Podcast Name: *ACM ByteCast*
Episode: Whitfield Diffie and Martin Hellman - Episode 37

Welcome to the *ACM ByteCast* podcast, a series from the Association for Computing Machinery! The podcast features conversations with researchers, practitioners, and innovators at the intersection of computing research and practice about their experiences, lessons learned, and visions for the future of computing. In this episode, host Rashmi Mohan interviews guests Whitfield Diffie and Martin Hellman who are the 2015 ACM Turing Award winners as the joint creators of the Diffie Hellman key exchange. They introduced the world to the transformative new idea of public key cryptography. Diffie is currently a consulting scholar at the Center for International Security and Cooperation at Stanford University. Hellman is a professor emeritus of electrical engineering at Stanford University. He is also a published author and a recipient of the RSA Lifetime Achievement Award, inducted into the National Cybersecurity Hall of Fame.

To begin, Whitfield Diffie shares his interest in cryptography began from his interest in the history of cryptography. He was not good at mathematics, and as a way to dodge the draft, he dived deep into computer science. Martin, on the other end, got into cryptography by first involving in information theory, which was his PhD. However, Peter Elias, one of the original contributors to information theory, gave him a copy of Claude Shannon's paper connecting information theory and cryptography. That's when Martin realized maybe he could do work from cryptography. Whitfield then shares his advice to people who are not academically fit. He says that his advice is to have good luck. Martin adds and says Albert Einstein had trouble in school. So school isn't designed for everybody. They also share their story on how they met. People used to say that Martin was too lazy to work in cryptography. It turns out most of the great breakthroughs are seen as foolish a priori.

Next, Diffie and Hellman share their insights on the importance of democratic research. They then share what their aha moment was like in public key cryptography. They were working to solve two problems, one which took five years and the other one ten years. In the modern description, the ten-year one would now call key management. Basically, they came up with the concept of a public key cryptosystem but didn't have a workable system for either key exchange or digital signatures. Martin continues to add on the absolute widespread use of their work when they first came up with this idea. They thought that within five or ten years, commercial cryptography would take off; it took more like 10 to 20 years. But the internet in the mid-90s was what catapulted it. Whitfield and Martin also shed more light on engagement in the evolution of cryptography and how the research evolved from the security organization perspective.

Finally, these two partners talk more about their journey associated with national security. There's a 50% divorce rate that shows that at the marital level, if you look at the wars that the United States has been involved in over the last 40 years, every single one of them has been needless and has hurt our national security rather than help it. And yet we don't learn from our mistakes. We really need to rethink national security. Whitfield shares his thoughts on the journey of cryptography, where he says that his virtue in this field is length and breadth rather than depth. They then share their thoughts on Quantum Computing. If quantum computing

comes through the way the physicists of the process are promising, and IBM certainly put on a very moving demonstration and discussion at its summit in New York recently, it will destroy Diffie Hellman and RSA, the public key cryptosystems that have been the workhorses of the last 40 years. They also touch on end-to-end encryption and the field of technology in the next five years.

Key Takeaways:
2:04 - About Whitfield Diffie and Martin Hellman
4:49 - Advice to young people not good in academics
6:24 - How Whitfield Diffie and Martin Hellman met
9:44 - Finding the right partner to solve problems
11:16 - Importance of democratic research
13:05 - The expected successful moment of public key cryptography
16:14 - Engagement in the evolution of the field of cryptography
18:37 - How the research evolved from the security organization's perspective
19:26 - The journey associated with national security
21:26 - How individuals can really get involved
24:10 - What Whitfield Diffie enjoyed about the journey of cryptography
25:45 - Quantum Computing
28:38 - Thoughts on end-to-end encryption
30:58 - The field of technology in the next 5 years

Links
Learn more about Whitfield Diffie
Learn more about Martin Hellman
Learn more about Rashmi Mohan
Learn more about the ACM ByteCast podcast at https://learning.acm.org/bytecast

Tags
Whitfield Diffie, Martin Hellman, Diffie Hellman, ACM ByteCast, Cryptography, Commercial Cryptography, Public Key Cryptography, Information Theory, National Security, Quantum Computing, End-to-End Encryption, MIT, Algorithms, Computing, Research, Technology, Internet, Cybersecurity, Computer Science