Vigenère through Shannon to Planck – a Short History of Electronic Cryptographic Systems

Peter C J Hill, *Life Senior Member, IEEE*
Cranfield University, DCMT, Defence Academy of the United Kingdom
Shrivenham, Swindon, Wiltshire, UK
Email: p.c.j.hill@cranfield.ac.uk

***Abstract*—The history of cryptography goes right back to ancient times but modern electronic coding for secrecy essentially uses similar principles for poly-alphabetic ciphers and their variants; recent algorithm developments are based on the rules of secrecy as enunciated by Claude Shannon in the late 1940's; many of these schemes are published as standards. We now have public-key systems, and quantum cryptography is now beginning to emerge from the research laboratories.**

***Index Terms*—Authentication, cipher systems, cryptography, digital signatures, history of cryptology, information theory.**

I. Introduction

The science of secret writing, or cryptography, goes back many thousands of years and is currently employed by the military, diplomatic, commercial and banking communities. The Spartan military 'skytale' around 500BC used a simple scrambling, or *transposition*, process. Later, another process, character *substitution*, emerged; the Caesar code is a well-known mono-alphabetic example from around 50BC.

The military regard cryptography as a weapon system in an information-theoretic war-game fought over the battleground of public channels; the cryptographic community, who devise cipher systems, and their clients or good guys, who use them, allied against the code-breakers or cryptanalytic community, or bad guys. Cryptanalysis leads to a *privacy* problem, whereas 'spoofing' constitutes an *authentication* problem. The strength of a crypto-system depends on the secrecy of the *key* and the complexity of the *algorithm*.

The first serious crypto-systems were the Vigenère poly-alphabetic ciphers, around mid-16th century, which used secret keywords iteratively derived from either the plaintext or previous ciphertext; these codes remained unbroken for about 300 years, finally being cracked by Kasiski, a Prussian army officer. With the invention of the electric telegraph, Babbage and Wheatstone entered the field in mid-19th century. The onset of WWI saw Vernam stream ciphers being used. These strong codes combined input plaintext with 'random' key-streams; nevertheless, Friedman et al managed to break these ciphers using statistical techniques.

Interest in cryptography grew significantly with WW II. The Germans were using an electromechanical rotor machine known as *Enigma* (Scherbius 1919), and later *Fish* 'one-time pads'. These codes were broken by some brilliant mathematicians led by Turing, with smart exhaustive code-searching using the *Colossus* computer at Bletchley, UK. At the same time in the USA, Claude Shannon, later known as the father of *information theory*, was evolving the fundamental principles of cryptography. These turned out to be the sequential use of substitution and transposition over many *involute* stages, to generate an *invertible* super-encipherment system in which both the key and also the plaintext statistics are well hidden. These principles are still in use today with systems such as the Data Encryption System (DES) and the International Data Encryption Algorithm (IDEA). Shannon also laid down the basis for perfect, ideal and *one-time pad* crypto-systems, including the important concept of *unicity distance*. Key length became a critical issue and DES was strengthened into the current 'unbreakable' Advanced Encryption Standard (AES); details are secret and held by NSA in the US and GCHQ in the UK.

In 1976, a novel *asymmetric* 2-key public-key system (PKS), was announced by Diffie & Hellman. The best-known algorithm, based on modulo prime-number mathematics, was later derived by three outstanding mathematicians – Rivest, Shamir & Adleman (RSA). Inter alia, RSA PKS solves the important problems of *digital signatures* in authentication and also key distribution, as well as providing data privacy. It turned out that scientists at GCHQ had secretly pre-invented the PKS system 2-3 years earlier. In 1991 a political stir arose in the US when Zimmermann publicly released Pretty Good Privacy (PGP) crypto-system based on RSA and DES; the argument for/against publicly available strong codes continues.

At the research level, *quantum cryptography* is fast developing; encrypted messages are made secure by the 'laws of physics'. Quantum-crypto exploits the Heisenberg 'uncertainty principle' and the phenomenon of 'quantum uncertainty'; photons are sent in one of four polarizations, which are chosen at random. An eavesdropper intercepting the photon stream will inevitably insert errors into the channel and be detected.

The paper traces the history of cryptography from the very early days through WWII to the present time.

II. The Start of Cryptography

The story of secret writing goes back to ancient times [1], with the original 'classic codes' being *mono-alphabetic*, the so-called *Caesar codes*, dating from around 50BC. Communications start as plaintext (PT) in the public channel, are encrypted into ciphertext (CT) for the secret channel, and then decrypted back into PT. In symmetric systems both sender and receiver use the same

key. Means have to be found to generate suitable key(s) and secretly distribute them to Alice and Bob; this key management process also needs a secure channel! The eavesdropper, cryptanalyst, or bad guy, known as Eve, sits on the cipher channel and, either taps the line and tries to break the code, or attempts to masquerade as a bona fide user (Fig. 1) in order to inject false messages into the secret channel.

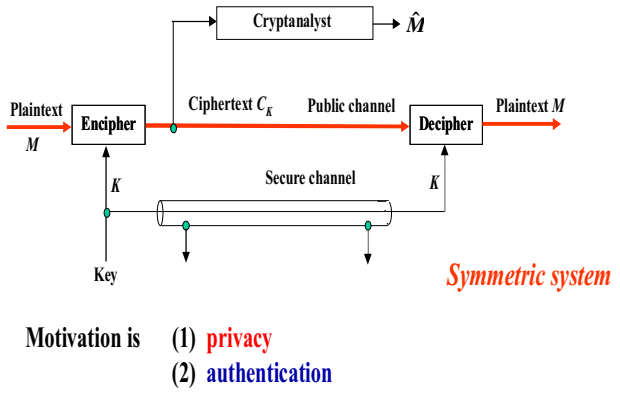

Fig. 1. Basic encryption/decryption system

Mono-alphabetic ciphers have limited *key-space*. For example, the simple Caesar codes, with linearly shifted alphabets for PT to CT coding, have a key-space of only 25 characters; progressive shifting is very similar.

This *substitution* process becomes much stronger if PT characters are mapped uniquely into arbitrary CT characters without repetition (bijection principle); we now have 26! keys, ie a key-space of roughly 4 x 10^{26}.

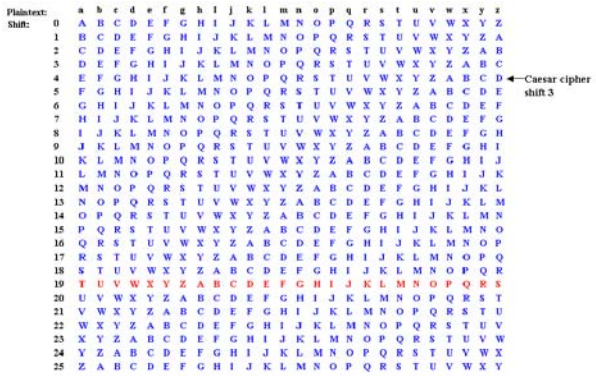

Fig. 2. The Trithemius progressive-key table

The principle of alphabet substitution is shown in the key-table of Fig. 2. Greater security may be obtained if the substitution is carried out with a jumbled alphabet but we now have a key distribution problem which is more severe if substitution is made *poly-alphabetic*, ie we have a number of jumbled alphabets used in succession. Then a compact key statement can be generated using a keyword. A simplified version of this scheme was the Vigenère cipher, published in 1586, in which keywords specify cyclic linear shifts without jumbling. For example the keyword 'HISTELCON' has a period of 8 and points to alphabets 7, 8, 18, ---- 14, 13 and is easily exchanged between sender A/B and recipient B/A. Stronger versions of this code use the running PT or even the previous CT characters as non-cyclic keywords. Modern cryptographic systems are essentially based on poly-alphabetic ciphers, as they are more robust against attack using letter frequency analysis. However, the Vigenère system was finally broken by the Prussian military (General Kasiski), and by Charles Babbage; apparently Charles Wheatstone also managed to crack these ciphers [2]. The method of attack, which was never published at the time, is based on the fact that, with keyword repetition, particular sequences of CT will inevitably appear at multiples of the key-length in a long message, and letter frequency analysis can then lead to the keyword.

In the 1860's, Wheatstone developed a novel type of geared concentric disk cryptograph machine in which the outer ring had PT letters in alphabetical order and the inner ring letters of the CT in random order. However, pre-dating that scheme was a cylinder cipher machine with 36 randomly ordered disks carrying jumbled letters on their peripheries – this poly-alphabetic device is attributed to US President Thomas Jefferson; it was apparently later re-invented by the US Navy in the 1920's and used for quite some time. The key-space is enormous at something like 10^{40}.

Mono-and poly-alphabetic codes are not restricted to enciphering single letters.

	1	**2**	**3**	**4**	**5**
1	H	I	S	T	E
2	L	C	O	N	A
3	B	D	F	G	J/K
4	M	P	Q	R	U
5	V	W	X	Y	Z

Fig. 3. The Polybius Square

In its original form (Fig. 3) a codeword (for example, 'HISTELCON') is written in a 5x5 grid and the remaining alphabetic letters are inserted in sequence; message PT letter pairs (*digraphs*) are then coded into X/Y coordinates for the CT. The *Playfair* system, invented by Wheatstone in 1854, is a more advanced cipher where the PT/CT relationship is based on four rules of diagonal table readout; these schemes are more difficult to break as letter frequencies are compounded. It is worth noting that the German ADFGX field cipher, invented by Nebel in 1918, is a Playfair system in which the X/Y CT coordinates are given by the 5-vector ADFGX.

III. The War Years

There is no doubt that both WWI, and WWII, spurred on a rapid development of crypto-systems; in fact it is fair to say that, the use of cryptography and code-breaking in military and diplomatic communications [3], has in the past, actually altered the course of history! Key events such as the Zimmerman telegram in the US and the breaking of Nazi German codes by the UK are clear examples from WWI and WWII respectively. This author makes no apology for emphasizing the *Enigma* story here [4], [5], [6]. After WWII, Churchill remarked that the UK code-breaking establishment at Bletchley Park (BP), '*were the geese that laid the golden eggs and never cackled*'. The Playfair type of diagraph cipher, described above, was used for tactical operations by British forces in the

2nd Boer War and also in WWI. Australian and German forces used them in WWII; they are fast and robust to crypto-attack. However, it soon became clear that much stronger cipher codes were required for secret military signals communication channels [7]. Moreover, electro-mechanical cipher machines and later fully electronic cryptography were on the horizon; soon there would be a requirement to encrypt traffic on digital networks [8].

The Playfair type of digraph cipher, described above, was actually used for tactical operations by British forces in the 2nd Boer War and also in WWI. Australian and German forces used them in WWII; they are fast and robust to crypto-attack. However, it soon became clear that much stronger cipher codes were required for secret military signals communications [7]. Moreover, electro-mechanical cipher machines, and later fully electronic cryptography, were on the horizon; soon there would be a requirement to encrypt digital traffic on networks [8].

In 1917 Gilbert Vernam (AT&T) invented a teletype cipher in which a 5-channel punched tape key sequence is combined, character by character, with a PT message to produce the CT. Decipherment is done by re-combining the same *key-stream* with the CT, with the original synchronisation, to produce the PT; correct operation of the system depends on perfect timing between the PT/CT and key streams. Although the original Vernam cipher was used to encrypt Baudot teletype code, the very same principle is used in modern *stream ciphers* in which the PT is XORed with a pseudo-random key-stream to generate the CT; decipherment is as before. An example is the C4 Vernam cipher used on the Internet. In the mid-1920's Joseph Mauborgne (US Army Signal Corps) patented a stream cipher with a purely random key-stream. The system is actually provably unbreakable and is known as a *one-time pad*. It was used extensively in WWII and beyond to encrypt highly classified channels such as the Churchill/Roosevelt hot-line; key-code disks were actually flown across the Atlantic.

Fig. 4. The Scherbius Enigma cipher machine

The Enigma story has been extensively covered in the literature and media together with a feature film based on the novel by Robert Harris. In summary, the story starts with the invention of an electro-mechanical rotor poly-alphabetic substitution cipher machine by Arthur Scherbius in Germany after WWI (Fig. 4). The basic stages: a keyboard for PT input, a scrambling unit for coding the PT into CT, and a display board with various lamps to indicate the CT letters; there were 3 (later 4) 26-position stepping rotors with different wiring patterns between the contacts. When Enigma was adopted by the Wehrmacht, they added a plugboard with 13 pairs of partly inter-connected alphabetic sockets. With the order of the rotor wheels arbitrarily set, and the number of plugboard cables increased from six to ten, the keyspace is around 1.6×10^{20}. Later the Germans introduced the 'Secret Writer' – the Lorenz machine, which was used to encrypt 5-digit Baudot coded messages; this was a double Vernam cipher known to the British as 'Fish' (or 'Tunny').

The UK created a secret establishment for cracking codes, Station X (Fig. 5). This was the Government Code & Cipher School (GC&CS) at Bletchley Park (BP), which employed up to 6000 staff by the end of hostilities. The crypto-analysts were top-flight mathematicians, scientists & engineers, chess-players, linguists etc, the most famous being the Cambridge mathematics don Alan Turing, father of the modern programmable computer.

Fig. 5. Bletchley Park Code & Cipher School

BP got its enciphered signals from radio stations known as Station Y. After the war the code breaking operations moved to GCHQ Cheltenham.

The code analysis work at BP was greatly assisted by Polish mathematicians, Marian Rejewski and colleagues, who had previously broken the commercial Enigma and also provided the British with technical drawings of the machine; they had developed in the 1930's, electro-mechanical *bombes* for fast investigation of the plug-board scrambler wiring [4].

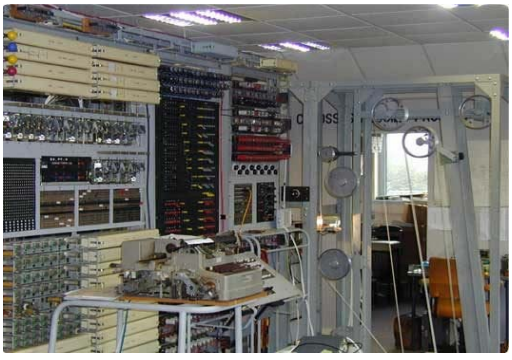

Fig. 6. The Colossus computer & bombes at BP

The fastest way into the codes was using 'cribs' (pieces of PT associated with pieces of CT) and careless operator

coding, such as repeating the encrypted start-key twice; also, a machine weakness was that it did not allow same letter-to-letter encryption. However, the real breakthrough was Turing's vital contribution of constructing improved bombes (Fig. 6) to nullify the effect of the Enigma plug-board wiring thus reducing the code-breaking effort by a factor of something like 10^{14}. The new bombes exploited cribs, found scrambler wheel settings and revealed message start-keys. The military intelligence gained at BP in this way was code-named ULTRA. For the record, it is worth pointing out here that William Friedman, in the US, had already done significant work in breaking Vernam ciphers using a technique known as the *index of co-incidence*: sliding different sections of a CT message over one another, counting letter coincidences, and then using the natural language letter frequencies to reveal key-words.

Fig. 7. The Hagelin C36 cipher machine

Once the Germans started to use more wheels, and then later the Lorenz (Tunny), the performance of the bombes became limited and a new electronic code-cracking machine, the *Colossus* computer, was born. This was based on a design by Max Newman and engineered by Tommy Flowers of the UK Post Office research center. It had 1500 thermionic valves, which frequently burnt out, but was very much faster than the relay-switched bombes. The battle between code-makers and code-breakers then began in earnest. After the war, Churchill ordered all Colossus computers to be broken up and all design documents to be destroyed; even today, some of the code-breaking tricks are still classified as secret.

The Allies were also using rotor cipher machines. The Hagelin C36 (1936) was used by the French but rejected by the USA (Fig. 7). It was later replaced by the C38 and upgraded to the M209 (1941); BP could also break these codes. The Swiss made an Enigma-like NEMA machine (1942/1947) with up to 10 wheels, which was declassified in 1993. In 1952, the UK MI6 was using NOREEN C52, a one-time pad Vernam cipher with 6 pin-wheels, known as BIDS 590. The Russians developed 'Fialka', a super Enigma in 1950; this allowed same letter encryption, which increased the strength of the cipher. Finally, in the 1950's NSA produced ADONIS KL7, which was also a super Enigma with 5+ wheels; it was used by NATO and, for example, installed on UK Royal Navy ships.

IV. Shannon and Modern Cryptography

Claude Shannon is the father of information theory but it is not generally known that he developed the statistical ideas through his work on cryptology, hiding data, where he needed a good metric for information; this work was done in WWII at the Bell Laboratories. Shannon (Fig. 8) established a solid theoretical basis for both cryptography and cryptanalysis. These principles are still in use today.

Fig. 8. Claude Shannon

The idea that a strong cipher system depends on the secrecy of the key, and not solely on the complexity, or the secrecy, of the coding algorithm, had already been enunciated by the Dutch linguist Auguste Kerckhoffs, (*La Cryptographie militaire*), in 1883, and Shannon further developed this reasoning [10]. His main principles were:

- *Substitution (S box)* – message confusion; introducing complexity in order to hide the key.
- *Transposition (T box)* – diffusion by smearing the PT into the CT; this is scrambling or permutation.
- *Multistage* – super-encipherment with serial stages of S & T boxes; also known as a 'product cipher'.

One of Shannon's main contributions to the science of ciphers was to quantify cryptographic strength with a new metric called *unicity distance*. This measure depends on the entropy of the keyspace and also the redundancy of the language. He showed that CT longer than this distance is reasonably certain to have only one meaningful decrypt. Shorter CT's produce ambiguous outputs and are therefore implicitly secure; for the English language, this distance is of order 30-40 for a poly-alphabetic cipher. Importantly, Claude Shannon showed how to increase the workload of the cryptanalysis; he clearly demonstrated the difference between *perfect* codes and *ideal* codes which led to the provability of secure one-time pads.

The Shannon principles were used to develop the first encryption standard. After a competition in the US, the IBM system known as Lucifer, originally due to Feistel, and had a 128-bit key, was finally adopted. However, the

NSA got at this and deliberately halved the key-length to 56 bits (FIPS 46-3). The Data Encryption Standard (DES), was published in 1977; it was primarily for commercial businesses such as banks. It is a 64-bit block cipher. The 16-stage S & T encryption algorithm and the known weak keys were put into the public domain, and interest in cryptography soon took off; various parties were able to break DES by exhaustive key search. Triple DES was then recommended, but then later, NIST (was NSA) replaced the standard, under FIPS 197 in 2001, with the new Advanced Encryption Standard (AES) which had a *secret* coding algorithm and a *double* key-length of 128 bits; this very substantially increased the number of keys from the original DES figure, of order 10^{18}, to a virtually unbreakable number. Other improved standards also emerged, such as FEAL (NTT Japan), LOKI (Australia), and IDEA (Switzerland) [9]. Block ciphers are rarely used in electronic codebook mode, as they are then vulnerable to repeat jamming. Other modes available are 'cipher block chaining', 'cipher feedback' (or CT-auto key), and 'output feedback' (or key-auto key). Key escrow systems have also been proposed in which session keys are stored in two encrypted halves at trusted sites so that, if necessary, law enforcement agencies (LEAs) could decrypt traffic such as digital mobile phone calls; this was the so-called 'clipper chip' system.

V. Public Key Systems and Digital Signatures

In cryptographic systems, the authentication process is generally more severe than secrecy issues. If a recipient, say Bob, gets a message, encrypted or not, from a sender called Alice, he needs to know that it really has come from A and not from someone else who is masquerading as the bona fide sender. Standard systems, such as a message authentication character (MAC), or a one-way hash function, do not solve the 'problem of trust'. However, in 1976, Whitfield Diffie and Martin Hellman, introduced a safe way of exchanging keys with a new *asymmetric-key* cipher system [11].

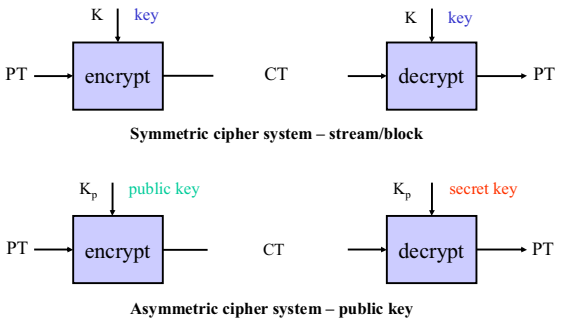

Fig. 9. Symmetric & asymmetric crypto-systems

Public key systems (PKS) are able to solve the problem of key distribution, which can be severe for a large network of users. In such a system, there is a secret key for the receiver and a related, but entirely different, publicly available key for the sender(s) (Fig. 9). It turned out later that PKS had been previously invented in the early 1970's by mathematicians Clifford Cocks, James Ellis and Malcolm Williamson at GCHQ, but for security reasons were not allowed to reveal this until 1997 [2]. In 1978, MIT academics Ronald Rivest, Adi Shamir and Len Adleman invented a PKS, known as RSA, which is based on discrete logarithms and the difficulty of factorizing products of large prime numbers. Euler's totient function, Euclid's algorithm and the Chinese remainder theorem were all there and pure mathematics had quite obviously come of age! The RSA algorithm [12] is the current pre-eminent PKS scheme, and which inter alia, protects our electronic transactions on the Internet.

Inverting the PKS channel with the secret key (S) at the sender's end and the public key (P) at the receiver solves the digital signature problem. Fig 10 shows how Alice authenticates herself to Bob; obviously the encryption and authentication channels can operate together if required.

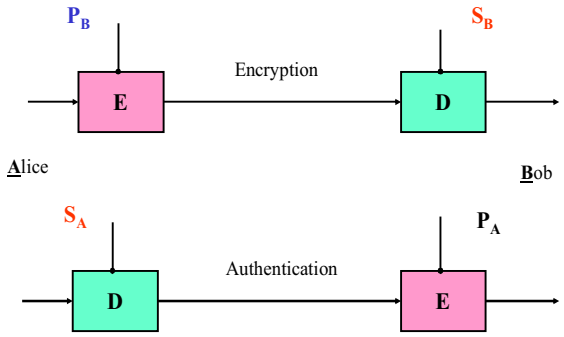

Fig. 10. The PKS used for secrecy and digital signatures

Normally the input to the authentication channel is a one-way hashed version of the PT message but it can be an initial shared secret, such as the maiden name of Alice's mother. Typical threats to combat are: alteration, deletion and addition of data; changing the apparent origin and actual destination; altering the block sequence, repeating previous data and falsifying acknowledgements. Although PKS is computationally intensive, it scales well compared with the conventional symmetric encryption schemes. As in all systems, key management is a significant problem and trusted key distribution centers must be employed with working certificates issued to trusted clients.

In 1991, Phil Zimmermann released the Pretty Good Privacy (PGP) encryption scheme on the Internet; it caused quite a political stir as the authorities did not want 'Jo Public' to use very strong ciphers which were difficult for them to break. The original idea was to speed up the RSA process. What came out was a DES system with the key sent by RSA, and a signature formed from a zipped up compressed message digest, using a standard hash function (MD 5) [9].

VI. Quantum Cryptography

A one-time pad system is unconditionally secure, in the Shannon sense, if the key is strictly random and only used once; it has limited use however because a new key would have to be distributed for each new PT message – a great logistical burden. Luckily, the laws of quantum physics have provided us with an excellent solution. Quantum key distribution (QKD), uses quantum mechanics to guarantee secure communication enabling two parties to share a random bit string known only to them, which can be used as a key to encrypt PT and decrypt CT messages [13]. Because the process of measuring a quantum parameter

generally disturbs the system, QKD allows users to detect the presence of an eavesdropping third party (bad guy Eve). Using 'quantum uncertainty', with Alice sending information to Bob as quantum states, Eve cannot quietly tap into the transmission. The chosen key(s) can be used with any chosen cipher system over an insecure channel. The popular QKD system works with polarized photon particles [14]; there are 4 polarizations involved.

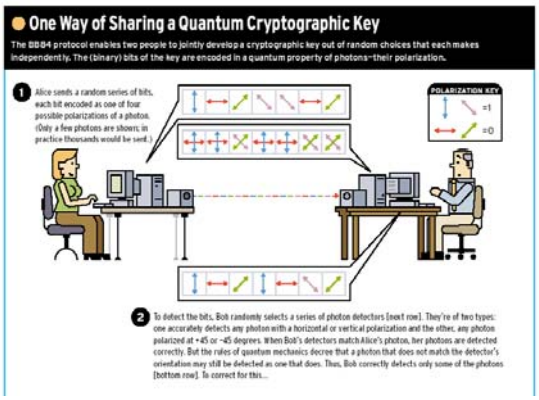

Fig. 11. Principle of QKD (from IEEE Spectrum)

In summary, QKD works as follows (Fig. 11):

- A sends a random series of bits, each one encoded as one of 4 possible polarizations.
- B randomly selects a series of photon detectors and when they match A's photons, her photons are detected correctly but only some are correct.
- B tells A the detectors he used and A tells B which ones correctly detected her photons.
- A and B keep only the correct bits and use them as their cryptographic key.

If E intercepts photons from A, and sends them on to B, she winds up with many code errors because her series of detectors is different from B's. Even worse for E is that her meddling has also introduced errors into A and B's shared key-stream, but they are able to jointly detect this.

The above BB84 quantum protocol is named after its inventors and the year of publication (Bennett & Brassard 1984). The maximum distance that BB84 QKD has been successfully transmitted is of order 120 km.

Finally, it is worth noting that if quantum computers finally become practicable technology, then everything is turned on its head as even the strongest codes, including one-time pads, will not be able to resist quantum computational cryptanalysis.

VII. Final Remarks

In the current era of electronic financial transfer and also various network-enabled systems, the science and application of cryptography has become increasingly important; the Internet is but one example. The paper has only been able to skim the area and its history, and there has not been the scope to include discussion of crypto-attack methods and the art of cryptanalysis; these subjects are very sensitive anyway, and could easily lead to classified material. Finally it is important to point out that the basic principles of cryptography have stood the test of time, from Greek secret writing to the electronic age.

References

[1] D. Kahn, "*The Codebreakers – The Story of Secret Writing*", Macmillan, New York, 1967 (reprinted 1996).

[2] S. Singh, "*The Code Book*", Fourth Estate Ltd., Chapt 2, 1999.

[3] F. L. Bauer, "*Decrypted Secrets – methods and maxims of cryptography*", Springer Verlag, 1997.

[4] J. Garliński, "*Intercept – the Enigma War*", Magnum Books, Menthuen Paperbacks Ltd., 1981.

[5] J. Copeland et al., "*Colossus – the Secrets of Bletchley Park's Codebreaking Computers*", Oxford University Press, 2006.

[6] "*Codebreakers – the Inside Story of Bletchley Park*", F. H. Hinsley and A. Stripp, Ed., Oxford University Press, 1993.

[7] H. Becker and F. Piper, "*Cipher Systems: the Protection of Communications*", Northwood Books, London, 1982.

[8] D. W. Davies and W. L. Price, "*Security for Computer Networks – an Introduction to Data Security in Teleprocessing and Electronic Funds Transfer*", John Wiley & Sons Ltd., *2nd Ed.,* 1989, Chap 2.

[9] B. Schneier, "*Applied Cryptography*", *2nd Ed.,* John Wiley & Sons Inc., 1996.

[10] C. E. Shannon, "Communication theory of secrecy systems", *BSTJ,* vol. 28, 656, October 1949.

[11] W. Diffie and M. E. Hellman, "New directions in cryptography",*Trans. IEEE on Information Theory,* IT-22, no.6, pp 644-654, November 1976.

[12] R.L. Rivest, A. Shamir and L. Adleman, "A method of obtaining digital signatures, and public key cryptosystems", *Comm. ACM,* vol. 21, no. 2, pp 120-126, February 1978.

[13] C. H. Bennett et al., "Quantum Cryptography", *Scientific American,* pp 50-57, October 1992.

[14] A. V. Sergienko, Ed., "*Quantum Communications and Cryptography*", CRC Press (Taylor & Francis), 2006.