Non-Secret Encryption - a “SECRET” no longer.

By Patrick Bomgardner, Standby Active Reserve, Center for Cryptologic History.

Self-identified iconoclast Whitfield Diffie who said, “I was always concerned about individuals, an individual's privacy as opposed to government secrecy,” and who in 2015 along with Martin Hellman won the Turing Award – the “Nobel Prize for Computing” – for fundamental contributions to modern cryptography, can now add 2020 Cryptologic Hall of Honor (HoH) Inductee to his long list of awards, accolades, and accomplishments.

Diffie’s 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. According to his HoH nomination, “In this single contribution, Diffie achieved a history-making advancement in protection of privacy and information security, and created an entire new field of scientific inquiry.”

However, unknown to Diffie and Hellman at the time, asymmetric key algorithms were also secretly developed by James H. Ellis, Clifford Cocks, and Malcolm Williamson at the UK’s Government Communications Headquarters (GCHQ) in 1973. In its official public disclosure – not made until 1997 - GCHQ claimed that these researchers had independently developed the Diffie-Hellman key exchange, and what would later become known as the RSA asymmetric key encryption algorithm. The GCHQ cryptographers referred to the technique as "non-secret encryption," or “NSE.”

Simply put, in public-key cryptography, or asymmetric cryptography, anyone can encrypt messages using the public key, but only the holder of the paired private key can decrypt. Security depends on the secrecy of the private key. In the Diffie-Hellman key exchange scheme, each party generates a public/private key pair and distributes the public key. After obtaining an authentic copy of each other's public keys, the parties can compute a shared secret offline. The shared secret can be used, for instance, as the key for symmetric cipher. It is the basis for the billions of secure banking and commercial transactions conducted on https internet sites.

Inside NSA, Andrew J. Arenth of the Communication Security (COMSEC) organization provided a succinct summary and damage assessment in a 15 October 1976 Memorandum for the Record -- Subject: Non-Secret Encryption: A Non-Secret. According to Arenth, Malcolm Williamson, in a TOP SECRET 1974 paper, originally described the notion of Non-Secret Encryption based on the difficulty of computing logarithms over a finite field. In their paper presented at the June 1976 National Computer Conference, Diffie and Hellman brought the abstract concept of Non-Secret Encryption into the public domain. They proposed it as a solution for key distribution on a multiuser network, but couldn’t yet make it work practically. They still needed to figure out an encipherment process “E” which is held in a public pool and the secret decipherment process “D” held by each user such that “D” cannot be easily obtained from “E.” James Ellis then confirmed in another classified paper in July of 1976 that Diffie’s and Hellman’s abstract concept could be achieved, but he prematurely and erroneously opined that they had little idea how to get to “E” and “D.” A month later, Diffie and Hellman did indeed get

there and wrote “New Directions in Cryptography.” Their new technique made use of the “apparent difficulty of computing logarithms over a finite field…” As a result, Arenth concluded that “Non-Secret Encryption is a “SECRET” no longer.”

At the time, Diffie’s and Hellman’s coincidental and inadvertent public disclosures of what NSA and GCHQ considered to be classified information had ominous implications for the intelligence agencies’ monopoly on cryptology. “Every company, every citizen now had routine access to the sorts of cryptographic technology that not many years ago ranked alongside the atom bomb as a source of power,” wrote Stephen Levy in “Battle of the Clipper Chip.”

As might be expected, at what was then jokingly called “No Such Agency” there was a great deal of angst and foreboding. NSA mathematician Dr. Robert E. Kibler could readily see that “many dangers lie ahead." In his Winter 1979 NSA Technical Journal Article “Public-Key Cryptosystems,” Kibler worried that:

> Perhaps one or more of the public-key algorithms will be implemented in a way which will provide better security than many currently available commercial devices, further hampering our SIGINT analysts who are already beset with difficulties as more and more products become available. But the surest hardship we must endure is the growing awareness and education of the world at large; the technical advantage which we now enjoy will certainly be eroded as others discover and disseminate ideas which formerly were known (as we suppose) only to us.

An interesting anecdote illustrates the early relationship between Diffie and the intelligence community. In a September 1982 classified memo, James Ellis describes a meeting he had with Diffie – long before Ellis’ involvement in non-secret encryption was publicly acknowledged. Because his involvement was then still classified, Ellis was wary of meeting with Diffie, not knowing what to expect, and had put off several requests to meet with him. However, Diffie was persistent and Ellis finally relented. Ellis consulted GCHQ authorities, as well as those at NSA, who told him that Diffie, “was causing trouble, that he was looking for snippets of information, and he was completely uncleared.” Ellis was convinced that Diffie was looking for information on NSE.

Ellis’ account of the meeting is somewhat amusing. Although he offered to take Ellis to dinner in Cheltenham, Diffie insisted on going to a pub instead of a restaurant – a fact that didn’t sit well with Ellis. “I had been pressed into accepting an invitation to dinner and then deprived of it. It was hardly the way to ingratiate oneself; a salesman doing this would get sacked. I can only assume that he felt that a bar atmosphere, with drink, would help free my tongue.”

They wound up at the Star in Regent Street because it had draught cider, and they had a snack and three pints each of Bulmer's "Strong Bow" which left Diffie, who was not used to strong cider “befuddled,” as Ellis put it. Ellis walked him around Cheltenham to sober up, then took him home and gave him black tea till he was in a fit state to drive.

Despite this, Ellis found Diffie to be “charming, plausible, and quite expert in portraying things to induce confidence.” Early in their conversation, Ellis was able to fend off Diffie’s oblique solicitations for information by going so far as to deny even being a cryptographer. Then Diffie went for a more direct, “shock tactic,” suddenly asking how Ellis came to invent NSE. Ellis

replied “that is what you did. Who said I did?” Diffie later opined that Ellis and Cocks must have been peeved that he and Hellman got all the credit for their work. Ellis replied that he could not discuss such matters.

In the end - having gained some knowledge and given practically none – Ellis was glad to have met with Diffie. He came to the conclusion that “we should be neither fearful nor complacent about meeting people like Diffie.” While, as did a lot of NSA and GCHQ employees of that time, he thought it best not to, if such meetings became unavoidable, “we should remember that they have no magic powers to get information unless we give it,” but, “one cannot safely relax.” Ellis thought it important to get as much prior information as possible to help avoid being misled.

Over the years, NSA would keep a wary eye on Diffie’s publications. They would clash over Diffie’s criticism of the security of the Data Encryption Standard and NSA’s alleged nefarious role in helping IBM develop it – but that’s an article in itself. They would argue over the rights of academics and non-government cryptologists to publish findings without NSA’s consent. Yet, despite all the hand wringing and pearl clutching, the cryptologic world did not end, NSA continued to successfully prosecute its mission, often with the help of academics such as Diffie, and consumers can buy things on the internet knowing their transactions are secure. For his part Diffie would come to appreciate the importance of NSA in keeping the nation safe and would participate in several Center for Cryptologic History-sponsored Cryptologic History Symposia. Not only would he become Vice President and Chief Security Officer of Sun Microsystems, but also an honorary member of the Phoenix Society - an association for NSA civilian retirees and prospective retirees.

As for those GCHQ cryptologists, sadly James Ellis died on 25 November 1997, a month before GCHQ made the public announcement, and Malcolm Williamson died in 2015. Only Clifford Cocks, who was elected as a Fellow of the Royal Society in 2015, survives. Their work was named an Institute of Electrical and Electronics Engineers (IEEE) Milestone in 2010. In March 2016, the director of GCHQ made a speech at MIT re-emphasizing GCHQ's early contribution to public-key cryptography and in particular the contributions of Ellis, Cocks and Williamson.