History of cryptography

Cryptography, the use of codes and ciphers to protect secrets, began thousands of years ago. Until recent decades, it has been the story of what might be called classic cryptography — that is, of methods of encryption that use pen and paper, or perhaps simple mechanical aids. In the early 20th century, the invention of complex mechanical and electromechanical machines, such as the Enigma rotor machine, provided more sophisticated and efficient means of encryption; and the subsequent introduction of electronics and computing has allowed elaborate schemes of still greater complexity, most of which are entirely unsuited to pen and paper.

The development of cryptography has been paralleled by the development of cryptanalysis — the "breaking" of codes and ciphers. The discovery and application, early on, of frequency analysis to the reading of encrypted communications has, on occasion, altered the course of history. Thus the Zimmermann Telegram triggered the United States' entry into World War I; and Allied reading of Nazi Germany's ciphers shortened World War II, in some evaluations by as much as two years.

Until the 1960s, secure cryptography was largely the preserve of governments. Two events have since brought it squarely into the public domain: the creation of a public encryption standard (DES), and the invention of public-key cryptography.

Contents

Antiquity

The earliest known use of cryptography is found in non-standard hieroglyphs carved into the wall of a tomb from the Old Kingdom of Egypt circa 1900 BC.[1] These are not thought to be serious attempts at secret communications, however, but rather to have been attempts at mystery, intrigue, or even amusement for literate onlookers.[1]

A Scytale, an early device for encryption.

Some clay tablets from Mesopotamia somewhat later are clearly meant to protect information—one dated near 1500 BC was found to encrypt a craftsman's recipe for pottery glaze, presumably commercially valuable.[2][3] Furthermore, Hebrew scholars made use of simple monoalphabetic substitution ciphers (such as the Atbash cipher) beginning perhaps around 600 to 500 BC.[4][5]

In India around 400 BC to 200 AD, Mlecchita vikalpa or "the art of understanding writing in cypher, and the writing of words in a peculiar way" was documented in the Kama Sutra for the purpose of communication between lovers. This was also likely a simple substitution cipher.[6][7] Parts of the Egyptian demotic Greek Magical Papyri were written in a cypher script.[8]

The ancient Greeks are said to have known of ciphers.[9] The scytale transposition cipher was used by the Spartan military,[5] but it is not definitively known whether the scytale was for encryption, authentication, or avoiding bad omens in speech.[10][11] Herodotus tells us of secret messages physically concealed beneath wax on wooden tablets or as a tattoo on a slave's head concealed by regrown hair, although these are not properly examples of cryptography *per se* as the message, once known, is directly readable; this is known as steganography. Another Greek method was developed by Polybius (now called the "Polybius Square").[5] The Romans knew something of cryptography (e.g., the Caesar cipher and its variations).[12]

Medieval cryptography

David Kahn notes in *The Codebreakers* that modern cryptology originated among the Arabs, the first people to systematically document cryptanalytic methods.[13] Al-Khalil (717–786) wrote the *Book of Cryptographic Messages*, which contains the first use of permutations and combinations to list all possible Arabic words with and without vowels.[14]

The first page of al-Kindi's manuscript *On Deciphering Cryptographic Messages*, containing the first descriptions of cryptanalysis and frequency analysis.

The invention of the frequency analysis technique for breaking monoalphabetic substitution ciphers, by Al-Kindi, an Arab mathematician,[15][16] sometime around AD 800, proved to be the single most significant cryptanalytic advance until World War II. Al-Kindi wrote a book on cryptography entitled *Risalah fi Istikhraj al-Mu'amma* (*Manuscript for the Deciphering Cryptographic Messages*), in which he described the first cryptanalytic techniques, including some for polyalphabetic ciphers, cipher classification, Arabic phonetics and syntax, and most importantly, gave the first descriptions on frequency analysis.[17] He also covered methods of encipherments, cryptanalysis of certain encipherments, and statistical analysis of letters and letter combinations in Arabic.[18][19] An important contribution of Ibn Adlan (1187–1268) was on sample size for use of frequency analysis.[14]

In early medieval England between the years 800–1100, substitution ciphers were frequently used by scribes as a playful and clever way to encipher notes, solutions to riddles, and colophons. The ciphers tend to be fairly straightforward, but sometimes they deviate from an ordinary pattern, adding to their complexity, and possibly also to their sophistication.[20] This period saw vital and significant cryptographic experimentation in the West.

Ahmad al-Qalqashandi (AD 1355–1418) wrote the *Subh al-a 'sha*, a 14-volume encyclopedia which included a section on cryptology. This information was attributed to Ibn al-Durayhim who lived from AD 1312 to 1361, but whose writings on cryptography have been lost. The list of ciphers in this work included both substitution and transposition, and for the first time, a cipher with multiple substitutions for each plaintext letter (later called homophonic substitution). Also traced to Ibn al-Durayhim is an exposition on and a worked example of cryptanalysis, including the use of tables of letter frequencies and sets of letters which cannot occur together in one word.

The earliest example of the homophonic substitution cipher is the one used by Duke of Mantua in the early 1400s.[21] Homophonic cipher replaces each letter with multiple symbols depending on the letter frequency. The cipher is ahead of the time because it combines monoalphabetic and polyalphabetic features.

Essentially all ciphers remained vulnerable to the cryptanalytic technique of frequency analysis until the development of the polyalphabetic cipher, and many remained so thereafter. The polyalphabetic cipher was most clearly explained by Leon Battista Alberti around AD 1467, for which he was called the "father of Western cryptology".[1] Johannes Trithemius, in his work Poligraphia, invented the tabula recta, a critical component of the Vigenère cipher. Trithemius also wrote the Steganographia. The French cryptographer Blaise de Vigenère devised a practical polyalphabetic system which bears his name, the Vigenère cipher.[1]

In Europe, cryptography became (secretly) more important as a consequence of political competition and religious revolution. For instance, in Europe during and after the Renaissance, citizens of the various Italian states—the Papal States and the Roman Catholic Church included—were responsible for rapid proliferation of cryptographic techniques, few of which reflect understanding (or even knowledge) of Alberti's polyalphabetic advance. "Advanced ciphers", even after Alberti, were not as advanced as their inventors / developers / users claimed (and probably even they themselves believed). They were frequently broken. This over-optimism may be inherent in cryptography, for it was then – and remains today – difficult in principle to know how vulnerable one's own system is. In the absence of knowledge, guesses and hopes are predictably common.

Cryptography, cryptanalysis, and secret-agent/courier betrayal featured in the Babington plot during the reign of Queen Elizabeth I which led to the execution of Mary, Queen of Scots. Robert Hooke suggested in the chapter *Of Dr. Dee's Book of Spirits*, that John Dee made use of Trithemian steganography, to conceal his communication with Queen Elizabeth I.[22]

The chief cryptographer of King Louis XIV of France was Antoine Rossignol; he and his family created what is known as the Great Cipher because it remained unsolved from its initial use until 1890, when French military cryptanalyst, Étienne Bazeries solved it.[23] An encrypted message from the time of the Man in the Iron Mask (decrypted just prior to 1900 by Étienne Bazeries) has shed some, regrettably non-definitive, light on the identity of that real, if legendary and unfortunate, prisoner.

Outside of Europe, after the Mongols brought about the end of the Islamic Golden Age, cryptography remained comparatively undeveloped. Cryptography in Japan seems not to have been used until about 1510, and advanced techniques were not known until after the opening of the country to the West beginning in the 1860s.

Cryptography from 1800 to World War II

Although cryptography has a long and complex history, it wasn't until the 19th century that it developed anything more than ad hoc approaches to either encryption or cryptanalysis (the science of finding weaknesses in crypto systems). Examples of the latter include Charles Babbage's Crimean War era work on mathematical cryptanalysis of polyalphabetic ciphers, redeveloped and published somewhat later by the Prussian Friedrich Kasiski. Understanding of cryptography at this time typically consisted of hard-won rules of thumb; see, for example, Auguste Kerckhoffs' cryptographic writings in the latter 19th century. Edgar Allan Poe used systematic methods to solve ciphers in the 1840s. In particular he placed a notice of his abilities in the Philadelphia paper *Alexander's Weekly (Express) Messenger*, inviting submissions of ciphers, of which he proceeded to solve almost all. His success created a public stir for some months.[24] He later wrote an essay on methods of cryptography which proved useful as an introduction for novice British cryptanalysts attempting to break German codes and ciphers during World War I, and a famous story, *The Gold-Bug*, in which cryptanalysis was a prominent element.

Cryptography, and its misuse, were involved in the execution of Mata Hari and in Dreyfus' conviction and imprisonment, both in the early 20th century. Cryptographers were also involved in exposing the machinations which had led to the Dreyfus affair; Mata Hari, in contrast, was shot.

In World War I the Admiralty's Room 40 broke German naval codes and played an important role in several naval engagements during the war, notably in detecting major German sorties into the North Sea that led to the battles of Dogger Bank and Jutland as the British fleet was sent out to intercept them. However its most important contribution was probably in decrypting the Zimmermann Telegram, a cable from the German Foreign Office sent via Washington to its ambassador Heinrich von Eckardt in Mexico which played a major part in bringing the United States into the war.

In 1917, Gilbert Vernam proposed a teleprinter cipher in which a previously prepared key, kept on paper tape, is combined character by character with the plaintext message to produce the cyphertext. This led to the development of electromechanical devices as cipher machines, and to the only unbreakable cipher, the one time pad.

During the 1920s, Polish naval-officers assisted the Japanese military with code and cipher development.

Mathematical methods proliferated in the period prior to World War II (notably in William F. Friedman's application of statistical techniques to cryptanalysis and cipher development and in Marian Rejewski's initial break into the German Army's version of the Enigma system in 1932).

World War II cryptography

By World War II, mechanical and electromechanical cipher machines were in wide use, although—where such machines were impractical—code books and manual systems continued in use. Great advances were made in both cipher design and cryptanalysis, all in secrecy. Information about this period has begun to be declassified as the official British 50-year secrecy period has come to an end, as US archives have slowly opened, and as assorted memoirs and articles have appeared.

Germany

The Germans made heavy use, in several variants, of an electromechanical rotor machine known as Enigma.[25] Mathematician Marian Rejewski, at Poland's Cipher Bureau, in December 1932 deduced the detailed structure of the German Army Enigma, using mathematics and limited documentation supplied by Captain Gustave Bertrand of French military intelligence. This was the greatest breakthrough in cryptanalysis in a thousand years and more, according to historian David Kahn. Rejewski and his mathematical Cipher Bureau colleagues, Jerzy Różycki and Henryk Zygalski, continued reading Enigma and keeping pace with the

evolution of the German Army machine's components and encipherment procedures. As the Poles' resources became strained by the changes being introduced by the Germans, and as war loomed, the Cipher Bureau, on the Polish General Staff's instructions, on 25 July 1939, at Warsaw, initiated French and British intelligence representatives into the secrets of Enigma decryption.

The Enigma machine was widely used by Nazi Germany; its cryptanalysis by the Allies provided vital Ultra intelligence.

Soon after the Invasion of Poland by Germany on 1 September 1939, key Cipher Bureau personnel were evacuated southeastward; on 17 September, as the Soviet Union attacked Poland from the East, they crossed into Romania. From there they reached Paris, France; at PC Bruno, near Paris, they continued working toward breaking Enigma, collaborating with British cryptologists at Bletchley Park as the British got up to speed on their work breaking Enigma. In due course, the British cryptographers – whose ranks included many chess masters and mathematics dons such as Gordon Welchman, Max Newman, and Alan Turing (the conceptual founder of modern computing) – made substantial breakthroughs in the scale and technology of Enigma decryption.

German code breaking in World War II also had some success, most importantly by breaking the Naval Cipher No. 3. This enabled them to track and sink Atlantic convoys. It was only Ultra intelligence that finally persuaded the admiralty to change their codes in June 1943. This is surprising given the success of the British Room 40 code breakers in the previous world war.

At the end of the War, on 19 April 1945, Britain's top military officers were told that they could never reveal that the German Enigma cipher had been broken because it would give the defeated enemy the chance to say they "were not well and fairly beaten".[26]

The German military also deployed several teleprinter stream ciphers. Bletchley Park called them the Fish ciphers, and Max Newman and colleagues designed and deployed the Heath Robinson, and then the world's first programmable digital electronic computer, the Colossus, to help with their cryptanalysis. The German Foreign Office began to use the one-time pad in 1919; some of this traffic was read in World War II partly as the result of recovery of some key material in South America that was discarded without sufficient care by a German courier.

The *Schlüsselgerät 41* was developed late in the war as a more secure replacement for Enigma, but only saw limited use.

Japan

A US Army group, the SIS, managed to break the highest security Japanese diplomatic cipher system (an electromechanical stepping switch machine called Purple by the Americans) in 1940, before World War II began. The locally developed Purple machine replaced the earlier "Red" machine used by the Japanese Foreign Ministry, and a related machine, the M-1, used by Naval attachés which was broken by the U.S. Navy's Agnes Driscoll. All the Japanese machine ciphers were broken, to one degree or another, by the Allies.

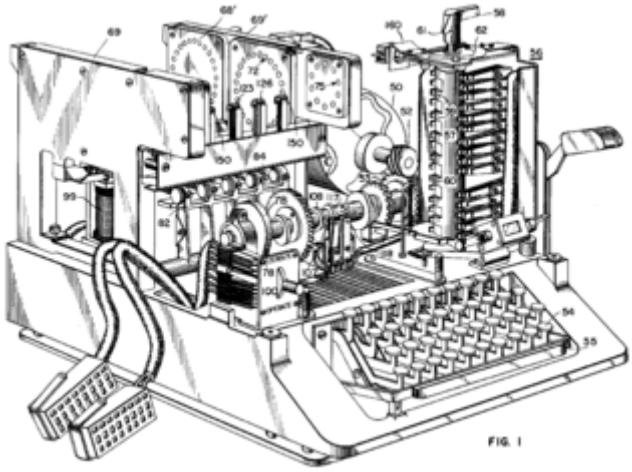
The Japanese Navy and Army largely used code book systems, later with a separate numerical additive. US Navy cryptographers (with cooperation from British and Dutch cryptographers after 1940) broke into several Japanese Navy crypto systems. The break into one of them, JN-25, famously led to the US victory in the

Battle of Midway; and to the publication of that fact in the Chicago Tribune shortly after the battle, though the Japanese seem not to have noticed for they kept using the JN-25 system.

Allies

The Americans referred to the intelligence resulting from cryptanalysis, perhaps especially that from the Purple machine, as 'Magic'. The British eventually settled on 'Ultra' for intelligence resulting from cryptanalysis, particularly that from message traffic protected by the various Enigmas. An earlier British term for Ultra had been 'Boniface' in an attempt to suggest, if betrayed, that it might have an individual agent as a source.

Allied cipher machines used in World War II included the British TypeX and the American SIGABA; both were electromechanical rotor designs similar in spirit to the Enigma, albeit with major improvements. Neither is known to have been broken by anyone during the War. The Poles used the Lacida machine, but its security was found to be less than intended (by Polish Army cryptographers in the UK), and its use was discontinued. US troops in the field used the M-209 and the still less secure M-94 family machines. British SOE agents initially used 'poem ciphers' (memorized poems were the encryption/decryption keys), but later in the War, they began to switch to one-time pads.



SIGABA is described in U.S. Patent 6,175,625 (https://www.google.com/patents/US6175625), filed in 1944 but not issued until 2001.

The VIC cipher (used at least until 1957 in connection with Rudolf Abel's NY spy ring) was a very complex hand cipher, and is claimed to be the most complicated known to have been used by the Soviets, according to David Kahn in *Kahn on Codes*. For the decrypting of Soviet ciphers (particularly when *one-time pads* were reused), see Venona project.

Role of women

The UK and US employed large numbers of women in their code-breaking operation, with close to 7,000 reporting to Bletchley Park[27] and 11,000 to the separate US Army and Navy operations, around Washington, DC.[28] By tradition in Japan and Nazi doctrine in Germany, women were excluded from war work, at least until late in the war. Even after encryption systems were broken, large amounts of work were needed to respond to changes made, recover daily key stettings for multiple networks, and intercept, process, translate, prioritize and analyze the huge volume of enemy messages generated in a global conflict. A few women, including Elizabeth Friedman and Agnes Meyer Driscoll, had been major contributors to US code-breaking in the 1930s and the Navy and Army began actively recruiting top graduates of women's colleges shortly before the attack on Pearl Harbor. Liza Mundy argues that this disparity in utilizing the talents of women between the Allies and Axis made a strategic difference in the war.[28]:p.29

Modern cryptography

Encryption in modern times is achieved by using algorithms that have a key to encrypt and decrypt information. These keys convert the messages and data into "digital gibberish" through encryption and then return them to the original form through decryption. In general, the longer the key is, the more difficult it is to crack the code. This holds true because deciphering an encrypted message by brute force would require the

attacker to try every possible key. To put this in context, each binary unit of information, or bit, has a value of 0 or 1. An 8-bit key would then have 256 or 2^8 possible keys. A 56-bit key would have 2^56, or 72 quadrillion, possible keys to try and decipher the message. With modern technology, cyphers using keys with these lengths are becoming easier to decipher. DES, an early US Government approved cypher, has an effective key length of 56 bits, and test messages using that cypher have been broken by brute force key search. However, as technology advances, so does the quality of encryption. Since World War II, one of the most notable advances in the study of cryptography is the introduction of the asymmetric key cyphers (sometimes termed public-key cyphers). These are algorithms which use two mathematically related keys for encryption of the same message. Some of these algorithms permit publication of one of the keys, due to it being extremely difficult to determine one key simply from knowledge of the other.[29]

Beginning around 1990, the use of the Internet for commercial purposes and the introduction of commercial transactions over the Internet called for a widespread standard for encryption. Before the introduction of the Advanced Encryption Standard (AES), information sent over the Internet, such as financial data, was encrypted if at all, most commonly using the Data Encryption Standard (DES). This had been approved by NBS (a US Government agency) for its security, after public call for, and a competition among, candidates for such a cypher algorithm. DES was approved for a short period, but saw extended use due to complex wrangles over the use by the public of high quality encryption. DES was finally replaced by the AES after another public competition organized by the NBS successor agency, NIST. Around the late 1990s to early 2000s, the use of public-key algorithms became a more common approach for encryption, and soon a hybrid of the two schemes became the most accepted way for e-commerce operations to proceed. Additionally, the creation of a new protocol known as the Secure Socket Layer, or SSL, led the way for online transactions to take place. Transactions ranging from purchasing goods to online bill pay and banking used SSL. Furthermore, as wireless Internet connections became more common among households, the need for encryption grew, as a level of security was needed in these everyday situations.[30]

Claude Shannon

Claude E. Shannon is considered by many to be the father of mathematical cryptography. Shannon worked for several years at Bell Labs, and during his time there, he produced an article entitled "A mathematical theory of cryptography". This article was written in 1945 and eventually was published in the Bell System Technical Journal in 1949.[31] It is commonly accepted that this paper was the starting point for development of modern cryptography. Shannon was inspired during the war to address "[t]he problems of cryptography [because] secrecy systems furnish an interesting application of communication theory". Shannon identified the two main goals of cryptography: secrecy and authenticity. His focus was on exploring secrecy and thirty-five years later, G.J. Simmons would address the issue of authenticity. Shannon wrote a further article entitled "A mathematical theory of communication" which highlights one of the most significant aspects of his work: cryptography's transition from art to science.[32]

In his works, Shannon described the two basic types of systems for secrecy. The first are those designed with the intent to protect against hackers and attackers who have infinite resources with which to decode a message (theoretical secrecy, now unconditional security), and the second are those designed to protect against hackers and attacks with finite resources with which to decode a message (practical secrecy, now computational security). Most of Shannon's work focused around theoretical secrecy; here, Shannon introduced a definition for the "unbreakability" of a cipher. If a cipher was determined "unbreakable", it was considered to have "perfect secrecy". In proving "perfect secrecy", Shannon determined that this could only be obtained with a secret key whose length given in binary digits was greater than or equal to the number of bits contained in the information being encrypted. Furthermore, Shannon developed the "unicity distance", defined as the "amount of plaintext that… determines the secret key."[32]

Shannon's work influenced further cryptography research in the 1970s, as the public-key cryptography developers, M. E. Hellman and W. Diffie cited Shannon's research as a major influence. His work also impacted modern designs of secret-key ciphers. At the end of Shannon's work with cryptography, progress slowed until Hellman and Diffie introduced their paper involving "public-key cryptography".[32]

An encryption standard

The mid-1970s saw two major public (i.e., non-secret) advances. First was the publication of the draft Data Encryption Standard in the U.S. *Federal Register* on 17 March 1975. The proposed DES cipher was submitted by a research group at IBM, at the invitation of the National Bureau of Standards (now NIST), in an effort to develop secure electronic communication facilities for businesses such as banks and other large financial organizations. After advice and modification by the NSA, acting behind the scenes, it was adopted and published as a Federal Information Processing Standard Publication in 1977 (currently at FIPS 46-3 (http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf)). DES was the first publicly accessible cipher to be 'blessed' by a national agency such as the NSA. The release of its specification by NBS stimulated an explosion of public and academic interest in cryptography.

The aging DES was officially replaced by the Advanced Encryption Standard (AES) in 2001 when NIST announced FIPS 197. After an open competition, NIST selected Rijndael, submitted by two Belgian cryptographers, to be the AES. DES, and more secure variants of it (such as Triple DES), are still used today, having been incorporated into many national and organizational standards. However, its 56-bit key-size has been shown to be insufficient to guard against brute force attacks (one such attack, undertaken by the cyber civil-rights group Electronic Frontier Foundation in 1997, succeeded in 56 hours.[33]) As a result, use of straight DES encryption is now without doubt insecure for use in new cryptosystem designs, and messages protected by older cryptosystems using DES, and indeed all messages sent since 1976 using DES, are also at risk. Regardless of DES' inherent quality, the DES key size (56-bits) was thought to be too small by some even in 1976, perhaps most publicly by Whitfield Diffie. There was suspicion that government organizations even then had sufficient computing power to break DES messages; clearly others have achieved this capability.

Public key

The second development, in 1976, was perhaps even more important, for it fundamentally changed the way cryptosystems might work. This was the publication of the paper New Directions in Cryptography (http://www-ee.stanford.edu/~hellman/publications/24.pdf) by Whitfield Diffie and Martin Hellman. It introduced a radically new method of distributing cryptographic keys, which went far toward solving one of the fundamental problems of cryptography, key distribution, and has become known as Diffie–Hellman key exchange. The article also stimulated the almost immediate public development of a new class of enciphering algorithms, the asymmetric key algorithms.

Prior to that time, all useful modern encryption algorithms had been symmetric key algorithms, in which the same cryptographic key is used with the underlying algorithm by both the sender and the recipient, who must both keep it secret. All of the electromechanical machines used in World War II were of this logical class, as were the Caesar and Atbash ciphers and essentially all cipher systems throughout history. The 'key' for a code is, of course, the codebook, which must likewise be distributed and kept secret, and so shares most of the same problems in practice.

Of necessity, the key in every such system had to be exchanged between the communicating parties in some secure way prior to any use of the system (the term usually used is 'via a secure channel') such as a trustworthy courier with a briefcase handcuffed to a wrist, or face-to-face contact, or a loyal carrier pigeon. This requirement is never trivial and very rapidly becomes unmanageable as the number of participants increases, or

when secure channels aren't available for key exchange, or when, as is sensible cryptographic practice, keys are frequently changed. In particular, if messages are meant to be secure from other users, a separate key is required for each possible pair of users. A system of this kind is known as a secret key, or symmetric key cryptosystem. D-H key exchange (and succeeding improvements and variants) made operation of these systems much easier, and more secure, than had ever been possible before in all of history.

In contrast, asymmetric key encryption uses a pair of mathematically related keys, each of which decrypts the encryption performed using the other. Some, but not all, of these algorithms have the additional property that one of the paired keys cannot be deduced from the other by any known method other than trial and error. An algorithm of this kind is known as a public key or asymmetric key system. Using such an algorithm, only one key pair is needed per user. By designating one key of the pair as private (always secret), and the other as public (often widely available), no secure channel is needed for key exchange. So long as the private key stays secret, the public key can be widely known for a very long time without compromising security, making it safe to reuse the same key pair indefinitely.

For two users of an asymmetric key algorithm to communicate securely over an insecure channel, each user will need to know their own public and private keys as well as the other user's public key. Take this basic scenario: Alice and Bob each have a pair of keys they've been using for years with many other users. At the start of their message, they exchange public keys, unencrypted over an insecure line. Alice then encrypts a message using her private key, and then re-encrypts that result using Bob's public key. The double-encrypted message is then sent as digital data over a wire from Alice to Bob. Bob receives the bit stream and decrypts it using his own private key, and then decrypts that bit stream using Alice's public key. If the final result is recognizable as a message, Bob can be confident that the message actually came from someone who knows Alice's private key (presumably actually her if she's been careful with her private key), and that anyone eavesdropping on the channel will need Bob's private key in order to understand the message.

Asymmetric algorithms rely for their effectiveness on a class of problems in mathematics called one-way functions, which require relatively little computational power to execute, but vast amounts of power to reverse, if reversal is possible at all. A classic example of a one-way function is multiplication of very large prime numbers. It's fairly quick to multiply two large primes, but very difficult to find the factors of the product of two large primes. Because of the mathematics of one-way functions, most possible keys are bad choices as cryptographic keys; only a small fraction of the possible keys of a given length are suitable, and so asymmetric algorithms require very long keys to reach the same level of security provided by relatively shorter symmetric keys. The need to both generate the key pairs, and perform the encryption/decryption operations make asymmetric algorithms computationally expensive, compared to most symmetric algorithms. Since symmetric algorithms can often use any sequence of (random, or at least unpredictable) bits as a key, a disposable *session key* can be quickly generated for short-term use. Consequently, it is common practice to use a long asymmetric key to exchange a disposable, much shorter (but just as strong) symmetric key. The slower asymmetric algorithm securely sends a symmetric session key, and the faster symmetric algorithm takes over for the remainder of the message.

Asymmetric key cryptography, Diffie–Hellman key exchange, and the best known of the public key / private key algorithms (i.e., what is usually called the RSA algorithm), all seem to have been independently developed at a UK intelligence agency before the public announcement by Diffie and Hellman in 1976. GCHQ has released documents claiming they had developed public key cryptography before the publication of Diffie and Hellman's paper. Various classified papers were written at GCHQ during the 1960s and 1970s which eventually led to schemes essentially identical to RSA encryption and to Diffie–Hellman key exchange in 1973 and 1974. Some of these have now been published, and the inventors (James H. Ellis, Clifford Cocks, and Malcolm Williamson) have made public (some of) their work.

Hashing

Hashing is a common technique used in cryptography to encode information quickly using typical algorithms. Generally, an algorithm is applied to a string of text, and the resulting string becomes the "hash value". This creates a "digital fingerprint" of the message, as the specific hash value is used to identify a specific message. The output from the algorithm is also referred to as a "message digest" or a "check sum". Hashing is good for determining if information has been changed in transmission. If the hash value is different upon reception than upon sending, there is evidence the message has been altered. Once the algorithm has been applied to the data to be hashed, the hash function produces a fixed-length output. Essentially, anything passed through the hash function should resolve to the same length output as anything else passed through the same hash function. It is important to note that hashing is not the same as encrypting. Hashing is a one-way operation that is used to transform data into the compressed message digest. Additionally, the integrity of the message can be measured with hashing. Conversely, encryption is a two-way operation that is used to transform plaintext into cipher-text and then vice versa. In encryption, the confidentiality of a message is guaranteed.[34]

Hash functions can be used to verify digital signatures, so that when signing documents via the Internet, the signature is applied to one particular individual. Much like a hand-written signature, these signatures are verified by assigning their exact hash code to a person. Furthermore, hashing is applied to passwords for computer systems. Hashing for passwords began with the UNIX operating system. A user on the system would first create a password. That password would be hashed, using an algorithm or key, and then stored in a password file. This is still prominent today, as web applications that require passwords will often hash user's passwords and store them in a database.[35]

Cryptography politics

The public developments of the 1970s broke the near monopoly on high quality cryptography held by government organizations (see S Levy's *Crypto* for a journalistic account of some of the policy controversy of the time in the US). For the first time ever, those outside government organizations had access to cryptography not readily breakable by anyone (including governments). Considerable controversy, and conflict, both public and private, began more or less immediately, sometimes called the crypto wars. They have not yet subsided. In many countries, for example, export of cryptography is subject to restrictions. Until 1996 export from the U.S. of cryptography using keys longer than 40 bits (too small to be very secure against a knowledgeable attacker) was sharply limited. As recently as 2004, former FBI Director Louis Freeh, testifying before the 9/11 Commission, called for new laws against public use of encryption.

One of the most significant people favoring strong encryption for public use was Phil Zimmermann. He wrote and then in 1991 released PGP (Pretty Good Privacy), a very high quality crypto system. He distributed a freeware version of PGP when he felt threatened by legislation then under consideration by the US Government that would require backdoors to be included in all cryptographic products developed within the US. His system was released worldwide shortly after he released it in the US, and that began a long criminal investigation of him by the US Government Justice Department for the alleged violation of export restrictions. The Justice Department eventually dropped its case against Zimmermann, and the freeware distribution of PGP has continued around the world. PGP even eventually became an open Internet standard (RFC 2440 or OpenPGP).

Modern cryptanalysis

While modern ciphers like AES and the higher quality asymmetric ciphers are widely considered unbreakable, poor designs and implementations are still sometimes adopted and there have been important cryptanalytic breaks of deployed crypto systems in recent years. Notable examples of broken crypto designs include the first Wi-Fi encryption scheme WEP, the Content Scrambling System used for encrypting and controlling DVD use, the A5/1 and A5/2 ciphers used in GSM cell phones, and the CRYPTO1 cipher used in the widely deployed MIFARE Classic smart cards from NXP Semiconductors, a spun off division of Philips Electronics. All of

these are symmetric ciphers. Thus far, not one of the mathematical ideas underlying public key cryptography has been proven to be 'unbreakable', and so some future mathematical analysis advance might render systems relying on them insecure. While few informed observers foresee such a breakthrough, the key size recommended for security as best practice keeps increasing as increased computing power required for breaking codes becomes cheaper and more available. Quantum computers, if ever constructed with enough capacity, could break existing public key algorithms and efforts are underway to develop and standardize post-quantum cryptography.

Even without breaking encryption in the traditional sense, side-channel attacks can be mounted that exploit information gained from the way a computer system is implemented, such as cache memory usage, timing information, power consumption, electromagnetic leaks or even sounds emitted. Newer cryptographic algorithms are being developed that make such attacks more difficult.

See also

- NSA encryption systems
- Steganography
- Timeline of cryptography
- Topics in cryptography
- Japanese cryptology from the 1500s to Meiji
- World War I cryptography
- World War II cryptography
- List of cryptographers
- Category:Undeciphered historical codes and ciphers

References

1. "A Brief History of Cryptography" (http://www.cypher.com.au/crypto_history.htm). Cypher Research Laboratories. 24 January 2006. Retrieved 18 September 2013.
2. "Cryptography in Ancient Civilizations" (http://cs.colgate.edu/faculty/chris/FSemWeb/FSem%20presentations/fsem%20slides%20Final.ppt). Retrieved 18 September 2013.
3. Kahn, David. *The Codebreakers: A Comprehensive History of Secret Communication from Ancient Times to the Internet, Revised and Updated*. Scribner. New York, New York. 1996.
4. "A Brief History of Cryptography." *Cryptozine.* 16 May 2008. (http://cryptozine.blogspot.com/2008/05/brief-history-of-cryptography.html)
5. "2.1 - A Short History of Cryptography" (http://all.net/edu/curr/ip/Chap2-1.html). *all.net*. Retrieved 19 March 2018.
6. Translators: Richard Burton, Bhagavanlal Indrajit, Shivaram Parashuram Bhide (18 January 2009). *The Kama Sutra of Vatsyayana (Translated From The Sanscrit In Seven Parts With Preface,Introduction and Concluding Remarks)* (http://www.gutenberg.org/files/27827/27827-h/27827-h.htm). The Project Gutenberg. Retrieved 3 December 2015.
7. David Kahn (December 1996). *The Codebreakers* (https://books.google.com/books?id=SEH_rHkgaogC&pg=PA1000&lpg=PA1000&dq=chinese+cryptography+history&source=bl&ots=_2hrl9t0B1&sig=2LAjURo7zlj5YBoExJjZXbjDhNU&hl=en&sa=X&ved=0ahUKEwiAidiN_KvJAhUUVI4KHfl9DA44ChDoAQgwMAQ#v=onepage&q=chinese%20cryptography%20history&f=false). Simon and Schuster. p. 74. ISBN 9781439103555. Retrieved 25 November 2015.
8. Hans Dieter Betz (1992). "The Greek Magical Papyri in Translation, Including the Demotic Spells, Volume 1" (http://press.uchicago.edu/ucp/books/book/chicago/G/bo3684249.html).

9. "History of Encryption" (https://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730). *SANS*.
10. Kelly, Thomas. "The Myth of the Skytale." Cryptologia 22.3 (1998): 244–260.
11. Lateiner, D. "Signifying Names and Other Ominous Accidental Utterances in Classical Historiography." Greek, Roman, and Byzantine Studies 45.1 (2010): 35–57. Print.
12. icitsuser (22 January 2017). "The Ancient Cryptography History" (http://www.icits2015.net/ancient-cryptography-history/). *ICITS*. Retrieved 7 April 2019.
13. Kahn, David (1996). *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* (https://books.google.com/books?id=3S8rhOEmDIIC&printsec=frontcover&dq=david+kahn+the+codebreakers&hl=en&sa=X&ved=0ahUKEwiG8OW9_L3aAhXCwxQKHS6hAA0Q6AEIlzAA#v=snippet&q=Arabs%20cryptology%20born&f=false). Simon and Schuster. ISBN 9781439103555.
14. Broemeling, Lyle D. (1 November 2011). "An Account of Early Statistical Inference in Arab Cryptology". *The American Statistician*. **65** (4): 255–257. doi:10.1198/tas.2011.10191 (https://doi.org/10.1198%2Ftas.2011.10191).
15. Leaman, Oliver (16 July 2015). "The Biographical Encyclopedia of Islamic Philosophy" (https://books.google.com/books?id=2wS2CAAAQBAJ&pg=PA279&dq=al+kindi+Arab&hl=en&sa=X&ved=0ahUKEwir87melZzYAhWCXBQKHTwOAKI4ChDoAQg1MAc#v=onepage&q=al+kindi+Arab&f=false/). Bloomsbury Publishing. Retrieved 19 March 2018 – via Google Books.
16. Al-Jubouri, I. M. N. (19 March 2018). "History of Islamic Philosophy: With View of Greek Philosophy and Early History of Islam" (https://books.google.com/books?id=3xJjNG5CNdwC&pg=PA199&dq=Al+Kindi+Arab&hl=en&sa=X&ved=0ahUKEwjsjMXP3ZvYAhUFthQKHQ2nCDk4HhDoAQgpMAQ#v=onepage&q=Al+Kindi+Arab&f=false/). Authors On Line Ltd. Retrieved 19 March 2018 – via Google Books.
17. Simon Singh, *The Code Book*, pp. 14–20
18. "Al-Kindi, Cryptgraphy, Codebreaking and Ciphers" (http://www.muslimheritage.com/topics/default.cfm?ArticleID=372). Retrieved 12 January 2007.
19. Ibrahim A. Al-Kadi (April 1992), "The origins of cryptology: The Arab contributions", *Cryptologia* **16** (2): 97–126
20. Saltzman, Benjamin A. "Ut hkskdkxt: Early Medieval Cryptography, Textual Errors, and Scribal Agency (Speculum, forthcoming)" (https://www.academia.edu/35034685/Ut_hkskdkxt_Early_Medieval_Cryptography_Textual_Errors_and_Scribal_Agency_Speculum_forthcoming_). *Speculum*.
21. David Salamon Coding for Data and Computer Communications (https://books.google.com/books?id=A88kvYwIVu0C&pg=PA224&lpg=PA224&dq=homophonic+mantua+1400s&source=bl&ots=yFuWvMfqjC&sig=1A9yxLbgHYsbL-LVmg9XatDGVxI&hl=en&sa=X&ved=0ahUKEwjEoMnxqvDKAhWGWCwKHXdPA_cQ6AEIGjAA#v=onepage&q&f=false). Springer, 2006.
22. Robert Hooke (1705). *The Posthumous Works of Robert Hooke* (https://books.google.com/books?id=6xVTAAAAcAAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false). Richard Waller, London. p. 203.
23. Lund, Paul (2009). *The Book of Codes* (https://archive.org/details/bookofcodesunder0000unse/page/106). Berkeley and Los Angeles, California: University of California Press. pp. 106–107 (https://archive.org/details/bookofcodesunder0000unse/page/106). ISBN 9780520260139.
24. Silverman, Kenneth. *Edgar A. Poe: Mournful and Never-ending Remembrance*. New York: Harper Perennial, 1991. p. 152-3
25. "Infographic - The History of Encryption" (http://www.egress.com/history-of-encryption-infographic/). *www.egress.com*. Retrieved 19 March 2018.
26. Fenton, Ben (22 June 2006). "Enigma and the British code of honour" (https://www.telegraph.co.uk/news/main.jhtml?xml=/news/2006/06/22/nenigma22.xml&sSheet=/news/2006/06/22/ixuknews.html). *The Daily Telegraph*. London.

27. Fessenden, Marissa (27 January 2015). "Women Were Key to WWII Code-Breaking at Bletchley Park" (https://www.smithsonianmag.com/smart-news/women-were-key-code-breaking-bletchley-park-180954044/). Smithsonian Magazine. Retrieved 10 May 2019. "At its height there were more than 10,000 people working at Bletchley Park, of whom more than two-thirds were women."
28. Mundy, Liza (2017). *Code Girls: The Untold Story of the American Women Code Breakers of World War II*. New York, Boston: Hachette Books. ISBN 978-0-316-35253-6.
29. Froomkin, Dan (8 May 1998). "Deciphering Encryption" (https://www.washingtonpost.com/wp-srv/politics/special/encryption/encryption.htm). *Washington Post*. Retrieved 18 September 2013.
30. Lee, Tom (August 2000). "Cryptography and the New Economy" (https://web.archive.org/web/20120216144832/http://www.aip.org/tip/INPHFA/vol-6/iss-4/p31.pdf) (PDF). *The Industrial Physicist*. **6** (4): 31. Archived from the original (http://aip.org/tip/INPHFA/vol-6/iss-4/p31.pdf) (pdf) on 16 February 2012. Retrieved 18 September 2013.
31. Communication theory of secrecy systems (http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf), Claude Shannon, 1949
32. Berlekamp, Elwyn; Solomon W. Golomb; Thomas M. Cover; Robert G. Gallager; James L. Massey; Andrew J. Viterbi (January 2002). "Claude Elwood Shannon (1916–2001)" (http://www.ams.org/notices/200201/fea-shannon.pdf) (pdf). *Notices of the AMS*. **49** (1): 8–16. Retrieved 18 September 2013.
33. Electronic Frontier Foundation, *Cracking DES*, O'Reilly, 1998.
34. Shon Harris. "Cryptography" (https://web.archive.org/web/20120915151722/http://www.cccure.org/Documents/Cryptography/cisspallinone.pdf) (PDF). Archived from the original (https://www.cccure.org/Documents/Cryptography/cisspallinone.pdf) (pdf) on 15 September 2012. Retrieved 18 September 2013.
35. Grah, Joseph Sterling. "Hash Functions in Cryptography" (https://bora.uib.no/bitstream/handle/1956/3206/47401627.pdf) (pdf). Retrieved 18 September 2013.

External links

- Helger Lipmaa's cryptography pointers (https://web.archive.org/web/20081221121411/http://research.cyber.ee/~lipmaa/crypto/)
- Timeline of cipher machines (http://users.telenet.be/d.rijmenants/en/timeline.htm)
