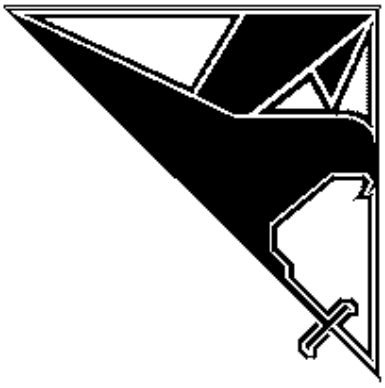
Next Generation Security Software



Quantum Cryptography

A study into the present technologies and future applications

Bill Grindlay
bill@ngssoftware.com
14th January 2003

www.ngssoftware.com

"*Anyone who is not dizzy after his first acquaintance with the quantum of action has not understood a word*."

- Niels Bohr (1885-1962)

"*When cryptography is outlawed, bayl bhgynjf jvyy unir cevinpl*."

- Anonymous

Contents

Introduction

In October 1989 at 3 o'clock in the morning at IBM's Thomas J. Watson Research Centre near New York, Dr. Charles Bennett and a research student named John Smolin witnessed the first ever quantum cryptographic exchange. Using polarised light photons, computers called Alice and Bob successfully negotiated a completely secure channel of communication over a distance of 32 centimetres. Quantum cryptography had now finally moved from the theoretical to the practical arena.

In this report I intend to demonstrate why many scientists now view quantum cryptography as the first ever completely unbreakable cipher, which will allow people all over the world to communicate securely and privately.
I shall also consider the implications which this will have on society as a whole, including potential problems for law enforcement organisations and the possible impact on civil liberties.

A Brief History of Cryptography

Cryptography (derived from the Greek words *kryptos* and *graphein* meaning *hidden writing*) is the science of codes and ciphers. A cipher is essentially a cryptographic algorithm which is used to convert a message, known as the plaintext, into unreadable ciphertext. The message can then be safely transmitted without fear of letting sensitive information fall into the hands of the enemy.

The first written evidence of cryptography dates back as far as 1900 BC, when an Egyptian scribe recorded information using a variation of standard hieroglyphics. The author made use of what is now known as a substitution cipher, meaning that certain hieroglyphs were substituted for others according to a set of rules. A modern equivalent of this would be if every letter in the plaintext represented another in the ciphertext, for instance swap every occurrence of the letter A in a message for B, and every B for C and so on.

Archaeologists discovered evidence of the first practical application of cryptography dating from 1500 BC in Mesopotamia (now part of modern day Iraq). A potter had encoded his formula for pottery glaze onto a clay tablet, presumably to prevent rivals from stealing it. This is an early example of what is now one of the main non-military uses for data encryption, protection of intellectual property.

The first military application of cryptography came in the fifth century BC and was invented by the Spartans of Greece. Their system involved wrapping a strip of leather around a staff (known as a *skytale*), writing the message lengthways along the staff and then removing the leather. The markings on the leather were then unintelligible to anyone without a matching staff. In a sense the *skytale* could be said to be the first cryptographic key, as the only people who could read the message were those who possessed a staff of exactly the same diameter as the one used to encipher the message.

Then, as now, the primary motivating factor behind cryptography development and research has been to keep military communications from the enemy. Julius Caesar used an early substitution cipher, which now bears his name, for communication with his generals. The Caesar cipher used a shift of three places along in the alphabet to convert a plaintext letter to a ciphertext one, so A enciphered to D, B to E and so on.

A political treatise known as The Arthashastra written around 300 BC and attributed to Kautilya, an Indian court advisor, made the first mention of cryptanalysis techniques. Cryptanalysis, the art of code-breaking, has developed as a science parallel to cryptography. Advances in code-making have thrown the onus onto the code-breakers, and their exposures of vulnerabilities have, in turn, challenged the cryptographers to produce even better ciphers.

During the Dark Ages and Mediaeval periods, many Arab and European scholars wrote books categorising the various types of cipher which had evolved by that point. An Arabic encyclopaedia from 1412 defined two types of cipher known as substitution (where every letter in the plaintext is substituted for another one in the ciphertext) and transposition (where the position of letters in the plaintext are changed or new letters added in order to produce the ciphertext). Italian scientist Giovanni Porta published a book in 1563 which detailed both of these ciphers, plus another called symbol-substitution (use of a strange alphabet).

The simple substitution cipher was now no longer as secure as it once had been due to a widely-used cryptanalysis technique known as frequency analysis. Code-breakers, when given a large enough piece of ciphertext, would detail the frequency with which each letter occurred. Using this information, and bearing in mind the frequency with which letters normally occur in standard written English (E is most common, followed by T, then A etc.) it is possible for the cryptanalyst to make tentative guesses as to which letters in the ciphertext equate to which in the plaintext. It is quickly apparent whether these guesses are accurate and using knowledge of other linguistic characteristics of English (U always comes after Q for example) the substitution cipher can be relatively easily unravelled.

The response to the insecurity of the substitution cipher came in 1466 with the first published example of a polyalphabetic cipher by Italian renaissance artist and scientist Leon Batista Alberti. The problem with the old monoalphabetic substitution cipher was that one letter in the plaintext was represented by one letter in the ciphertext, and it was the same mapping every time. The essence of this new type of cipher was the use of several different letter-to-letter mappings (cipher alphabets) depending on the position in the plaintext, ensuring that a certain letter in the plaintext did not always encrypt to the same letter in the ciphertext. The most famous polyalphabetic cipher is known as the Vigenère cipher, after Blaise de Vigenère a French diplomat and cryptographer who developed it into its final form. The Vigenère cipher requires a keyword which is written above the plaintext message repeatedly as shown:

S	E	C	R	E	T	S	E	C	R	E	T	S	E	C	R	E	T	S	E	C	R	E	T
T	H	E	R	E	D	C	O	W	F	L	I	E	S	A	T	M	I	D	N	I	G	H	T

Letters are enciphered as with other substitution ciphers, but the strength of the Vigenère cipher is that, unlike the Caesar cipher where the offset is always 3 letters, the enciphering offset changes depending on which letter of the keyword is above the plaintext letter. This gives the cipher 26 possible enciphering alphabets, and in order to find which one should be used for which letter a Vigenère square is used (see Appendix I). The ciphertext letter is found by looking at the intersection between the plaintext letter selected at the top, and the keyword letter selected along the left-hand side. Every time the keyword letter changes, a different horizontal row of the square is used, and therefore a different cipher alphabet is applied:

S	E	C	R	E	T	S	E	C	R	E	T	S	E	C	R	E	T	S	E	C	R	E	T
T	H	E	R	E	D	C	O	W	F	L	I	E	S	A	T	M	I	D	N	I	G	H	T
L	**L**	**G**	**I**	**I**	**W**	**U**	**S**	**Y**	**W**	**P**	**B**	**W**	**W**	**C**	**K**	**Q**	**B**	**V**	**R**	**K**	**X**	**L**	**M**

The resultant ciphertext does not bear a direct one-to-one mapping with the plaintext. For example the three T's in the plaintext are encoded first as L, then as K and finally as M. This makes the ciphertext impervious to standard frequency analysis.

The Vigenère method became known as *le chiffre indéchiffrable* (the indecipherable cipher), but of course it was not unbreakable for long. Charles Babbage, an English inventor and scientist is best known for designing the difference engine, a mechanical calculation device which was the precursor to the modern digital computer. He was also interested in codes and ciphers and was the first to realise that the Vigenère cipher was essentially a series of monoalphabetic ciphers. Babbage's technique involved looking for repetitions of character strings in the ciphertext and assuming that these are the same plaintext letters being enciphered with the same keyword letters. It is now possible to guess the length of the keyword (n) and thus split the ciphertext into n number of groups. Standard frequency analysis can now be applied to each group of ciphertext letters to obtain all n mono-alphabetic cipher alphabets.

Code-making and breaking really came into their own during the First and Second World Wars. The development of radio communications by Guglielmo Marconi at the turn of the 19th century generated a huge amount of interest within the military. However the very fact which made it so appealing, immediate communications over great distances, also meant that the enemy could easily intercept vast quantities of information. There was clearly a great need for secure encryption, something which had not yet been achieved since the successful breaking of the Vigenère cipher.

It seemed that for the first time in history the cryptanalysts had comprehensively gained the upper hand. This was made all the more apparent by the 1917 decipherment by British intelligence of what became known as the Zimmerman telegram (see Appendix II), which effectively brought America into the First World War. The telegram was sent by German Foreign Minister Arthur Zimmerman to the German embassy in Mexico, and promised US territory to Mexico if they allied with Germany. When the contents of this were made public, American popular opinion, previously fairly neutral, became decidedly pro-war and the US declared war against Germany within a month. This event is still held by many experts to be the single most historic decipherment ever made.

In the same year as the Zimmerman telegram made code-breaking history, Gilbert Vernam, an employee of AT&T in America, built a machine to generate pseudo-random strings of characters for use as encryption keys in a cipher called a one-time pad (also referred to as the Vernam cipher). Before the advent of quantum cryptography the one-time pad was widely regarded as the only cryptosystem which guaranteed absolute security – often termed the 'holy grail' of cryptography. The one-time pad uses a random key of the same length as the plaintext, if the message is intercepted the cryptanalyst has absolutely nothing to give them a foothold. The pseudo-random encryption key means that there is no point looking for repeating patterns, so essentially the only information an attacker has is that if the ciphertext is n letters long, the plaintext must be one of all the possible messages of length n.

One-time pads are currently only used when security is of the utmost importance, for example to encode the telephone line between Downing Street and the White House; this is due to the problem of key distribution. For a one-time pad cryptosystem to work effectively both the receiver and the sender need identical sets of strings of random characters to use as encryption keys. New keys must be physically exchanged on a regular basis to avoid key reuse, a very time consuming operation if the correspondents are geographically distant.

Key distribution was a catch-22 situation for all ciphers regardless of security; if two people wanted to communicate secretly they had to share a secret key, which itself could not be exchanged unless they could communicate secretly. After the Second World War with the introduction of increasingly complex ciphers thanks to the digital computer, key distribution began to be seen as the weakest link in the chain. In the 1970s the American agency COMSEC managed encryption keys for the US government and transported tonnes of paper, cards and floppy disks under armed guard. If the US government was spending this amount of resources and money on ensuring secrecy, many people reasoned, what chance did civilians ever have of privacy?

The cryptography breakthrough[1] was made in 1975 by Whitfield Diffie, a research cryptographer and mathematician, who envisaged what is now known as public key cryptography. He developed an algorithm with a colleague, Martin Hellman, which allowed two people, who may have never met, to negotiate a secret key over a public communications channel. This was not a complete solution however as it still required that both parties had to be online at the same time. There was also no way that both parties could be sure they were actually talking to each other, and not to an impostor.

In 1977, encouraged by Diffie's efforts, three researchers from the Massachusetts Institute of Technology published their paper on the world's first asymmetric cipher named RSA (after the authors Rivest, Shamir and Adleman). The essence of asymmetry is that different keys are used to encrypt and decrypt the message. A pair of keys, known as public and secret keys, is generated by every user of the system. The public key is made available to everyone and the secret key is kept secret. A message to a user is encrypted with the recipient's public key by the sender, and then decrypted by the recipient with their secret key.

The effect of the RSA algorithm was to revolutionise cryptography. For the first time ever two people could communicate securely across public networks without the prior need to establish a shared secret key. Messages encrypted using RSA are not unbreakable, but the conventional computing power required to derive the secret key from the public key is so vast as to make it totally unfeasible. Claims that the US National Security Agency (NSA), owner of the most processing power in the world, can break popular encryption algorithms such as DES (Digital Encryption Standard) are, as yet, unproven. As William Crowell, Deputy Director of the NSA, succinctly put it:

> "*If all the personal computers in the world − approximately 260 million computers − were to be put to work on a single [public-key] encrypted message, it would take on average an estimated 12 million times the age of the universe to break a single message*".

The future possibility of quantum computers, with the ability to break RSA within minutes, would certainly cast doubt on the security of the cipher. Cryptographic research has recently turned to harnessing quantum physics instead to provide a cipher which provides a secure means of key exchange plus the absolute security of the one-time pad, immune to the code-breaking attempts of a quantum computer. Is quantum cryptography the final unbreakable cipher in the history of code-making?

[1] It is now widely accepted that a complete system of public-key cryptography was in fact first developed in 1975 by James Ellis, Clifford Cocks and Malcolm Williamson, a team working at the UK's Government Communications Headquarters (GCHQ) but owing to military secrecy issues they were not allowed to publicise their work at the time.

The Development of Quantum Theory

A quantum theory of matter began to be developed around the beginning of the 20th century, in response to a series of unexpected experimental results which did not conform to the previously accepted Newtonian model of the universe. The essence of quantum theory is the realisation that elementary particles (electrons, protons, neutrons etc.) also have the ability to behave as waves. A test which neatly demonstrates this peculiar behaviour, known as *wave/particle duality*, in light photons is the twin slit interference experiment. If light is directed at two slits in a screen the waves will radiate outwards as shown below in Fig.1:

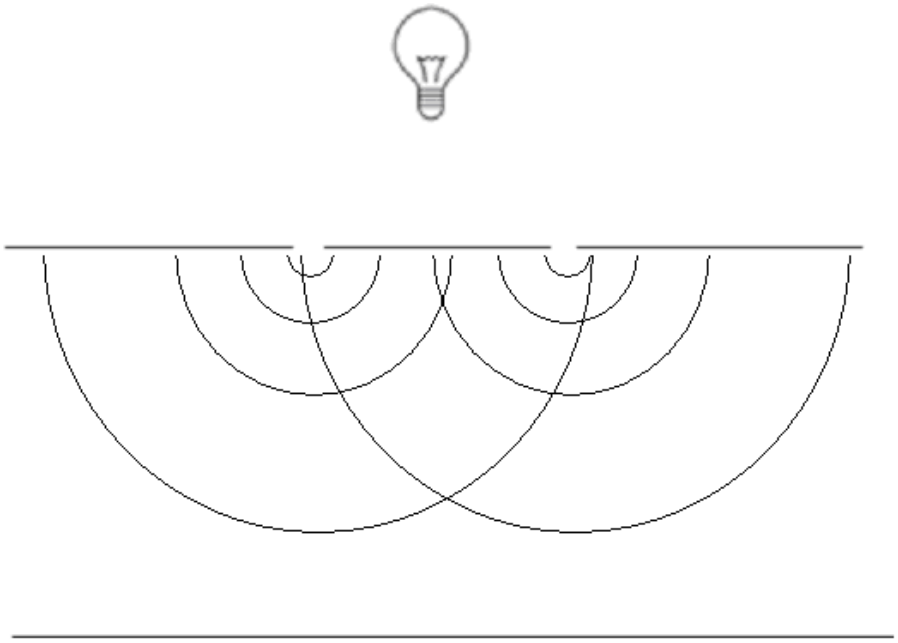


Fig.1: Light waves in the twin slit interference experiment

The light waves will interfere with each other in a very similar way to ripples in water. Where two peaks meet, an even greater peak (more light) is created, and where two troughs meet, an even lower trough (less light) is formed. When the light hits the back screen an 'interference pattern' is created:

Fig.2: Pattern formed on screen showing differing intensities caused by light wave interference

So far this conforms to the accepted Newtonian universe model; but it was found that if the light was instead used to repeatedly emit just a single photon (a quantum of light) over a period of time, exactly the same interference pattern was formed on the screen. This was a startling result, and completely challenged conventional physics. When it is emitted the photon either goes through one slit, or the other. In order to produce an interference pattern the photon must have somehow affected itself.

Two schools of thought have developed to explain the results of the twin slit interference experiment, both holding opinions which seem to defy common sense. The first theory suggests that, as the exact behaviour of each photon is unknown, it is reasonable to believe that the photon can perform all possibilities simultaneously, passing through both slits. Each possibility is called a state, and as long as the photons are not observed, the experiment is said to be in a *superposition of states*. The second camp instead posits the idea that at the moment when the photon has the choice between slits the universe divides into two and in one universe the photon passes through the left slit and in the other it passes through the right one. This plurality of universes is known as the *multiverse*.

Even though it is not yet fully understood exactly how the results of the experiment occur, they cannot be disputed. Quantum theory has now found applications in many areas of electronics, such as computer processors and lower power consumption lasers in compact disc players.

A particularly exciting application of quantum mechanics which is still currently in the theoretical stage is that of quantum computing. Conventional computers use binary digits (bits) set to either one or zero to perform calculations. Quantum computers, it has been proposed, could use electrons spinning either clockwise or anti-clockwise to represent ones and zeroes (qubits). If these are in a superposition of states, and not observed, all the possible states will be evaluated simultaneously and the correct answer to the calculation obtained in a fraction of the time it would have taken a standard computer. This promised leap in processing power is a real threat to the security of all currently existing ciphers. The current effectiveness of RSA could be eliminated at a stroke, so clearly there is a pressing need to pre-emptively develop a more resilient cipher.

The Advent of Quantum Cryptography

Shortly before British physicist David Deutsch published the first paper[2] proposing quantum computers in 1985, cryptologists had united quantum theory with code-making. In the early 1980s two computer scientists, Charles Bennett a researcher for IBM, and Gilles Brassard from the University of Montreal, realised that the application of quantum theory in the field of cryptography could have the potential to create a cipher giving absolute security for eternity. Initial work was hampered by the ubiquitous problem of key distribution; if a conventional key-exchange system was used, such as RSA, any security would be quickly lost to a brute-force attack using a quantum computer.

The cryptosystem developed by Bennett and Brassard uses polarised light photons to transfer data between two points. As a photon travels through space it vibrates perpendicularly to its plane of movement, the direction of vibration is known as its polarisation. For the sake of simplicity I have restricted the depicted directions of vibration to horizontal and vertical, although in actuality the photons will also move in all angles in between those shown:

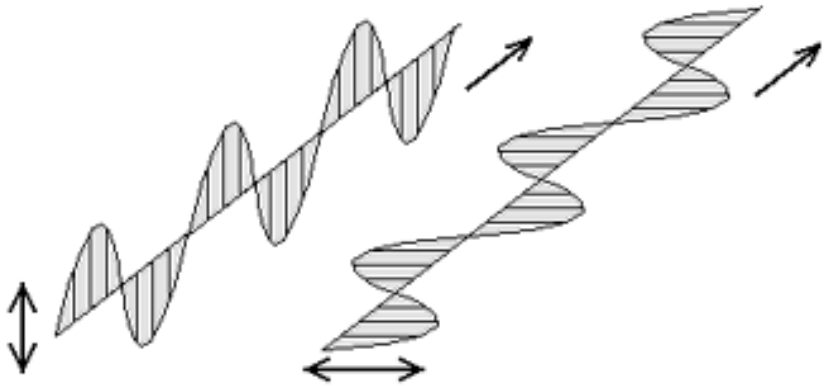


Fig.3: Diagram showing vertically and horizontally polarised light

Polarising filters can be created from plastic polymers which will only allow light of a certain polarisation through. These filters, or Polaroids, will block photons of a diametrically opposite polarisation, but will allow those with the same polarisation through. If a light photon has up to a 45˚ difference in polarisation then the photon faces a quantum decision, and approximately half of the photons will make it through and half will be blocked.

[2] This influential paper is available online at the Centre for Quantum Computation: http://www.qubit.org/oldsite/resource/deutsch85.pdf

Bennett and Brassard's proposed scheme takes advantage of the fact that an observer will have no idea which angle of polarising filter should be used for a certain photon to pass successfully through. Supposing that the binary ones and zeroes of digital communication are represented respectively by, in one scheme vertically (↕) and horizontally (↔) (rectilinearly) polarised photons, and in the other left-diagonally (↖↘) and right-diagonally (↗↙) polarised photons. The sender of the message will randomly swap between the rectilinear (+) and diagonal (×) schemes, known in quantum cryptography as bases, during transmission. An eavesdropper attempting to intercept the photons will have no idea whether to use a rectilinear or diagonal filter. Around half of the time a totally inaccurate measurement will be made when a photon will change its polarisation in order to pass through an incorrect filter. The cryptosystem neatly takes advantage of one of the fundamental features of quantum theory, a manifestation of Heisenberg's uncertainty principle[3], that the act of observing will change the system itself. In this way it is impossible for an attacker to make an accurate measurement of the data without knowledge of which scheme is being used, essentially the cryptographic key.

Unfortunately, when this method was first developed, the intended recipient of the message had no more idea as to the schemes being used than an attacker did, due to the long-standing problem of secure key exchange. Obviously traditional key exchange protocols such as RSA and Diffie-Hellman were out of the question as they are ultimately breakable, and would negate the absolute security offered by a quantum cryptosystem. Bennett and Brassard made the breakthrough in 1984, and in the process created an entirely self-sufficient unbreakable cipher.

Assuming that two people named (using the popular cryptographic notation) Alice and Bob wish to communicate securely. Their method for key-exchange starts with Alice transmitting a stream of random bits as polarised photons and continually swapping randomly between the rectilinear and diagonal encoding schemes. Bob at this point has no idea which schemes are being used for which bit, and so he will also swap randomly between schemes. Alice will now contact Bob insecurely and tell him which scheme was used for each photon, Bob can say which ones were guessed correctly and all the incorrect guesses are discarded. Both parties now share a secret key, with no useful information leakage to an eavesdropper. In fact it will become immediately apparent to both if someone is monitoring the photons in transit, because their use of an incorrect filter is likely to change the polarity of photons before they reach Bob. If, when comparing a small part of their shared secret key over a public channel they do not match, it will be clear to both Alice and Bob that the photons have been observed in transit.

[3] Werner Heisenberg, a German physicist, demonstrated that it is impossible to measure accurately both the momentum and location of an electron. The act of measurement itself is enough to alter readings of the other property.

The publication of Bennett and Brassard's cryptosystem caused a great deal of excitement in the scientific community, but it was not until 1989 that the first physical demonstration system (Fig.4) was built by Bennett and Smolin at IBM's T. J. Watson Research Laboratories in New York State. Since then the challenge has been to produce functional systems over greater distances, hindered by the fact that specifically polarised photons do not travel well through air as the molecules can alter their polarity.

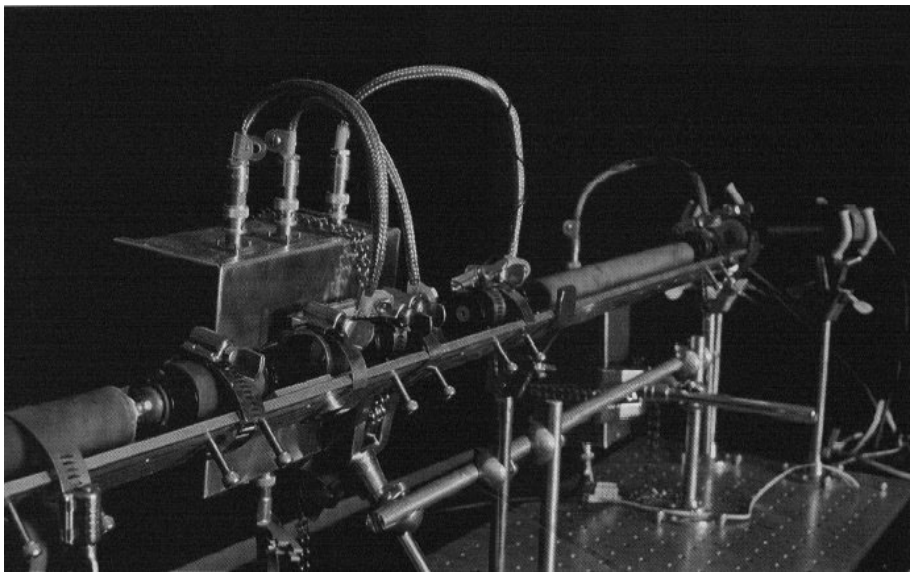


Fig.4: Quantum cryptographic apparatus constructed at IBM. Flashes of polarised light, each one tenth of a photon, are generated and measured across a free air optical path of 32 centimetres.

Recent quantum cryptosystems have concentrated on using optical fibres to transmit the photons. In March of this year a Swiss team of researchers successfully conducted a quantum key exchange over the telephone network between Geneva and Lausanne[4], a distance of 67 kilometres. In August last year in the US, a team based in Los Alamos, New Mexico, managed to transmit using two portable units across six miles of desert[5].

The work at Los Alamos is geared towards eventually sending quantum-encrypted information from the ground to satellites, which would remove all limits to the distances over which communications could be secured.

[4] Quantum Key Distribution Over 67km with a Plug and Play System, *The New Journal of Physics* – Vol.4/41, July 2002

[5] Los Alamos Develops Quantum Crypto System, *The EETimes* – August 23rd 2001

Is Quantum Cryptography Secure?

It may seem that this question has been answered quite comprehensively in the preceding chapter. A message encrypted using quantum cryptography is secured by the laws of quantum physics, so if it was provably insecure the most successful theory in the history of physics would be disproved and our current understanding of the universe shattered. However, there are issues of data security relevant to a cipher beyond its confidentiality.

It is acknowledged in the 1991 paper "Experimental Quantum Cryptography"[6] contributed to by Bennett and Brassard, that there are issues of authentication not fully resolved by the current system. It is stated that "*the assumption that the public messages cannot be corrupted by [an eavesdropper] is necessary*" to avoid what is known as the man-in-the-middle attack. As both Alice and Bob have no way within the proposed system of proving their identity to each other, it is possible for an attacker to sit between them and impersonate Bob to Alice, and Alice to Bob thus negotiating a secret key with each of them. The suggested solutions are an "*unjammable public channel*" or a standard authentication scheme which would require that both Alice and Bob shared some secret information beforehand. The latter approach would seem to negate the main advantage of Bennett and Brassard's key exchange protocol, which is the ability for two entities to negotiate shared secret knowledge in a public channel without the need for any prior secrets. This, as it currently stands, suffers from the same drawback as the one-time pad which provides absolute secrecy but with the additional headache of securely distributing the keys. It would be possible to extend Bennett and Brassard's protocol to include an adaptation of the current certification authority authentication mechanism for conventional public keys. The current system uses trusted agencies to digitally sign public keys and so verify the identity of their owner. This however, whilst removing the need for shared secret knowledge, relies on computationally infeasible, but breakable, mathematical equations and, as such, would not offer an absolutely secure means of identification.

Another element of a quantum cipher's security is that of availability, which has not previously been an issue with conventional encryption. The root of the problem is an eavesdropper's ability to alter photons in transit and so prevent two entities from achieving an error free channel. This could be seen as a denial of service (DoS) vulnerability, and a malicious user is not limited to this line of attack. Even if Alice and Bob are sharing secret authentication keys, an attacker could repeatedly corrupt the public authentication exchange leading to both parties exhausting their supplies of keys before a secure connection is established. However the majority of DoS attacks, whilst annoying, are not considered security critical, and there is certainly no way for an attacker to trick Alice and Bob into believing that a secure connection exists.

[6] Experimental Quantum Cryptography – C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, *Journal of Cryptology*, vol. 5, no. 1, 1992, pp. 3 – 28

There are physical attacks which may be mounted on the transmission medium itself. Assuming that an eavesdropper has access to unlimited technology, two major techniques which have been identified are intercept/resend and beam-splitting.

Intercept/resend takes advantage of the fact that current photon detecting equipment is far from perfect; only around 1 in 400 pulses (one tenth of a photon) are successfully transmitted and received. As Alice and Bob know to expect this level of photon loss, an attacker can intercept selected pulses of light before they reach Bob, measure them, and then resend them on with the detected polarity. However, due to the difficulties in quantum measurement of photons, the probability of the resent and measured photons still having the correct polarisation when measured by Bob is only 0.25 or one in four[6]. The discrepancies will therefore be apparent to both Alice and Bob. Additionally Bennett's calculations as to any advantage gained by the eavesdropper puts the probability that they have correctly guessed a particular bit as $1/\sqrt{2}$ or approximately 0.7 (1 DP). For a cipher to be absolutely secure, it is unacceptable that even partial disclosure of the key occurs, so therefore whilst the optical technology is imperfect, any errors in transmission must be treated as an eavesdropping attempt and the entire exchange repeated.

Beam-splitting utilises the fact that the pulses of light which Alice and Bob use to communicate, in practice, are not single photon-states. The attacker uses a mirror to deflect part of the original light beam allowing it to continue, albeit with reduced intensity, towards Bob. The deflected pulses will be stored until Alice and Bob publicly announce the bases used to encode each bit, at which point the stored beam can be correctly measured. At the current time the technology does not exist, and it is not known if it is possible, to store polarised light pulses. However a present-day attacker is still able to make guesses as to the correct measurements of their diverted beam, as in the intercept/resend attack, with the added bonus of avoiding error creation in the data stream. The drop in beam intensity is likely to alert Alice and Bob to an intruder, and a sufficient delay before the bases are publicly discussed will also allow time for any stored photons to decay.

After a quantum key exchange has completed, according to Bennett and Brassard "*Alice and Bob are now in the possession of a string that is almost certainly shared, but only partly secret*". This is due to their assumption that the exchange will be eavesdropped, and that it will be done to the best of an attacker's ability. Instead of repetition of the whole process, Alice and Bob can make an estimation as to the amount of their secret key which can have been divulged (or lucky guessed), and then perform a process known as "privacy amplification". This involves publicly selecting a hashing function from a shared secret set, and then applying it to their shared secret key. The result will be a different secret key which they both share, and of which an attacker knows nothing.

The protocol developed by Bennett & Brassard et al is the first quantum cryptographic protocol ever produced. Quantum cryptography itself is still very much in its infancy, and has not yet made it out of the laboratory and become widely and publicly used. It is not surprising therefore, that while the physics behind the idea are unshakable, there are issues which may impede its rapid take-up and acceptance. The very feature of quantum physics which gives quantum cryptography its security as a confidential cipher also reduces its security as a reliable cryptosystem. The act of observation of a quantum key exchange will irreversibly alter it, destroy data and possibly necessitate the repetition of the exchange. In practice in a public channel, this could easily be classified a denial of service attack, and at the very least will waste time and cause frustration.

As the protocol stands, the issue of authentication is not fully resolved. A small amount of shared data is required between communicants before the exchange even begins, if this is necessary *before* a secure channel is established then it is an echo of the key-distribution problems faced by Diffie and Hellman, and GCHQ in the Sixties. The protocol however does allow for a key to be exchanged between two parties who may never have met, although there is no way for them to be assured that they are actually negotiating with each other.

The telephone networks in the countries which would lead the implementation of quantum cryptosystems are heavily reliant on optical fibres. These use pulses of light to transfer telephone conversations in digital form. The existing infrastructure of optical fibres would be an ideal medium for the transfer of quantum encrypted data. An added advantage is the perceived security of the telephone system in comparison to a local network or the Internet on which anyone with a grounding in security can sniff traffic. The practice of placing telephone taps has so far largely been restricted to law enforcement and requires more engineering and electrical knowledge than most malicious attackers will possess. There is physical security at local exchanges giving another barrier to eavesdropping. Essentially this adds up to an existing, secure infrastructure for the rollout of quantum cryptography. Indeed, as previously mentioned, a Swiss team has already used the Swiss network for a successful quantum exchange.

The Swiss team used a technique known as quantum entanglement to transmit their exchange. This involves using a crystal to split a polarised photon into a pair of photons, each in a superposition of polarised states. When the polarity of one member of an entangled pair is measured, the other member immediately assumes its companion's polarity, a quantum effect which Einstein disparagingly termed "*spooky action at a distance*". This method was first proposed by Oxford physicist Artur Ekert, and involves sending pairs of entangled photons to both Alice and Bob simultaneously. Entanglement makes statistical analysis of the transmitted data useless, as neither member of the pair has polarisation until it is measured. This ensures absolute randomness of keys generated by the quantum exchange.

Absolute Security and the Wider Social Issues

The communications security offered by quantum encryption cannot be disputed. If two people have established a secret key and are passing polarised photons between two points, the laws of quantum physics dictate that it is impossible for the information exchanged to be compromised. The ability of private citizens to achieve this, which has never before been possible, is likely to be of particular interest to national government and law enforcement agencies. Since computer encryption has been available to the public it has been legislated and the export of algorithms from country to country tightly controlled.

When Rivest, Shamir and Adleman first developed the RSA algorithm in 1977 the American National Security Agency (NSA) put great pressure on both the researchers and their employer, the Massachusetts Institute of Technology (MIT), to prevent publication[7]. They published regardless, and in their hurry lost patent rights to the algorithm outside the US where most countries require registration before publication.

In the past America has maintained strict controls on the export to other countries of cryptographic algorithms or software, in effect treating them as munitions comparable to missiles or machine guns. In January 2000, in a historic move, the government relaxed controls on all cryptographic software exported by US companies. Following this, in March 2001, the government allowed strong encryption (128 bit keys) for export, from a previous maximum of 40 bits. There is still some distance to go, and there is still great pressure in the senate for further relaxation of controls.

In 1991 Phil Zimmerman released a software package called PGP (Pretty Good Privacy) which uses RSA encryption within a simple user interface. The software was directed at the home user, and was intended to give everyone secure Internet communications. The effects of Zimmerman's altruistic efforts were to make him the target of an FBI enquiry and a grand jury investigation. Zimmerman released his software for free on the Internet and, as it contained cryptographic code, had effectively become an international arms dealer. The US government eventually dropped its investigation in 1996.

In 1991 the US government attempted to pass Senate Bill 266, which stipulated that all encryption software must have a back-door built into it to allow officials to read private messages. It read in part:

> *"It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall insure that communications systems permit the Government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law"* [8].

---

[7] Crypto: How the Code Rebels Beat the Government - Saving Privacy in the Digital Age – Steven Levy, ePenguin, B00005UOTX (e-Book)

[8] Comprehensive Counter-Terrorism Act of 1991 (Senate Bill 266)

The bill was defeated after strong protests from civil liberties groups. This is a parallel to the UK government's Regulation of Investigatory Powers Bill which was enacted into law[9] in July 2000. This now allows for "*lawful interception*" of all communications data, meaning that anyone using cryptography must give up a copy of their key if a warrant is obtained. Failure to do so is punishable by up to two years in prison.

A practical and widely-used quantum cryptosystem would pose serious problems for the NSA and render much of the previous cryptography legislation redundant at a stroke. Obtaining a crypto-key with a warrant is of very little use if you don't have a copy of the original encrypted message, as current technology does not allow storage of light photons for long.

There is clearly a public safety issue here, as presumably the NSA and GCHQ do not want access to encrypted emails simply to keep tabs on political opponents. Currently public-key encryption is widely used by organised crime and terrorist networks. Computers owned by al-Qaeda operatives in Afghanistan contained files encrypted using 40-bit DES. Before March 2001, this was the strongest encryption which could be shipped internationally from the US; journalists broke it using a brute-force attack within five days[10]. Crypto-software using 128 bit keys can now be exported internationally; this gives exponentially more security and, using the journalist's setup, would be absolutely unfeasible to crack.

In 1995 the Aum Shinrikyo cult released sarin nerve gas on the Tokyo subway, killing 12 people and injuring thousands. When their headquarters were raided the authorities retrieved RSA encrypted documents, and after finding the key on a floppy disk, decoded plans to deploy weapons of mass destruction in Japan and the US. Had they not had the luck to also discover the key, these documents could have been lost forever.

Quantum cryptography, as it stands at the moment, is purely a transmission cryptosystem. There is no provision for storage of encrypted data which can, and does, impede criminal investigations. Dorothy Denning listed the threats to society posed by encryption in her 1997 paper as:

> "*failure to get evidence needed for convictions, failure to get intelligence vital to criminal investigations, failure to avert catastrophic or harmful attacks, and failure to get foreign intelligence vital to national security. Encryption can also delay investigations, increase their costs, and necessitate the use of investigative methods which are more dangerous or invasive of privacy*"[11].

---

[9] Regulation of Investigatory Powers Act 2000 – Chapter 23 (ISBN 0105423009) http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm

[10] Weakened Encryption Lays Bare Al-Qaeda Files – Will Knight, *New Scientist*, 17/1/2002

[11] Encryption and Evolving Technologies as Tools of Organized Crime and Terrorism – Dorothy E. Denning, 1997

When quantum cryptography enters widespread public use it will only protect data in transit across public networks. However, assuming that eventually advances in particle physics will occur that allow storage of polarised photons, it will be possible to hold data could be completely unreadable without the key, and indeed any unauthorised attempt to read it will result in that data's destruction. The obvious legal response to this has already been enacted in the UK in the form of the mandatory key disclosure part of the RIP Act 2000.

It is currently still a contested issue to what extent existing cryptography hampers law enforcement, and it is difficult to obtain accurate information due to the secrecy of government agencies. Most of the investigators Denning spoke to did *not* find that "*encryption was obstructing a large number of investigations. They were, however, concerned about the future*". Denning estimated the number of criminal cases worldwide involving encryption in 1997 to be around 500, so using her 50%-100% estimation of annual growth, that puts the 2002 figure at somewhere between 4 000 and 16 000. The encryption systems encountered ranged from the well known DES, RSA and IDEA (International Data Encryption Algorithm) to more obscure proprietary systems and custom made ciphers. In the same year, 1997, in which the FBI contested that "*court ordered wire-tapping is the single most effective investigative technique used by law enforcement to counter illegal drugs, terrorism, violent crime, espionage and organized crime*", a White House official confirmed a worrying trend that "*organized crime members are some of the most advanced users of computer systems and of strong encryption*". In 2000 before a Senate panel, the director of the FBI, Louis Freeh stated that "*uncrackable encryption is allowing terrorists - Hamas, Hezbollah, Al-Qaeda and others - to communicate about their criminal intentions without fear of outside intrusion*".

In February 1997 the Australian Attorney-General's Department put a stop to the public release of the Walsh report, a review of the government's policies on cryptography. After one failed attempt to force disclosure of the document, the civil liberties group Electronic Frontiers Australia (EFA) successfully obtained a heavily edited version in June of 1997 under the Freedom of Information Act. In December 1998 the missing sections were recovered, and provide a rare insight into governmental attitudes to the increasing use of cryptography. Section 4.3.1 warned that:

> "*the loss of real-time access to communications would require the AFP the NCA and ASIO (and all State and Territory police services) to rely more heavily on human sources of information, on the use of listening devices, on tracking devices, on video surveillance, and on physical surveillance - all more invasive intrusions on a person's privacy*".

Later in section 4.3.4 the document confirms law enforcement's concern for the increasing criminal reliance on cryptography to destroy evidence:

> "*there is an observable pattern of changed encryption behaviour following arrests and even searches of property. Either the power of the encryption being employed is increased or the encryption practice, which may have been flawed because of poor password protection or similar, is enhanced*".

The Australian government originally suppressed these parts of the report under a section of the Freedom of Information Act which deals with documents affecting the enforcement of law and public safety. This suggests that a major component of the legal opposition to strong cryptography is based on restricting widespread knowledge of the available techniques; insecurity through obscurity is not an approach which is likely to prove effective in the long run.

Much of the press relating to cryptography is positive and focuses on the potential for protection from criminals. A major story in July of 2002 was the release by an offshoot from the hacking group Cult of the Dead Cow called Hacktivismo of a free tool called Camera/Shy which was touted as a worldwide benefit to democracy. The software uses steganography, hiding a secret message, combined with 256-bit encryption to encapsulate messages within GIF format picture files. The group maintains their product is aimed at political dissidents in countries with strict controls over the Internet, such as China, and will allow them to communicate securely with the rest of the world without fear of reprisals. It is a very valid point that a vital part of freedom of speech is the freedom to speak privately. Indeed it is recognised by Article 12 of the United Nations Universal Declaration of Human Rights:

> "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*"[12].

The future problem for the governments and security services will be that quantum cryptography can provide absolutely secure transmission of data with no degrees. There is no way to mitigate the level of security to allow provisos for people with a valid legal reason to access the data. Article 12 of the Declaration of Human Rights is increasingly being used as a justification for unfettered civilian access to strong cryptography, however the use in the article of the word "arbitrary" can be taken to mean that citizens may communicate privately only if it does not interfere with law enforcement.

[12] United Nations Universal Declaration of Human Rights, Article 12, http://www.un.org/Overview/rights.html

Key escrow, the legal requirement that all private citizens wishing to use digital encryption must register a copy of their encryption key with a trusted third party, has been vigorously contested by civil liberties groups in all countries where it has been proposed, most notably in the UK in the three years before the passing of the RIP Bill in 2000. The rejection of escrow and acceptance of the bill can be seen as a reasonable compromise, preserving privacy for users unless there is an explicitly court sanctioned warrant.

Echelon is the codename for a system which captures and keyword checks digital communications across the globe and is monitored by the five participant countries, the United States, the United Kingdom, Canada, Australia and New Zealand. Some sources claim up to 90% of Internet traffic is passed through Echelon[13], although claims are impossible to verify as all countries except Australia and New Zealand refuse to even acknowledge its existence. It is the indiscriminate gathering of information which most concerns civil libertarians, arguing that everyone's privacy is more important than any perceived reduction in crime. Successful implementation of a global network secured by quantum cryptography would quickly invalidate Echelon if we are to believe that terrorists and organised crime syndicates are the early adopters of cryptographic technology. Any eavesdropping techniques attempted by the security services would only allow them to damage the traffic, without discovering its contents. A report on Echelon published in 1988 found that:

> "*Whilst there is much information gathered about potential terrorists, there is a lot of economic intelligence, notably intensive monitoring of all the countries participating in the GATT [General Agreement on Tariffs and Trade] negotiations*"[14].

The release of the report sparked French protests that the US was using the system for industrial espionage. This is an echo of previously correct allegations that the American government was misusing telephone wire-taps in the Sixties to gather information which could be used to discredit perceived enemies, such as Martin Luther King Jr, whose civil rights campaign was regarded as a national security issue.

[13] The Government Is Reading Your E-Mail – Greg Lindsay, *Time Digital Daily*, June 24, 1999

[14] Somebody's Listening, Duncan Campbell – *New Statesman*, 12 August 1988

It is the opinion of many of the cryptography pioneers such as Rivest and Zimmerman, the idea of restricting a technology simply because it has the potential for criminal misuse is no argument at all. Rivest drew the parallel between cryptography and a pair of gloves, which could be used legitimately, or could be used to avoid leaving fingerprints at a crime scene. Dr Brian Gladman, Crypto Policy Co-ordinator at the UK organisation Cyber-Rights and Cyber-Liberties, has stated:

> "*I don't think there is any middle ground - we must sweep away all restrictions on crypto and, if we need to do so, introduce laws that control the bad uses of this technology. It is not illegal to own a kitchen knife but it is illegal to use one for murder. This is the only logical way forward.*"[15]

There are a variety of techniques which intelligence gathering organisations employ which no degree of encryption can prevent. The *tempest*[16] attack entails monitoring the variation between faint electromagnetic impulses which are emitted by keyboard cables when different keys are struck. The cable acts as an aerial and can broadcast this information outside the building where the computer is based. This can allow the capturing of an entire message in plaintext before any encryption is applied. In the US it is required to obtain a government license before fitting electro-magnetic shielding in a building, which suggests that this method is regularly used by intelligence agencies.

Trojans and backdoors are another type of tool for bypassing encryption. It is possible to develop a software daemon which, when unwittingly installed by a user, will listen for private key usage and then send the key together with passphrase to a designated Internet address[17]. There have been a number of high profile criminal cases recently involving FBI keystroke logging techniques, most notably that of loan shark Nicodemo S. Scarfo Jr who pleaded guilty in a New Jersey court to a charge of illegal gambling[18] in March 2002. Keystroke loggers are invisible processes running on a machine which make a note of every key pressed and can relay this information back to a server or email account. Defence attorneys in this particular case attempted to invalidate the evidence as unconstitutional; the prosecution in return invoked the Classified Information Protection Act 2001, which successfully defended the system as being essential to national security.

---

[15] Cryptology: Law Enforcement & National Security vs. Privacy, Security & The Future of Commerce – Nick Ellsmore, 1999, http://cryptome.org/crypto97-ne.htm

[16] An abbreviation for **T**ransient **E**lectro**m**agnetic **P**ulse **E**manation **St**andard

[17] The Caligula Word macro virus, found in the wild in 1998, captured private PGP keys and attempted to upload them to the author's FTP site (http://www.symantec.com/avcenter/venc/data/w97m.cali.a.html)

[18] Mobster Nailed By FBI Keystroke Logger Pleads Guilty – George A. Chidi Jr, *IDG News Service*, http://www.idg.net/idgns/2002/03/01/MobsterNailedByFBIKeystrokeLogger.shtml

It can be inferred that the tempest and keystroke logging approaches are, from the evidence available, widely utilised by at least the American intelligence services as a way around strong encryption. If this is indeed the case, the introduction of unbreakable quantum cryptography may not make as great an impact on the effectiveness of law enforcement as has been suggested by White House and FBI officials. The ideal balance between privacy and protection could still be realised, confidentiality for those who want it, with legal recourse to prevent abuse.

Conclusion

What has so far, in the history of cryptography, been a battle between the code-makers and the code-breakers looks set to become a conflict between civil libertarians and government agencies. A public and practical implementation of quantum cryptography would render multi-billion dollar departments of security agencies redundant. Existing or future legislation on key escrow or mandatory key disclosure would be completely ineffective. The only way in which these agencies could continue to harvest information regarded as essential to national security would be to limit civilian access to the new technology in the same way that crypto-software's export key lengths were restricted. The previous approach to controls was flawed because it was on entirely software based encryption mechanisms, requiring only an unauthorised software release by Phil Zimmerman to destroy all restrictions. Quantum cryptography, however, requires a relatively complex array of hardware to operate, or at least out of the reach of the average home user. Bennett and Smolin needed Pockels cells to set the polarity of the sender's photons, a calcite Wollaston prism to split the received beam and photomultiplier tubes to sense the individual received photons[19] (see Appendix III for a full diagram of the apparatus).

The most likely implementation of quantum cryptography which resolves the hardware issue will be on a local exchange level, similar to the current telephone network. The consumers of hardware encryption solutions at the current time are restricted to governments are large corporations where speed is of great importance. The vast majority of home users are unlikely to be persuaded of the benefits of total quantum security offset against the cost of the required optical hardware. If the quantum encryption itself is performed at a local exchange, this gives security agencies the opportunity to place taps to record information before it is unbreakably encrypted.

The real threat to criminal enquiries at the moment seems to stem from an increasing adoption of conventional digital encryption methods by organised crime and terrorist groups. Law enforcement officers warn of increasingly technologically aware criminals, and the fact that often a prosecution's success can hang on the outcome of file decryption attempts. In this environment, where 1024-bit RSA encryption can put a stop to a trial, it is difficult to see how the introduction of quantum cryptography could aid criminals. The change will happen when, and if, quantum computers become reality and destroy the security of all currently existing conventional ciphers. The most structured and well funded organised crime and terrorist groups will in all probability have both the resources and the technology to make use of satellite or cable-based quantum cryptosystems. The private citizen, on the other hand, is unlikely to have the means to achieve this and is in danger of being left behind in the race for absolute security.

[19] Experimental Quantum Cryptography – C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, *Journal of Cryptology*, vol. 5, no. 1, 1992, pp. 3 – 28

Impermeable encryption will, first and foremost, be a major boon for the world's militaries and corporations. E-commerce companies were a powerful lobbying force in favour of the relaxation of crypto export controls, due to the increase in security for Internet shopping, which was seen as leading to greater consumer confidence and higher revenues. Businesses also store vast quantities of confidential and 'mission critical' data which must be held and transmitted without the possibility of eavesdropping by malicious hackers or spies working for their rivals. The civil libertarians have a powerful ally in big business, and in the current absence of a clear danger posed by universal access to strong encryption, coupled with pressure from the commercial sector for liberalisation of restraints, Western governments in the future are likely to be more liberal in their crypto legislation.

FBI Director, Louis Freeh, described key escrow as balancing "*fundamental societal concerns involving privacy, information security, electronic commerce, public safety, and national security*". Mandatory key escrow is certainly a possibility for the future of conventional cryptography, the civil libertarian argument that this is the equivalent to giving the government keys to our houses overlooks the fact that law enforcement already has the right, if in possession of a warrant, to enter and search any private house. This may strike the right balance for conventional cryptosystems at the present time, however adapting it to the quantum model may prove problematic. Quantum communications *cannot* be invisibly intercepted, so any prior key knowledge would be of no use to anyone. In the future the two opposing camps across the crypto divide are liable to become even more polarised as quantum computers render conventional ciphers useless, and the choice we are left with offers quantum cryptography and absolute security, or none at all.

Only time will tell how cryptography will evolve in the future, the catalyst for development will be practical quantum computers which currently still lie in the realm of science fiction. The public may become more sympathetic to law enforcement and allow stringent laws limiting or prohibiting the use of unbreakable cryptography, or the reverse may occur leading to universal access to strong crypto and forcing law enforcement agencies back to more conventional and personal surveillance techniques. For the first time in the four thousand year history of the science of cryptography absolute security has been achieved, but is this state too dangerous for a modern society to tolerate?

Bibliography

The books and articles listed below have been used as general background research for the project. Where more specific information has been used in the text, the source has been credited using a footnote.

Brief History of Cryptography

Cryptography Timeline – Carl Ellison
http://world.std.com/~cme/html/timeline.html

The Codebreakers – David Kahn
Simon and Schuster, 1997, ISBN 0-68483-130-9

The Code Book – Simon Singh
Fourth Estate, 1999, ISBN 1-85702-879-1

Cryptographic Timeline – Thinkquest.org
http://library.thinkquest.org/28005/flashed/timemachine/timeline.shtml

The Zimmerman Telegram – Thinkquest.org
http://library.thinkquest.org/28005/flashed/timemachine/courseofhistory/zimmerman.shtml

The Development of Quantum Theory

Alice in Quantumland: An Allegory of Quantum Physics – Robert Gilmore
Copernicus Books, 1995, ISBN 0-38791-495-1

Quantum Mechanics History – J. J. O'Conner & E. F. Robertson
http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/The_Quantum_age_begins.html

Quantum Theory and Wave/Particle Duality – John K. N. Murphy
http://www.hotquanta.com/wpd.html

Introducing Quantum Theory – J. P. McEvoy & Oscar Zarate
Icon Books, 1999, ISBN 1-84046-057-1

The Centre for Quantum Computation
http://www.qubit.org

David Deutsch's Homepage
http://www.qubit.org/people/david/David.html

The Advent of Quantum Cryptography

Quantum Cryptography: Quantum Key Distribution and Coin Tossing – C. H. Bennett and G. Brassard
Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984, pp. 175 - 179

Crypto Set For a Quantum Leap – Niall McKay
Wired Magazine, 5th April 1999
http://www.wired.com/news/print/0,1294,18936,00.html

Experimental Quantum Cryptography – C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin
Journal of Cryptology, vol. 5, no. 1, 1992, pp. 3 - 28

Quantum Cryptography – C. H. Bennett, G. Brassard and A. K. Ekert
Scientific American, July 1992

Absolute Security and the Wider Social Issues

The Debate Over Cryptography and Scientific Freedom – Alexander Fowler
Professional Ethics Report, Volume X, Number 4, Autumn 1997

The Walsh Report (Australian Government Policy on Encryption)
http://www.efa.org.au/Issues/Crypto/Walsh/

Encryption, Organized Crime and Terrorism – Dorothy E. Denning, 1997

The Wassenaar Arrangement
http://www.wassenaar.org