation of the problem to us.

Plutte: Okay. How much did the NSA or CIA help or hinder your work? What was your relationship?

Diffie: Well, they helped my work a great deal, but this wasn't entirely their intention. I mean, to start with, they told Larry Roberts.

Plutte: Can we start again?

Diffie: Absolutely. Did NSA help me or hinder me? Well, it cuts both ways. On balance, they probably helped me more than they hindered me. First, by Howard Rosenblum telling Larry Roberts that he wasn't willing to do any public work on security of the Arpanet. That's what got me into cryptography. But there actually are several more ingredients. Some time in 1965, I was walking around Tech Square in Cambridge, talking to a friend named Bill Mann, who had been doing database work ________ and he told me mistakenly that they encrypted the telephones within their own buildings. Now, they don't do much of that now, and they didn't barely do any of it then. They just had two telephone systems and ran them in separate shielded conduits and that's a perfectly fine solution within a set of buildings. But what got me, I could understand how you could do this. I think I underestimated how difficult it was at that time. But what I didn't understand was what [the] benefit you could get from it, because my concept of a secure phone call is, I'm talking to you and nobody else in the world can understand us. So all the way, as I could see of doing it, meant that somebody else, maybe some mechanism that managed keys, and I probably didn't think that clearly about it at that time, but I knew that somebody else would be able to get a hold of the key and the fact that that would serve the needs of a large institution like that, as distinct from the needs of private individuals, just didn't occur to me in the way I thought.

Then I also learned a good deal from the same person, I guess in the summer of '75 or so. He was working on what's called "the private line interface," the first cryptographic device developed to work on the Arpanet. NSA had come around by this time, at least partially. And I came to understand something about what the actual requirements for cryptographic systems were in terms of the way. I even said to them, "So why don't you just write a program that does this, that and the other?" And he said, "Well, this won't meet the specs because," and he began to explain the requirements for isolation of cryptographic functions. So at least on three points, and probably on some others, of course, I owe them a lot. The minute DES came out, I thought to myself, "Well, they can't publish a secure algorithm because they wouldn't want one nobody can break. And they can't publish one that somebody might break, because then they'd have an awful black eye." And that's' what led me to the notion of a trapdoor cryptosystem. I inputted to them some wonderful piece of mathematics, I don't think they knew or know, that they could build a system and they could prove it was secure, unless you knew the secret piece of information and they would have that, and other people wouldn't and so forth. And that basically is what led me to public-key cryptography. I came to see that that could be done in a way that would serve a much wider constituency. On the other hand, I think NSA has never, that I'm aware of, been anything other than rude to me. There are some people who got screwed, they issued secrecy orders against some people's patents. Some people feel they were threatened, etcetera. Nobody has ever threatened me. People have been sometimes justifiably and sometimes not, fed up with me. But the institution has ranged from being rude to being incredibly, openly welcoming. When I wrote to the director after the death of Frank Roluette [ph?], who was the last surviving member of the first generation of US governmental cryptography, started working in 1930. And I had learned that there was some celebration that they'd planned of his life that they weren't going to do, and I thought they cancelled it all together. I wrote an indignant letter to the director, to which came the response, "Well, what we're going to do instead is we're going to name the commons[ph?] building, Ops 3, after Frank Roulette, and we'd like you to come speak at the dedication." And so that's probably the height of our cordial relations.

Plutte: There's some interesting questions which are not necessarily time-sequenced.

<crew talk>

W1: You haven't hit the moment at which you made the discovery and we want that.

Plutte: All right.

Diffie: So I made, you're curious as to what the process of discovery was actually like. Well, John McCarthy, the person who had been head of the lab, in 1975 was invited to Japan for, I don't know, three months or something of that sense, three or four months. And that meant he needed somebody to take care of his 13-year old. She's perfectly capable of taking care of herself, except for the fact she can't drive. And you have to be able to drive, or you can't get anywhere, and lived off in the middle of the Stanford campus. So he invited Mary and me to stay at his place while he was away. And this just worked out wonderfully. Mary was taking care, supporting us, she was working for British Petroleum up in San Francisco, and I was playing house husband, and a combination of taking care of everybody, had a boarder as well as his daughter. And I was doing all of the cooking and I also had a long-term project to clean up the house, and this sort of occupied part of my day. And then, I had John's, what would now be standard, but John had a home terminal. John had a wonderful 5,000 bit a second connection to a computer over at the lab. And so I had that place to work, and I got to working. I couldn't solve the problems I really wanted to solve by proving the correctness of cryptography. So I got to working on what I had a list of what I called problems for an ambitious theory of cryptography. And at some point, I started thinking about how to combine two things that I knew about.

One is what's very widely used in protecting passwords in Unix and other systems, which is called a one-way cypher, so that the password table doesn't contain anything sensitive. That's a slight exaggeration in terms of current computer practice, but the notion, and it's a very, very sound one is, that you don't have secrets in the password table. That makes the password table much easier for the sys admins [system administrators] to manage. In particular, if you have an account on that computer and they want to give you an account on this computer, they just go get your table entry with your name and your password out of that computer, and then put it in this computer. That's over easy [ph?]. The other direction is also now very common, it's a little token, so you get a challenge. You're trying to log in and it displays a challenge, and you type the challenge into the token and then it gives you an answer, and you type the answer back. That's called "identification friend or foe." And at that time, the only place that that was much used was in military aircraft. A fire control radar sends a message to an airplane, says "Hey, you, I'm thinking of taking a shot, and are you a friend of ours?" And it expects the aircraft to decrypt the message, modify it, re-encrypt it and send it back. So I had this notion, these protect you against two different things. One protects you against compromise of the lock. The other protects you against somebody sort of shoulder-surfing the typing of the password. And I had this notion you could somehow combine the two by protocol to get both benefits out of it. Nobody has ever succeeded in doing that as far as I know. But after a while it's led me to realize to think of what, you know, of signatures. I suddenly realized I had in hand the possibility of the solution of a problem that I've been worrying about since 1970.

1970 I arrived at Stanford and John McCarthy was off in Bordeaux, giving a paper about what we would now call Internet commerce. He called it buying and selling through home terminals. I'll just pause for a second you can get out fast rather than alright you can cough instead of getting out. Last time you went out you were worried about making a sound at the door. So when I learned about- John came back and talked to us about the buying and selling through home terminals, I began to think about a paperless office. And what bothered me about a paperless office was, I didn't see what you'd do for signatures. Because what you do on paper is the fact that it's very hard to copy a signature exactly; whereas digital documents can be copied absolutely, we depend critically on the fact that you can make perfect copies.

So in the spring of '75, sitting and keeping house at John's I realized that the possibility of a problem. The problem with that property and I thought about that for a while and I had some instructions involving matrices and so forth that weren't good enough but seemed to indicate the right sort of thing. And then about a week later, and unfortunately I have lost the date, though I think it may be somewhere in somebody's papers, because I realized I discovered something very important, and I was keeping my notes on the computer and I knew very well the computer wasn't secure, but what I realized that you could turn this around, the signature mechanism around, so that you could solve this key negotiation problem that I had imagined that I had been worrying about since 1965.

So I had two problems I had been thinking about one for 10 years and one for 5 years, and suddenly in the course of a week, I had the solution to both problems. And Mary came home from San Francisco, and she remembers this much more clearly than I do but I had prepared dinner and I sat her down and told her that I thought I had made a wonderful discovery. And then after dinner I walked downhill. It happens John McCarthy's house is right uphill from Marty Hellman's house and there's a sort of stair down the back and I walked downstairs and I talked to Marty and it took me an hour or so to persuade Marty that this could be done. And then he said, "I have an invitation from Jim Massey to submit a paper to the Transactions on Information Theory about cryptography, how would you like to join me on that? And that is the paper that became New Directions. And so then Marty's memory on that point differs a little from mine, and I've never… there must be documentary evidence in the form of letters from Massey or something, but I have never nailed it down.

Plutte: This is in the realm of, just looking for some sorts [ph?] right?

Diffie: I like <inaudible> the realm of, this is the realm of fantastic.

Plutte: What was Marty Hellman as you call him like to work with and do you have some interesting or funny stories that you can tell about your relationship?

Diffie: Ask Mary, she's laughing already. Well I mean, what was Marty like to work with. My working relationship with Marty and other people in _______ are curious in the sense that I think the normal pattern of a doctoral student with an advisor, is that the advisor knows more about what the problems are and what the field is and what the problems are and proposes problems and good graduate students then pick those up and work out details and so forth and write theses and in many respects my relationship with Marty worked the other way around. My view is that I'm not terribly smart, but I'm reasonably imaginative. Marty is extremely smart, given any problem he can contribute to it. So there's this combination of being a good talent scout and very good at working with people and adding to seeds of discovery. So his working relationship with me, with Ralph, with Steve Polig [ph?], with Teharo Gamahl [ph?] those are the one or two other people, I think had very much that form that he talent scout spotted his students and then they would do things and he would then bring his broad knowledge of mathematics of coding theory and such to bear and say, "Oh, did you go about this, you could try doing this this way." I think that's the major, it'd be interesting to see if Marty sees if that way if you would interview him if he thinks of it the same or differently. You may have to ask Marty what I was like to work with, I don't have complete __________.

Plutte: He had a good answer, he passed actually.

Diffie: I have a better answer, I'm insufferable.

Plutte: How about Ralph Merkle to work with, as a person too?

Diffie: When I wrote a history called "the first ten years of public cryptography" I said of Merkel now enters the most imaginative character in the public he saw that [ph?]. I happen he personally, not intellectually I think terribly congenial was Merkel, that is to say his solutions to problems all tend to involve a lot of storage or a lot of bandwidth or something, I didn't find them as charming as some other things I've learned, but Merkel is the most independent of anybody if you draw a dependency graph of who got ideas from whom; Ralph is independent of anyone I know and he is an influence on us. So he is the one who most in isolation came up with these problems and he had basically nobody, I mean you talk to Blatman [ph?] was interested in classical cryptography, but I've never heard either of them say that Blatman was any terrific influence on Merkel in this matter. So Merkel worked all by himself for several months before he got involved with us. And I never worked with him mano a mano, one to one, we were together at Bell Northern Research for a few months after he got his degree which is probably June '79, but that never, we had different ideas and it didn't go on for very long.

Mary: It seems to me that you were a lone wolf for two years working entirely alone with these ideas, with absolutely no participation from other scholars. I think you were able to work alone as lone wolfs sort of in your own ways but I wouldn't say that Ralph was the most independent; I think you two were both very independent as scholars and as greater intellects, I think you're misrepresenting.

Diffie: Okay so that is a very good point, that is to say, if you're asking what I brought to this, the thing, I brought a great deal of energy to do something that was for a long time very unrewarding, so when I sat out, the time I set out traveling in the Spring of 1973, cryptographic literature of any kind was very hard to find; almost nobody who knew about it professionally [or] was willing to talk about it and even what one should expect of a cryptographic system was hard to know. I spent in some sense, the first two years thinking about the requirements, and came up with such notions as a known plaintext attack, the assumption that the opponents know vast amounts of corresponding plaintext and ciphertext, that's what's usually not true of say you know puzzles in the Sunday Times. Or then extended that to what's called a chosen ciphertext attack that for a long time you cooperate with them. They send you messages, you encrypt them and send them back the results. They send you cryptograms, you decrypt them and send back the results and then at some point you say, you know I'm fed up with you, I won't do anything more. From that moment on, they should be able to do nothing, they should not have learned how to encrypt and decrypt for themselves. So there's a great deal, you know, when I described Merkel as working in isolation, I meant narrowly on the public key problem. So I acknowledge a seed of inspiration from him, that is to say Blatman told me he was working on the problem of secure communication over insecure channels and I persuaded Blatman that it wasn't possible and then it went back to thinking about it. But indeed for the general fleshing out we, Marty and I and Ralph contributed on bounds [ph?] a lot more to cryptography than just public key and a great deal of that resulted from the amount of time I spent studying this and combining the techniques of an investigator and an investigative reporter. So I didn't find very many people who were willing to talk, but I chased them down very energetically and questioned them at great length.

Plutte: Actually I'd like to get into that a little bit because you did take this road trip and you were looking for something and I know you were investigating and you were trying to find information, but there's something underneath that, there's something you were really trying to get an answer to something, what do you think that-

Diffie: Must be the meaning of life, the way you said it.

Plutte: Yeah.

Diffie: So I set out imagining I was going to travel around the world, I intended to bring the car back home before I sat out on the rest of the journey, but I never got any farther at that stage than the US because I met Mary and as we traveled together then for 18 months or so before we settled down and bought a house in Berkeley. But setting out, you know it's sort of been cooped up by dodging- working technical jobs to dodge the draft for the 5 years or so that I'd been out of- 5- 7 years- 8 years I'd been out of school, and so I was fed up and wanted to travel around and I don't know that I took the trip for the purpose of investigating cryptography, and I'm not sure I could articulate very well.

Mary: <inaudible>.

Diffie: I mean I was thinking about it all the time, that's certainly true.

Plutte: And you were visiting specific people here and there, how did you locate people that you even wanted to visit, what was the research you did before you-

Diffie: Okay so that goes sort of as far, I mean a lot of people I visited were friends, I mean I traveled around the country largely staying with people but the explicit people I'd visited cryptographically, I guess there are three sort of different ones early on. One is an old friend of Mary's in Cambridge had worked on this IFF [Identification Friend or Foe] problem years before and it took a long time to get him to talk, but that was lubricated by the fact that we went down just about the same time to see Alan Tritter. And Alan Tritter was work; other person in that group, the key person in cryptography is Horst Feistel. Horst Feistel had been the head of the group that the Air Force came at research center, circa 1950, and he was a member of the mathematics department at IBM Watson. And you think I'm single minded, I mean he basically worked on cryptography; he wouldn't work on anything but cryptography his whole life. He'd been thinking about it as a teenager, he moved from Germany to the US at 20, tried to work on it again during the second world war and they told him they thought it wasn't the time for a German to be talking about cryptography and then after the war, this opportunity came up about the IFF and they began working on it. So I think Tritter had learned a good deal from him. Tritter had also worked sort of indirectly for NSA years earlier and Tritter told me about the IFF notion, and so knowing what laboratory was in question I was able to say to those men, "Oh you must be working on IFF," and he did a double take and then I began to be able to draw him out. That was one direction. The other one goes from Tritter to a man named Jim Simons [ph?]. Jim Simons is the world's best-paid mathematician; he has a hedge fund called Renaissance Ventures and he got there because a friend of mine named Dick Libler fired him about 1968. He was working for Libler at the Communications Research Division of the Institute for Defense Analyses in Prin-

Plutte: Why don't you say it all again?

Diffie: Okay. So, Jim Simons was working for Dick Libler, who was the Director of the Communications Research Division of the I'm sorry. Institute for Defense Analyses, I'm not going to get those right. The problem with this is that for a long time, it was the in group thing to say was "CRD," the Communications Research Division, then they changed their name, etcetera. Anyway, he was working essentially for NSA. Jim Simons was working essentially for NSA at a laboratory in Princeton and he said rather too publicly, that is to Time Magazine, that he wasn't going to do any more secret work until the war was over. Dick Libler said, "We don't do anything but secret work--get out!" And Simons went off and briefly was the head of the Mathematics Department at State University of New York at Stony Brook, but he went into predicting the prime rate was his first gambit and over the decades one financial success after another, he cherry picked some of the best brains out of Dick's organization. Now who was it, Toulouse-Lautrec, some one of those people said, "Life being what it is, one dreams of revenge." And Jim Simons was the best compensated fund manager on Wall Street for several years, billions a year. And he's competition; he's the sponsor of the Museum of Mathematics in New York.

Plutte: Okay. So what I'm gathering is the cast of characters is real interesting. People are really really passionate about this subject. Why this subject? Why do people become so passionate?

Diffie: I don't- why are people passionate about cryptography? I don't know. I'll give you some ideas. One, there is something fascinating about secrets. Cryptography somehow well beyond rationality captures the fascination of finding out secret things and the under the fact is, it is mathematically the solidest of all of the security subjects. It directly leads to difficult mathematical problems and so that drew lots of people interested in mathematics into it. But it's some combination of a sort of a mature professional interest, with a child-like "Oh wow," this is a puzzle, this is a secret, this is a mystery. And so if you imagine taking the Dan Brown sort of fascination with the conspiracies, with the history, with the things that lead way back, here you have something that one, has a lot of that, I mean, there's lots of you know, at that time there is no end of stuff that other people have done in cryptography that they are keeping secret from you. And in my particular way of working, I mean I have- I don't think it could be unique, but I have a rare way of working, which is to work the way a historian or investigative reporter does, going and looking at literature and asking people things and so forth. At the same time, I work directly on the problems. And I've had enough success that has the effect of making people who know things respect me and want to show off to me. So I have much more luck in certain ways questioning crypto-mathematicians than a historian like David Kahn who doesn't know any mathematics, hasn't directly done any cryptography himself does.

Mary: There's another thing.

Diffie: There's another thing?

Mary: All the people, all the persona in this story, they're all what you might call nerds.

Diffie: All what?

Mary: What you might call nerds.

Diffie: Nerds.

Mary: Hellman is the least so. Hellman is the most business one and the most civilized and the most integrated into society. <Inaudible>. Several of the other people. You know this wasn't an accepted social behavior. These people were not as accepted in society at that time. It's hard to think back on that world.

Diffie: Yeah nerds we've done pretty well for ourselves and that gets a certain.

Mary: But at that time they were kind of the kids who were the odd man out in high school; they were laughed at; they had trouble getting dates; they were the head of the Math Club and the Chess Club but not the football hero or something. All of these people got used to feeling secretive about themselves.

Diffie: Oh.

Mary: All these people felt as though they were on the outs. They all became very sympathetic to social groups like Civil Rights movements and things like that, because they felt as though they weren't really in the heart of society and they were sneaky kids. I mean they didn't mean to be, they all had good hearts, but they were always being accused by other people of having something to hide and eventually they felt as though they did and I think that's an intrinsic part of why they went into cryptography. And these were people who considered themselves secretive.

Diffie: You've expressed that better than I could, come over and take the seat.

Plutte: Do you feel that you grew up as an outside to society?

Diffie: Well did I grow up as an outsider to society? A childhood friend of mine said to me in 1971; one of them said to Mary, "This guy had an alternate lifestyle when he was five years old." Actually he didn't know that because I didn't meet him until I was six but he was five, and his brother later said to me, "You were a freak back when nobody was a freak, how did you know to be a freak back then?" So I think this would take us on a long detour, but my parents were very out of the ordinary in the neighborhood in which I grew up. My parents are southern kids; my mother's from Tennessee, my father's from Texas, they met in Madrid in 1925. They married in Paris in 1928, they moved to New York in 1930 and I happened to have been born in Washington because of the war, but we grew up in an upper middle class, mostly Jewish neighborhood in which, I still keep remembering you know, I was just so out of touch with the culture of that neighborhood, that I still keep remembering things that I didn't understand at the time that I now understand. So yeah I think with some legitimacy I felt like an outsider.

Plutte: So do you feel that's a kind-

Diffie: I don't know if you ask Marty. Marty had the same experience the other way around; Marty Hellman grew up in the Bronx in a goy-sh [non-Jewish] neighborhood.

Plutte: So do you feel that regardless of that that this is a motivation for a lot of people who get into cryptography that they are-

Diffie: I don't know. You know this would, I know some people and the aforementioned Frank Rowlette [ph?] simply needed a job; applied to the civil service _________ and got hired into a job that he did then as remarkably as anybody else has ever done it. Friedman who was his boss got drawn into it by the First World War, he was working at a laboratory that was working on the Shakespearean ciphers and he was working on cryptography for literary criticism. I didn't know the other two guys Friedman hired as well, so I don't know exactly why they started doing it. Subsequent to our work and you'd have to divide it into periods, so you look at people mostly worked for the government and why they worked for the government and then after we made the subject popular it became very visible as an academic subject and something that you could get papers published about something you could do a doctorate on.

Plutte: Actually it almost feels like you'd sort of touched on it the eras of the different kinds of people who worked on cryptography were motivated by their times, <inaudible> a lot of this stuff happened in the sixties and seventies which was a really different time than the thirties and forties. Do you feel that the era in which you were doing a lot of this work influenced you?

Diffie: Of course. Of course. I mean I had so let me start out, bore you with a little, you know, just a general history of the subject. The modern era of information security starts with radio. Radio bypassed all of the known information security techniques which consisted mostly of locking your drawers and guarding your building and vetting the personnel and things like that. And suddenly there's this new technique and only one known information security technique which had been a backwater, right? ______ cryptography has been around a long time but it was a shadow of what it is today. The First World War just made this an absolute necessity and from the late teens on we have been in an era of the automation of cryptography. Now socially, prior to that, it was an esoteric, but not a terribly secret- not a secret subject the way it became at a later date. The whole machinery of bureaucratized machinery of governmental security and clearances and oaths and so forth had a big surge in the 20th century. So if you look at their other kinds of military secrets that were around in the 1890's and so forth, torpedoes, mines, they were an esoteric knowledge; the distinction between the sort of mainstream practitioners and the arms merchants and the smugglers and so forth was not as sharp as it would seem to be later. Then from circa 1930 to 1970, the governments managed to dominate cryptography and in particular in the US after it was codified in 1952, NSA managed to squeeze out everybody else working on the subject; shut down that Air Force laboratory, leaned on quite a few- captured basically the one mandate with exception of minor points from the CIA to work on this. The trouble is, that couldn't hold and it's a movements, political science sort of explanation would say well, there's a rising need for it and electronic networks, and there's a falling cost of either practicing it or doing research in it, because of the falling cost of computers. And then at a personalities level, now for example, Horst Feistel, who was you could have said everything Horst Feistel knew was secret; I mean he did all when he was working for the Air Force. But that job dissolved; he worked for Mitre for a while, he got squeezed out of doing cryptography there; then he went to IBM which was a good bit more independent of the government and so he just you know, went back to doing what he liked to do. So I think that's one of the people. You know, you can find certain people with a nut passion for the subject. I have developed one, right, but..

Mary: You were- the reason that everybody was nervous about you was because you were the first private cryptographer in modern times, really.

Diffie: That could be.

Mary: And the government just couldn't wrap its mind around that.

Diffie: So it's actually, it's more assertive than that on my part. I mean my view, when I was trying to talk people into working on cryptography in the last sixties; my basic view was that cryptography was the one security technology I knew that could protect the individual. At the time, I was in the same building with a project called Multics, which is the ancestor of UNIX, and is the most ambitious computer operating system project of all time. Multics had very elaborate file protection mechanisms and I thought to myself, what good is that? Right? They'll put a subpoena on system programmers. System programmers aren't going to go to jail to protect your files; they'll just turn them over. And the only thing I saw would protect your files was if you had them encrypted so that the system programmers couldn't read them. So that's the way, that's the type, whether we live, we now see that as a lot less, you know, there are a many a slip between that conception and getting it actually to work, but that was the way I saw it at the time. So I was not only independent of government, I was very assertively so. I didn't want to go to work for them to get a clearance with them, etcetera; my attitude <inaudible> I said, they know a lot of things very valuable to human privacy at NSA that they won't tell us, and we have to set out to rediscover them.

Plutte: That's good.

Diffie: Have you thought of a career as a teleprompter?

Mary: <Inaudible> that there would be a world in which remote communications would be one of the primary _______ of interaction. I could not see that. That was forty years ago. I just thought he was mad. And he told me, we were sitting in the school yard and he said, I asked him what he was interested in and he started talking about this and he said that some day there would be a world in which relationships, friendships, even lovers somewhat would be conducted remotely. Business relationships; and there had to be some way for people to know who they were dealing with. So he was interested both in authentication and in secrecy very, very early. And he was really consumingly interested in it, and I in my superior wisdom tried to assure him that that couldn't possibly be true; that you know, why would any- it seemed like a cold universe to me where you'd want to conduct-

Diffie: It probably still does.

Mary: I do think that the universe is a little colder than I like but emotionally, but he foresaw both of these needs at a time when it was impossible. I mean so many things had to be invented. So many pieces of the puzzle had to come together. He was not, I don't mean to misspeak but neither of us could foresee how fast it would happen. Once he invented cryptography and everything started happening at once, you know that was very exciting and all, but it still seemed like a narrowly academic sort of thing and government people were tremendously interested but it seemed as though it wouldn't leave a ripple on the public mind and then all of a sudden, industry became very interested in becoming computerized and computers could communicate with other parts of the world and things became non-local and the world he envisioned suddenly came to pass. It was like he rubbed a lamp or something and suddenly it sprang up. But nobody I think nobody could have foreseen the speed with which it- but he foresaw all of that. And it's so strange.

Diffie: So if he's so smart, why ain't he rich? Hmm.

Plutte: So forty years ago did you foresee a connected world and what did you think the issues would be with that?

Diffie: Forty years ago I saw through a grass brightly and through a grass darkly. My vision when I got into cryptography; I was aware of the Arpanet, it was already around, I had used it, but I did not see that transformation the way it's occurred. I imagined everybody having a secure telephone. I thought we'll have 100 million secure telephones in North America and you know, any two of those people might want to talk to each other privately, so I had sense of scale, right? But I didn't have a clear, much later I didn't have a clear sense; like many people I saw what was needed, I saw the problem the web solved, but I didn't see quite the right things about how to do it. But what Mary was referring to is a conversation we had in the summer of 1973 sitting in a school yard in Willingboro, New Jersey and we were there walking dogs and a saluki named Jabi [ph?] was running back and forth at 40 miles and hour, and as I told her and Mary remembers this much more vividly than I do; I remember the occurrence, sitting on, I think on a see saw, something like that and talking about this, and that I did say that we're going you know, in telecommunications world, and of course I also thought of something that has only barely come to pass so far, which is moving into space. I mean if we move out to where we occupy the moon and the planets and so forth, then they'll really be the cost of going from one to another physically will so dwarf the cost of communication that it will make this an utter necessity and I can't tell you whether I'm surprised or not, the degree to which a globalized world produced one in which people have relationships, discover people and may not meet these people for years or ever. Kind of like 84 Charing Cross Road; it's a book about a 20 or 30 year correspondence that the woman had with the booksellers at 84 Charing Cross Road and she wrote to them and ordered books from them and sent them things during rationing and never got to see them, eventually all died off.

Plutte: Okay.

Mary: The interesting thing is that these were people who weren't that much in the mainstream when they started out and I said-

Plutte: You really should be interviewing her. ______ Conference did a great job with that and got some very good footage.

Mary: I said _______. When I was a child, when Whit was a child, they kept talking about one world as an ideal that people would all get along together, people would communicate with each other; people would deal with each other. These out of the center guys made it happen. They brought everybody else together. It's an amazing story that people who were so eccentric made the mainstream able to communicate freely over boundaries, across political systems, and it is one world now. Maybe it had been.

Diffie: Kind of like a country house mystery, I still have to figure out who got murdered.

Mary: <inaudible> to watch it.

Diffie: <inaudible> the list of questions was so long when I started reading it I never got beyond three or four because I thought I was supposed to send you a written answer or something.

Plutte: No I think that actually to me we've covered everything in great detail that I have as questions, how about you? Are you interested in talking on camera for a few minutes?

Diffie: Goodie.

Mary: I'm willing to, we didn't want to <inaudible>.

Diffie: You should stop crying and come talk on camera.

END OF INTERVIEW