Whitfield Diffie

Bailey Whitfield Diffie is responsible for pioneering public key cryptography. He was responsible in part for the now widespread method of distributing keys called Diffie-Hellman key exchange. This solution to a fundamental problem in cryptography was first put forward in Diffie and Hellman's paper *New Directions in Cryptography*. This is what spurred on the development of asymmetric key algorithms.

After his work on these fundamental security concepts he moved on to work in Sun Microsystems for years, followed by the ICANN,and has served as a visiting scholar at a number of Institutions, including Stanford.

Early Life

School and University

Diffie was born in Washington, but raised in Queens. His father was a Professor and his Mother was a Scholar, so he was raised in a fairly academic environment. When he was ten years old, his father brought home books on Cryptography from teh City Library and this sparked Diffies interest in computers.

Even though Diffie did not apply himself in High School he still managed to secure a place in MIT due to his high SAT scores. He did have an interest in Mathematics throughout high school however and this is what he went on to study at MIT. Whilst studying at University he began to program computers, however he considered them 'very low class', as he was a pure mathematician and was interested in more advanced topics.

Career

Diffie's rekindled interest in Computers after University can be attributed to him trying to avoid the Vietnam Draft. To avoid getting drafted he joined the MITRE Corporation, where he became a residence guest at the MIT artificial intelligence lab. He also worked on a general purpose algebra system called Mathlab(Macsyma). After this he then moved on to the Stanford artificial intelligence lab.

Stanford is where Diffie started becoming more interested in cryptography and privacy. He read *The CodeBreakers* and worked on his first ARPAnet security problem. Diffie soon tired of this and decided to travel around the US to learn as much as possible about cryptography.

Cryptographic Research

It was at this stage in his life when Diffie made his mark on the computing world. He

wanted to solve two big problems that he saw with current cryptographic methods:

1. All current systems were dependant on a third party, which made them vulnerable.
2. There was a need for a digital signature to allow authentic transfer of information online.

There was a lot of information on Cryptography that Diffie was not allowed to access, as most of it was kept secretive by the National Security Agency(NSA) at the time. His search brought him all over the country, including back to New York where he talked to someone from IBM Research. IBM research was one of the only non governmental agencies that were also looking into Cryptography, however they were not able to divulge any information so he was put onto contact with Martin Hellman.

Martin Hellman was an electrical engineering professor at Stanford who was also looking into Cryptography research, so Diffie and him teamed up and shared ideas.

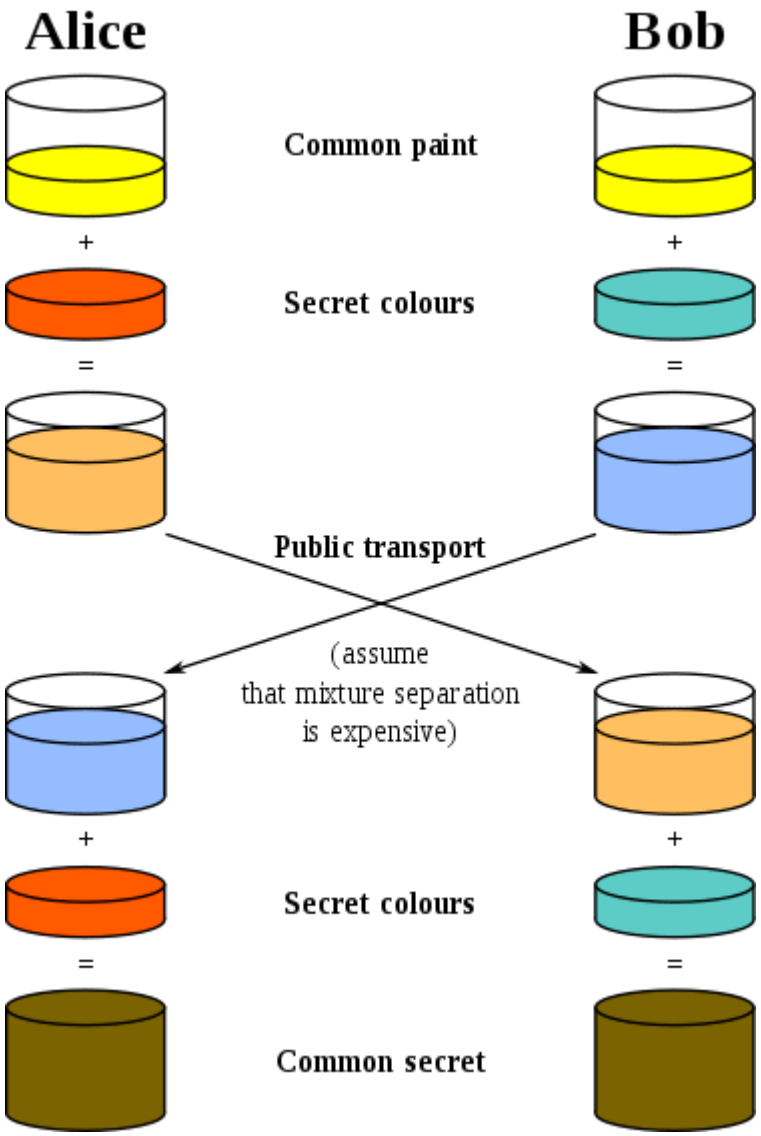
Asymmetric Cryptography

This new technology is what has made such an impact on the world today. *Asymmetric* or *Public Key Cryptography* is used in most, if not all, secure web communications to this day. It solves the key distribution problem and broke cryptography free from the control that governments could have whereby they would control the cryptographic technologies used.

Diffie-Hellman Key Exchange

A classic example for how Diffie-Hellman key exchange works is as follows:

- Alice and Bob need to communicate securely.
- They both have a secret color, the aim is that they can make a common secret color at the end.
- Alice and Bob both choose publicly to use Yellow as their public color.
- If Bob mixes his secret color with Yellow, and sends it to Alice, anyone who sees this communication will only see the mix.
- When Alice gets this, she can mix her secret in as well.
- Alice also sends Bob her mix of colors and bob mixes in his secret color too.
- They now have a common secret color that only they know.



The above method can be implemented using modular arithmetic and was a massive breakthrough in the way information could be sent. This was a great step forward for personal privacy. Diffie and Hellman had previously criticized the DES protocol for not being secure, and they were proved right when it was shown that the NSA interfered to shorten the Key length.

This sort of interference by Government Agencies is no longer proved possible with this type of cryptography and freed people from an effective monopoly.

For their work on this impressive breakthrough, Diffie and Hellman won the Turing Award in 2015 for "*fundamental contributions to modern cryptography. Diffie and Hellman's groundbreaking 1976 paper, 'New Directions in Cryptography', introduced the ideas of public-key cryptography and digital signatures, which are the foundation for most regularly-used security protocols on the internet today.*". Diffie has also received an honorary doctorate from the Swiss Federal Institute of Technology and is a fellow of two Foundations. He has various other awards for his work on Asymmetric Cryptography.

Conclusion

It is unquestionable that Whitfield Diffie has made a profound impact as a Software Engineer, laying the groundwork for a whole new field of cryptography that is in use all over the internet today. As well as this industry impact he has also definitely continued his impact in his research and visiting scholar positions. One of the most admirable things about his discoveries is that he stated he always believed in privacy for individuals rather than for government. This breakthrough was good for everyone's personal freedom and we should be grateful that he did not let the government, or any other agencies interfere.