Cryptography

Cryptography, or **cryptology** (from Ancient Greek: κρυπτός, romanized: *kryptós* "hidden, secret"; and γράφειν *graphein*, "to write", or -λογία *-logia*, "study", respectively[1]), is the practice and study of techniques for secure communication in the presence of adversarial behavior.[2] More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages.[3] Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, information security, electrical engineering, digital signal processing, physics, and others.[4][5] Core concepts related to information security (data confidentiality, data integrity, authentication, and non-repudiation) are also central to cryptography.[6] Practical applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.[5]

Lorenz cipher machine, used in World War II to encrypt communications of the German High Command

Cryptography prior to the modern age was effectively synonymous with encryption, converting readable information (plaintext) to unintelligible nonsense text (ciphertext), which can only be read by reversing the process (decryption). The sender of an encrypted (coded) message shares the decryption (decoding) technique only with intended recipients to preclude access from adversaries. The cryptography literature often uses the names "Alice" (or "A") for the sender, "Bob" (or "B") for the intended recipient, and "Eve" (or "E") for the evesdropper adversary.[7] Since the development of rotor cipher machines in World War I and the advent of computers in World War II, cryptography methods have become increasingly complex and their applications more varied.

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in actual practice by any adversary. While it is theoretically possible to break into a well-designed system, it is infeasible in actual practice to do so. Such schemes, if well designed, are therefore termed "computationally secure"; theoretical advances (e.g., improvements in integer factorization algorithms) and faster computing technology require these designs to be continually reevaluated, and if necessary, adapted. Information-theoretically secure schemes that provably cannot be broken even with unlimited computing power, such as the one-time pad, are much more difficult to use in practice than the best theoretically breakable, but computationally secure, schemes.

The growth of cryptographic technology has raised a number of legal issues in the Information Age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export.[8] In some jurisdictions where the use of cryptography is legal, laws permit investigators to compel the disclosure of encryption keys for documents relevant to an investigation.[9][10] Cryptography also plays a major role in digital rights management and copyright infringement disputes in regard to digital media.[11]

Contents

Terminology

The first use of the term "cryptograph" (as opposed to "cryptogram") dates back to the 19th century—originating from "The Gold-Bug," a story by Edgar Allan Poe.[12][13]

Until modern times, cryptography referred almost exclusively to "encryption", which is the process of converting ordinary information (called plaintext) into an unintelligible form (called ciphertext).[14] Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. A cipher (or cypher) is a pair of algorithms that carry out the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and, in each instance, by a "key". The key is a secret (ideally known only to the communicants), usually a string of characters (ideally short so it can be remembered by the user), which is needed to decrypt the ciphertext. In formal
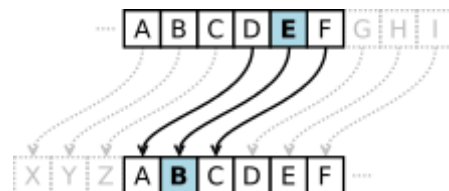
Alphabet shift ciphers are believed to have been used by Julius Caesar over 2,000 years ago.[7] This is an example with $k = 3$. In other words, the letters in the alphabet are shifted three in one direction to encrypt and three in the other direction to decrypt.

mathematical terms, a "cryptosystem" is the ordered list of elements of finite possible plaintexts, finite possible cyphertexts, finite possible keys, and the encryption and decryption algorithms that correspond to each key. Keys are important both formally and in actual practice, as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless (or even counter-productive) for most purposes. Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks.

There are two main types of cryptosystems: symmetric and asymmetric. In symmetric systems, the only ones known until the 1970s, the same secret key encrypts and decrypts a message. Data manipulation in symmetric systems is significantly faster than in asymmetric systems. Asymmetric systems use a "public key" to encrypt a message and a related "private key" to decrypt it. The advantage of asymmetric systems is that the public key can be freely published, allowing parties to establish secure communication without having a shared secret key. In practice, asymmetric systems are used to first exchange a secret key, and then secure communication proceeds via a more efficient symmetric system using that key.[15] Examples of asymmetric systems include Diffie–Hellman key exchange, RSA (Rivest–Shamir–Adleman), ECC (Elliptic Curve Cryptography), and Post-quantum cryptography. Secure symmetric algorithms include the commonly used AES (Advanced Encryption Standard) which replaced the older DES (Data Encryption Standard).[16] Insecure symmetric algorithms include children's language tangling schemes such as Pig Latin or other cant, and all historical cryptographic schemes, however seriously intended, prior to the invention of the one-time pad early in the 20th century.

In colloquial use, the term "code" is often used to mean any method of encryption or concealment of meaning. However, in cryptography, code has a more specific meaning: the replacement of a unit of plaintext (i.e., a meaningful word or phrase) with a code word (for example, "wallaby" replaces "attack at dawn"). A cypher, in contrast, is a scheme for changing or substituting an element below such a level (a letter, a syllable, or a pair of letters, etc.) in order to produce a cyphertext.

Cryptanalysis is the term used for the study of methods for obtaining the meaning of encrypted information without access to the key normally required to do so; i.e., it is the study of how to "crack" encryption algorithms or their implementations.

Some use the terms "cryptography" and "cryptology" interchangeably in English,[17] while others (including US military practice generally) use "cryptography" to refer specifically to the use and practice of cryptographic techniques and "cryptology" to refer to the combined study of cryptography and cryptanalysis.[18][19] English is more flexible than several other languages in which "cryptology" (done by cryptologists) is always used in the second sense above. RFC 2828 (https://datatracker.ietf.org/doc/html/rfc 2828) advises that steganography is sometimes included in cryptology.[20]

The study of characteristics of languages that have some application in cryptography or cryptology (e.g. frequency data, letter combinations, universal patterns, etc.) is called cryptolinguistics.

History

Before the modern era, cryptography focused on message confidentiality (i.e., encryption)—conversion of messages from a comprehensible form into an incomprehensible one and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge (namely the key needed for decryption of that message). Encryption attempted to ensure secrecy in communications, such as those of spies, military leaders, and diplomats. In recent decades, the field has expanded beyond confidentiality concerns to include techniques for message integrity checking, sender/receiver identity authentication, digital signatures, interactive proofs and secure computation, among others.

Classic cryptography

The main classical cipher types are transposition ciphers, which rearrange the order of letters in a message (e.g., 'hello world' becomes 'ehlol owrdl' in a trivially simple rearrangement scheme), and substitution ciphers, which systematically replace letters or groups of letters with other letters or groups of letters (e.g., 'fly at once' becomes 'gmz bu podf' by replacing each letter with the one following it in the Latin alphabet).[21] Simple versions of either have never offered much confidentiality from enterprising opponents. An early substitution cipher was the Caesar cipher, in which each letter in the plaintext was replaced by a letter some fixed number of positions further down the alphabet. Suetonius reports that Julius Caesar used it with a shift of three to communicate with his generals. Atbash is an example of an early Hebrew cipher. The earliest known use of cryptography is some carved ciphertext on stone in Egypt (ca 1900 BCE), but this may have been done for the amusement of literate observers rather than as a way of concealing information.

Reconstructed ancient Greek *scytale*, an early cipher device

The Greeks of Classical times are said to have known of ciphers (e.g., the scytale transposition cipher claimed to have been used by the Spartan military).[22] Steganography (i.e., hiding even the existence of a message so as to keep it confidential) was also first developed in ancient times. An early example, from Herodotus, was a message tattooed on a slave's shaved head and concealed under the regrown hair.[14] More modern examples of steganography include the use of invisible ink, microdots, and digital watermarks to conceal information.

In India, the 2000-year-old Kamasutra of Vātsyāyana speaks of two different kinds of ciphers called Kautiliyam and Mulavediya. In the Kautiliyam, the cipher letter substitutions are based on phonetic relations, such as vowels becoming consonants. In the Mulavediya, the cipher alphabet consists of pairing letters and using the reciprocal ones.[14]

In Sassanid Persia, there were two secret scripts, according to the Muslim author Ibn al-Nadim: the *šāh-dabīrīya* (literally "King's script") which was used for official correspondence, and the *rāz-saharīya* which was used to communicate secret messages with other countries.[23]

David Kahn notes in *The Codebreakers* that modern cryptology originated among the Arabs, the first people to systematically document cryptanalytic methods.[24] 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.[25]
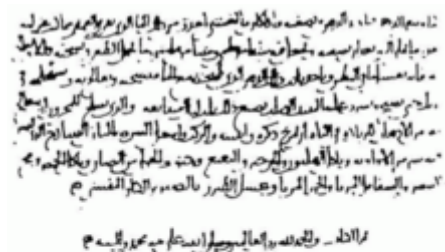
Ciphertexts produced by a classical cipher (and some modern ciphers) will reveal statistical information about the plaintext, and that information can often be used to break the cipher. After the discovery of frequency analysis, perhaps by the Arab mathematician and polymath Al-Kindi (also known as *Alkindus*) in the 9th century,[26] nearly all such ciphers could be broken by an informed attacker. Such classical ciphers still enjoy popularity today, though mostly as puzzles (see cryptogram). Al-Kindi wrote a book on cryptography entitled *Risalah fi Istikhraj al-Mu'amma* (*Manuscript for the Deciphering Cryptographic Messages*), which described the first known use of frequency analysis cryptanalysis techniques.[26][27]

Language letter frequencies may offer little help for some extended historical encryption techniques such as homophonic cipher that tend to flatten the frequency distribution. For those ciphers, language letter group (or n-gram) frequencies may provide an attack.

Essentially all ciphers remained vulnerable to cryptanalysis using the frequency analysis technique until the development of the polyalphabetic cipher, most clearly by Leon Battista Alberti around the year 1467, though there is some indication that it was already known to Al-Kindi.[27] Alberti's innovation was to use different ciphers (i.e., substitution alphabets) for various parts of a message (perhaps for each successive plaintext letter at the limit). He also invented what was probably the first automatic cipher device, a wheel which implemented a partial realization of his invention. In the Vigenère cipher, a polyalphabetic cipher, encryption uses a *key word*, which controls letter substitution depending on which letter of the key word is used. In the mid-19th century Charles Babbage showed that the Vigenère cipher was vulnerable to Kasiski examination, but this was first published about ten years later by Friedrich Kasiski.[28]

First page of a book by Al-Kindi which discusses encryption of messages

Although frequency analysis can be a powerful and general technique against many ciphers, encryption has still often been effective in practice, as many a would-be cryptanalyst was unaware of the technique. Breaking a message without using frequency analysis essentially required knowledge of the cipher used and perhaps of the key involved, thus making espionage, bribery, burglary, defection, etc., more attractive approaches to the cryptanalytically uninformed. It was finally explicitly recognized in the 19th century that secrecy of a cipher's algorithm is not a sensible nor practical safeguard of message security; in fact, it was further realized that any adequate cryptographic scheme (including ciphers) should remain secure even if the adversary fully understands the cipher algorithm itself. Security of the key used should alone be sufficient for a good cipher to maintain confidentiality under an attack. This fundamental principle was first explicitly stated in 1883 by Auguste Kerckhoffs and is generally called Kerckhoffs's Principle; alternatively and more bluntly, it was restated by Claude Shannon, the inventor of information theory and the fundamentals of theoretical cryptography, as *Shannon's Maxim* —'the enemy knows the system'.

16th-century book-shaped French cipher machine, with arms of Henri II of France

Different physical devices and aids have been used to assist with ciphers. One of the earliest may have been the scytale of ancient Greece, a rod supposedly used by the Spartans as an aid for a transposition cipher. In medieval times, other aids were invented such as the cipher grille, which was also used for a kind of steganography. With the invention of polyalphabetic ciphers came more sophisticated aids such as Alberti's own cipher disk, Johannes Trithemius' tabula recta scheme, and Thomas Jefferson's wheel cypher (not publicly known, and reinvented independently by Bazeries around 1900). Many mechanical encryption/decryption devices were invented early in the 20th century, and several patented, among them rotor machines—famously including the Enigma machine used by the German government and military from the late 1920s and during World War II.[29] The ciphers implemented by better quality examples of these machine designs brought about a substantial increase in cryptanalytic difficulty after WWI.[30]

Enciphered letter from Gabriel de Luetz d'Aramon, French Ambassador to the Ottoman Empire, after 1546, with partial decipherment

Early computer-era cryptography

Cryptanalysis of the new mechanical ciphering devices proved to be both difficult and laborious. In the United Kingdom, cryptanalytic efforts at Bletchley Park during WWII spurred the development of more efficient means for carrying out repetitious tasks, such as military code breaking (decryption). This culminated in the development of the Colossus, the world's first fully electronic, digital, programmable computer, which assisted in the decryption of ciphers generated by the German Army's Lorenz SZ40/42 machine.

Extensive open academic research into cryptography is relatively recent, beginning in the mid-1970s. In the early 1970s IBM personnel designed the Data Encryption Standard (DES) algorithm that became the first federal government cryptography standard in the United States.[31] In 1976 Whitfield Diffie and Martin Hellman published the Diffie–Hellman key exchange algorithm.[32] In 1977 the RSA algorithm was published in Martin Gardner's *Scientific American* column.[33] Since then, cryptography has become a widely used tool in communications, computer networks, and computer security generally.

Some modern cryptographic techniques can only keep their keys secret if certain mathematical problems are intractable, such as the integer factorization or the discrete logarithm problems, so there are deep connections with abstract mathematics. There are very few cryptosystems that are proven to be unconditionally secure. The one-time pad is one, and was proven to be so by Claude Shannon. There are a few important algorithms that have been proven secure under certain assumptions. For example, the infeasibility of factoring extremely large integers is the basis for believing that RSA is secure, and some other systems, but even so, proof of unbreakability is unavailable since the underlying mathematical problem remains open. In practice, these are widely used, and are believed unbreakable in practice by most competent observers. There are systems similar to RSA, such as one by Michael O. Rabin that are provably secure provided factoring $n = pq$ is impossible; it is quite unusable in practice. The discrete logarithm problem is the basis for believing some other cryptosystems are secure, and again, there are related, less practical systems that are provably secure relative to the solvability or insolvability discrete log problem.[34]

As well as being aware of cryptographic history, cryptographic algorithm and system designers must also sensibly consider probable future developments while working on their designs. For instance, continuous improvements in computer processing power have increased the scope of brute-force attacks, so when specifying key lengths, the required key lengths are similarly advancing.[35] The potential impact of quantum computing are already being considered by some cryptographic system designers developing post-quantum cryptography. The announced imminence of small implementations of these machines may be making the need for preemptive caution rather more than merely speculative.[6]

Modern cryptography

Prior to the early 20th century, cryptography was mainly concerned with linguistic and lexicographic patterns. Since then cryptography has broadened in scope, and now makes extensive use of mathematical subdisciplines, including information theory, computational complexity, statistics, combinatorics, abstract algebra, number theory, and finite mathematics.[36] Cryptography is also a branch of engineering, but an unusual one since it deals with active, intelligent, and malevolent opposition; other kinds of engineering (e.g., civil or chemical engineering) need deal only with neutral natural forces. There is also active research examining the relationship between cryptographic problems and quantum physics.

Just as the development of digital computers and electronics helped in cryptanalysis, it made possible much more complex ciphers. Furthermore, computers allowed for the encryption of any kind of data representable in any binary format, unlike classical ciphers which only encrypted written language texts; this was new and significant. Computer use has thus supplanted linguistic cryptography, both for cipher

design and cryptanalysis. Many computer ciphers can be characterized by their operation on binary bit sequences (sometimes in groups or blocks), unlike classical and mechanical schemes, which generally manipulate traditional characters (i.e., letters and digits) directly. However, computers have also assisted cryptanalysis, which has compensated to some extent for increased cipher complexity. Nonetheless, good modern ciphers have stayed ahead of cryptanalysis; it is typically the case that use of a quality cipher is very efficient (i.e., fast and requiring few resources, such as memory or CPU capability), while breaking it requires an effort many orders of magnitude larger, and vastly larger than that required for any classical cipher, making cryptanalysis so inefficient and impractical as to be effectively impossible.
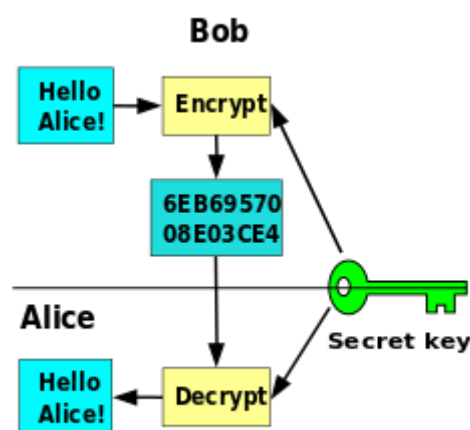
Modern cryptography

Symmetric-key cryptography

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976.[32]

Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A block cipher enciphers input in blocks of plaintext as opposed to individual characters, the input form used by a stream cipher.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs that have been designated cryptography standards by the US government (though DES's designation was finally withdrawn after the AES was adopted).[37] Despite its deprecation as an official standard, DES (especially its still-approved and much more secure triple-DES variant) remains quite popular; it is used across a wide range of applications, from ATM encryption[38] to e-mail privacy[39] and secure remote access.[40] Many other block ciphers have been designed and released, with considerable variation in quality. Many, even some designed by capable practitioners, have been thoroughly broken, such as FEAL.[6][41]

Stream ciphers, in contrast to the 'block' type, create an arbitrarily long stream of key material, which is combined with the plaintext bit-by-bit or character-by-character, somewhat like the one-time pad. In a stream cipher, the output stream is created based on a hidden internal state that changes as the cipher operates. That internal state is initially set up using the secret key material. RC4 is a widely used stream cipher.[6] Block ciphers can be used as stream ciphers by generating blocks of a keystream (in place of a Pseudorandom number generator) and applying an XOR operation to each bit of the plaintext with each bit of the keystream.[42]

Symmetric-key cryptography, where a single key is used for encryption and decryption
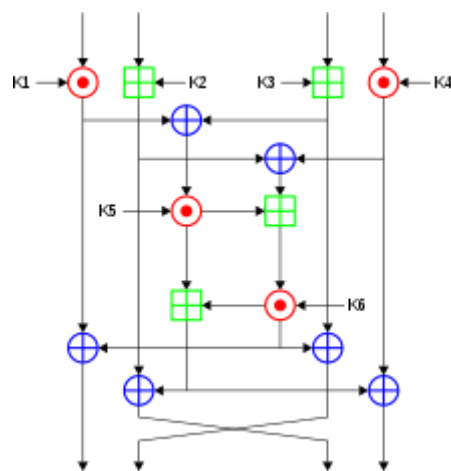
One round (out of 8.5) of the IDEA cipher, used in most versions of PGP and OpenPGP compatible software for time-efficient encryption of messages
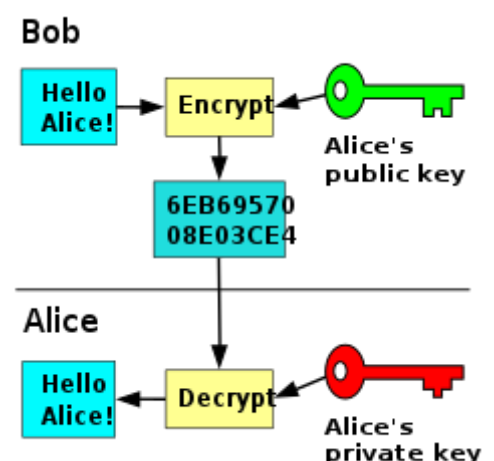
Message authentication codes (MACs) are much like cryptographic hash functions, except that a secret key can be used to authenticate the hash value upon receipt;[6][43] this additional complication blocks an attack scheme against bare digest algorithms, and so has been thought worth the effort. Cryptographic hash functions are a third type of cryptographic algorithm. They take a message of any length as input, and output a short, fixed-length hash, which can be used in (for example) a digital signature. For good hash functions, an attacker cannot find two messages that produce the same hash. MD4 is a long-used hash function that is now broken; MD5, a strengthened variant of MD4, is also widely used but broken in practice. The US National Security Agency developed the Secure Hash Algorithm series of MD5-like hash functions: SHA-0 was a flawed algorithm that the agency withdrew; SHA-1 is widely deployed and more secure than MD5, but cryptanalysts have identified attacks against it; the SHA-2 family improves on SHA-1, but is vulnerable to clashes as of 2011; and the US standards authority thought it "prudent" from a security perspective to develop a new standard to "significantly improve the robustness of NIST's overall hash algorithm toolkit."[44] Thus, a hash function design competition was meant to select a new U.S. national standard, to be called SHA-3, by 2012. The competition ended on October 2, 2012, when the NIST announced that Keccak would be the new SHA-3 hash algorithm.[45] Unlike block and stream ciphers that are invertible, cryptographic hash functions produce a hashed output that cannot be used to retrieve the original input data. Cryptographic hash functions are used to verify the authenticity of data retrieved from an untrusted source or to add a layer of security.

Public-key cryptography

Symmetric-key cryptosystems use the same key for encryption and decryption of a message, although a message or group of messages can have a different key than others. A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating parties must, ideally, share a different key, and perhaps for each ciphertext exchanged as well. The number of keys required increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all consistent and secret.

Public-key cryptography, where different keys are used for encryption and decryption.

Whitfield Diffie and Martin Hellman, authors of the first published paper on public-key cryptography.

In a groundbreaking 1976 paper, Whitfield Diffie and Martin Hellman proposed the notion of *public-key* (also, more generally, called *asymmetric key*) cryptography in which two different but mathematically related keys are used—a *public* key and a *private* key.[46] A public key system is so constructed that calculation of one key (the 'private key') is computationally infeasible from the other (the 'public key'), even though they are necessarily related. Instead, both keys are generated secretly, as an interrelated pair.[47] The historian David Kahn described public-key cryptography as "the most revolutionary new concept in the field since polyalphabetic substitution emerged in the Renaissance".[48]

In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. In a public-key encryption system, the *public key* is used for encryption, while the *private* or *secret key* is used for decryption. While Diffie and Hellman could not find such a system, they showed that

public-key cryptography was indeed possible by presenting the Diffie–Hellman key exchange protocol, a solution that is now widely used in secure communications to allow two parties to secretly agree on a shared encryption key.[32] The X.509 standard defines the most commonly used format for public key certificates.[49]
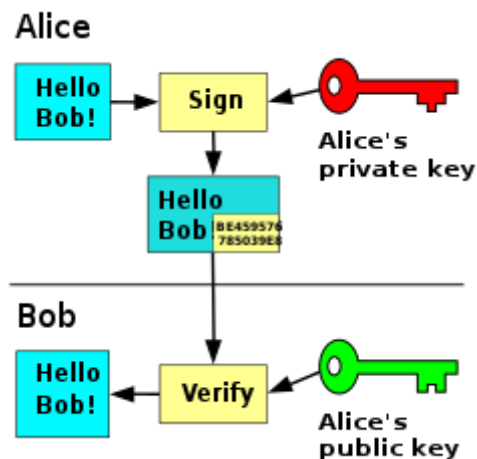
Diffie and Hellman's publication sparked widespread academic efforts in finding a practical public-key encryption system. This race was finally won in 1978 by Ronald Rivest, Adi Shamir, and Len Adleman, whose solution has since become known as the RSA algorithm.[50]

The Diffie–Hellman and RSA algorithms, in addition to being the first publicly known examples of high-quality public-key algorithms, have been among the most widely used. Other asymmetric-key algorithms include the Cramer–Shoup cryptosystem, ElGamal encryption, and various elliptic curve techniques.

A document published in 1997 by the Government Communications Headquarters (GCHQ), a British intelligence organization, revealed that cryptographers at GCHQ had anticipated several academic developments.[51] Reportedly, around 1970, James H. Ellis had conceived the principles of asymmetric key cryptography. In 1973, Clifford Cocks invented a solution that was very similar in design rationale to RSA.[51][52] In 1974, Malcolm J. Williamson is claimed to have developed the Diffie–Hellman key exchange.[53]

Public-key cryptography is also used for implementing digital signature schemes. A digital signature is reminiscent of an ordinary signature; they both have the characteristic of being easy for a user to produce, but difficult for anyone else to forge. Digital signatures can also be permanently tied to the content of the message being signed; they cannot then be 'moved' from one document to another, for any attempt will be detectable. In digital signature schemes, there are two algorithms: one for *signing*, in which a secret key is used to process the message (or a hash of the message, or both), and one for *verification*, in which the matching public key is used with the message to check the validity of the signature. RSA and DSA are two of the most popular digital signature schemes. Digital signatures are central to the operation of public key infrastructures and many network security schemes (e.g., SSL/TLS, many VPNs, etc.).[41]

In this example the message is only signed and not encrypted. 1) Alice signs a message with her private key. 2) Bob can verify that Alice sent the message and that the message has not been modified.

Public-key algorithms are most often based on the computational complexity of "hard" problems, often from number theory. For example, the hardness of RSA is related to the integer factorization problem, while Diffie–Hellman and DSA are related to the discrete logarithm problem. The security of elliptic curve cryptography is based on number theoretic problems involving elliptic curves. Because of the difficulty of the underlying problems, most public-key algorithms involve operations such as modular multiplication and exponentiation, which are much more computationally expensive than the techniques used in most block ciphers, especially with typical key sizes. As a result, public-key cryptosystems are commonly hybrid cryptosystems, in which a fast high-quality symmetric-key encryption algorithm is used for the message itself, while the relevant symmetric key is sent with the message, but encrypted using a public-key algorithm. Similarly, hybrid signature schemes are often used, in which a cryptographic hash function is computed, and only the resulting hash is digitally signed.[6]

Cryptographic Hash Functions

Cryptographic Hash Functions are cryptographic algorithms that are ways to generate and utilize specific keys to encrypt data for either symmetric or asymmetric encryption, and such functions may be viewed as keys themselves. They take a message of any length as input, and output a short, fixed-length hash, which can be used in (for example) a digital signature. For good hash functions, an attacker cannot find two messages that produce the same hash. MD4 is a long-used hash function that is now broken; MD5, a strengthened variant of MD4, is also widely used but broken in practice. The US National Security Agency developed the Secure Hash Algorithm series of MD5-like hash functions: SHA-0 was a flawed algorithm that the agency withdrew; SHA-1 is widely deployed and more secure than MD5, but cryptanalysts have identified attacks against it; the SHA-2 family improves on SHA-1, but is vulnerable to clashes as of 2011; and the US standards authority thought it "prudent" from a security perspective to develop a new standard to "significantly improve the robustness of NIST's overall hash algorithm toolkit."[44] Thus, a hash function design competition was meant to select a new U.S. national standard, to be called SHA-3, by 2012. The competition ended on October 2, 2012, when the NIST announced that Keccak would be the new SHA-3 hash algorithm.[45] Unlike block and stream ciphers that are invertible, cryptographic hash functions produce a hashed output that cannot be used to retrieve the original input data. Cryptographic hash functions are used to verify the authenticity of data retrieved from an untrusted source or to add a layer of security.

Cryptanalysis

Variants of the Enigma machine, used by Germany's military and civil authorities from the late 1920s through World War II, implemented a complex electro-mechanical polyalphabetic cipher. Breaking and reading of the Enigma cipher at Poland's Cipher Bureau, for 7 years before the war, and subsequent decryption at Bletchley Park, was important to Allied victory.[14]

The goal of cryptanalysis is to find some weakness or insecurity in a cryptographic scheme, thus permitting its subversion or evasion.

It is a common misconception that every encryption method can be broken. In connection with his WWII work at Bell Labs, Claude Shannon proved that the one-time pad cipher is unbreakable, provided the key material is truly random, never reused, kept secret from all possible attackers, and of equal or greater length than the message.[54] Most ciphers, apart from the one-time pad, can be broken with enough computational effort by brute force attack, but the amount of effort needed may be exponentially dependent on the key size, as compared to the effort needed to make use of the cipher. In such cases, effective security could be achieved if it is proven that the effort required (i.e., "work factor", in Shannon's terms) is beyond the ability of any adversary. This means it must be shown that no efficient method (as opposed to the time-consuming brute force method) can be found to break the cipher. Since no such proof has been found to date, the one-time-pad remains the only theoretically unbreakable cipher. Although well-implemented one-time-pad encryption cannot be broken, traffic analysis is still possible.

There are a wide variety of cryptanalytic attacks, and they can be classified in any of several ways. A common distinction turns on what Eve (an attacker) knows and what capabilities are available. In a ciphertext-only attack, Eve has access only to the ciphertext (good modern cryptosystems are usually effectively immune to ciphertext-only attacks). In a known-plaintext attack, Eve has access to a ciphertext and its corresponding plaintext (or to many such pairs). In a chosen-plaintext attack, Eve may choose a plaintext and learn its corresponding ciphertext (perhaps many times); an example is gardening, used by the British during WWII. In a chosen-ciphertext attack, Eve may be able to *choose*

ciphertexts and learn their corresponding plaintexts.[6] Finally in a man-in-the-middle attack Eve gets in between Alice (the sender) and Bob (the recipient), accesses and modifies the traffic and then forwards it to the recipient.[55] Also important, often overwhelmingly so, are mistakes (generally in the design or use of one of the protocols involved).

Cryptanalysis of symmetric-key ciphers typically involves looking for attacks against the block ciphers or stream ciphers that are more efficient than any attack that could be against a perfect cipher. For example, a simple brute force attack against DES requires one known plaintext and 2^{55} decryptions, trying approximately half of the possible keys, to reach a point at which chances are better than even that the key sought will have been found. But this may not be enough assurance; a linear cryptanalysis attack against DES requires 2^{43} known plaintexts (with their corresponding ciphertexts) and approximately 2^{43} DES operations.[56] This is a considerable improvement over brute force attacks.

Poznań monument (*center*) to Polish cryptanalysts whose breaking of Germany's Enigma machine ciphers, beginning in 1932, altered the course of World War II

Public-key algorithms are based on the computational difficulty of various problems. The most famous of these are the difficulty of integer factorization of semiprimes and the difficulty of calculating discrete logarithms, both of which are not yet proven to be solvable in polynomial time (**P**) using only a classical Turing-complete computer. Much public-key cryptanalysis concerns designing algorithms in **P** that can solve these problems, or using other technologies, such as quantum computers. For instance, the best-known algorithms for solving the elliptic curve-based version of discrete logarithm are much more time-consuming than the best-known algorithms for factoring, at least for problems of more or less equivalent size. Thus, to achieve an equivalent strength of encryption, techniques that depend upon the difficulty of factoring large composite numbers, such as the RSA cryptosystem, require larger keys than elliptic curve techniques. For this reason, public-key cryptosystems based on elliptic curves have become popular since their invention in the mid-1990s.

While pure cryptanalysis uses weaknesses in the algorithms themselves, other attacks on cryptosystems are based on actual use of the algorithms in real devices, and are called *side-channel attacks*. If a cryptanalyst has access to, for example, the amount of time the device took to encrypt a number of plaintexts or report an error in a password or PIN character, he may be able to use a timing attack to break a cipher that is otherwise resistant to analysis. An attacker might also study the pattern and length of messages to derive valuable information; this is known as traffic analysis[57] and can be quite useful to an alert adversary. Poor administration of a cryptosystem, such as permitting too short keys, will make any system vulnerable, regardless of other virtues. Social engineering and other attacks against humans (e.g., bribery, extortion, blackmail, espionage, torture, ...) are usually employed due to being more cost-effective and feasible to perform in a reasonable amount of time compared to pure cryptanalysis by a high margin.

Cryptographic primitives

Much of the theoretical work in cryptography concerns cryptographic *primitives*—algorithms with basic cryptographic properties—and their relationship to other cryptographic problems. More complicated cryptographic tools are then built from these basic primitives. These primitives provide fundamental properties, which are used to develop more complex tools called *cryptosystems* or *cryptographic protocols*, which guarantee one or more high-level security properties. Note, however, that the distinction between cryptographic *primitives* and cryptosystems, is quite arbitrary; for example, the RSA algorithm is sometimes considered a cryptosystem, and sometimes a primitive. Typical examples of cryptographic primitives include pseudorandom functions, one-way functions, etc.

Cryptosystems

One or more cryptographic primitives are often used to develop a more complex algorithm, called a cryptographic system, or *cryptosystem*. Cryptosystems (e.g., El-Gamal encryption) are designed to provide particular functionality (e.g., public key encryption) while guaranteeing certain security properties (e.g., chosen-plaintext attack (CPA) security in the random oracle model). Cryptosystems use the properties of the underlying cryptographic primitives to support the system's security properties. As the distinction between primitives and cryptosystems is somewhat arbitrary, a sophisticated cryptosystem can be derived from a combination of several more primitive cryptosystems. In many cases, the cryptosystem's structure involves back and forth communication among two or more parties in space (e.g., between the sender of a secure message and its receiver) or across time (e.g., cryptographically protected backup data). Such cryptosystems are sometimes called *cryptographic protocols*.

Some widely known cryptosystems include RSA, Schnorr signature, ElGamal encryption, and Pretty Good Privacy (PGP). More complex cryptosystems include electronic cash[58] systems, signcryption systems, etc. Some more 'theoretical' cryptosystems include interactive proof systems,[59] (like zero-knowledge proofs),[60] systems for secret sharing,[61][62] etc.

Lightweight cryptography

Lightweight cryptography (LWC) concerns cryptographic algorithms developed for a strictly constrained environment. The growth of Internet of Things (IoT) has spiked research into the development of lightweight algorithms that are better suited for the environment. An IoT environment requires strict constraints on power consumption, processing power, and security.[63] Algorithms such as PRESENT, AES, and SPECK are examples of the many LWC algorithms that have been developed to achieve the standard set by the National Institute of Standards and Technology.[64]

Applications

General

Cryptography is widely used on the internet to help protect user-data and prevent eavesdropping. To ensure secrecy during transmission, many systems use private key cryptography to protect transmitted information. With public-key systems, one can maintain secrecy without a master key or a large number of keys.[65] But, some algorithms like Bitlocker and Veracrypt are generally not private-public key cryptography. Such as Veracrypt, it uses a password hash to generate the single private key. However, it can be configured to run in public-private key systems. The C++ opensource encryption library OpenSSL provides free and opensource encryption software and tools. The most commonly used encryption cipher suit is AES,[66] as it has hardware acceleration for all x86 based processors that has AES-NI. A close contender is ChaCha20-Poly1305, which is a stream cipher, however it is commonly used for mobile devices as they are ARM based which does not feature AES-NI instruction set extension.

Cybersecurity

Cryptography can be used to secure communications by encrypting them. Websites use encryption via HTTPS.[67] "End-to-end" encryption, where only sender and receiver can read messages, is implemented for email in Pretty Good Privacy and for secure messaging in general in WhatsApp, Signal and Telegram.[67]

Operating systems use encryption to keep passwords secret, conceal parts of the system, and ensure that software updates are truly from the system maker.[67] Instead of storing plaintext passwords, computer systems store hashes thereof; then, when a user logs in, the system passes the given password through a cryptographic hash function and compares it to the hashed value on file. In this manner, neither the system nor an attacker has at any point access to the password in plaintext.[67]

Encryption is sometimes used to encrypt one's entire drive. For example, University College London has implemented BitLocker (a program by Microsoft) to render drive data opaque without users logging in.[67]

Cryptocurrencies and cryptoeconomics

Cryptographic techniques enable cryptocurrency technologies, such as distributed ledger technologies (e.g., blockchains), which finance cryptoeconomics applications such as decentralized finance (DeFi).[68][69] Key cryptographic techniques that enable cryptocurrencies and cryptoeconomics include, but are not limited to: cryptographic keys, cryptographic hash functions, asymmetric (public key) encryption, Multi-Factor Authentication (MFA), End-to-End Encryption (E2EE), and Zero Knowledge Proofs (ZKP).[69]

Legal issues

Prohibitions

Cryptography has long been of interest to intelligence gathering and law enforcement agencies.[10] Secret communications may be criminal or even treasonous. Because of its facilitation of privacy, and the diminution of privacy attendant on its prohibition, cryptography is also of considerable interest to civil rights supporters. Accordingly, there has been a history of controversial legal issues surrounding cryptography, especially since the advent of inexpensive computers has made widespread access to high-quality cryptography possible.

In some countries, even the domestic use of cryptography is, or has been, restricted. Until 1999, France significantly restricted the use of cryptography domestically, though it has since relaxed many of these rules. In China and Iran, a license is still required to use cryptography.[8] Many countries have tight restrictions on the use of cryptography. Among the more restrictive are laws in Belarus, Kazakhstan, Mongolia, Pakistan, Singapore, Tunisia, and Vietnam.[70]

In the United States, cryptography is legal for domestic use, but there has been much conflict over legal issues related to cryptography.[10] One particularly important issue has been the export of cryptography and cryptographic software and hardware. Probably because of the importance of cryptanalysis in World War II and an expectation that cryptography would continue to be important for national security, many Western governments have, at some point, strictly regulated export of cryptography. After World War II, it was illegal in the US to sell or distribute encryption technology overseas; in fact, encryption was designated as auxiliary military equipment and put on the United States Munitions List.[71] Until the development of the personal computer, asymmetric key algorithms (i.e., public key techniques), and the Internet, this was not especially problematic. However, as the Internet grew and computers became more widely available, high-quality encryption techniques became well known around the globe.

Export controls

In the 1990s, there were several challenges to US export regulation of cryptography. After the source code for Philip Zimmermann's Pretty Good Privacy (PGP) encryption program found its way onto the Internet in June 1991, a complaint by RSA Security (then called RSA Data Security, Inc.) resulted in a lengthy criminal investigation of Zimmermann by the US Customs Service and the FBI, though no charges were ever filed.[72][73] Daniel J. Bernstein, then a graduate student at UC Berkeley, brought a lawsuit against the US government challenging some aspects of the restrictions based on free speech grounds. The 1995 case *Bernstein v. United States* ultimately resulted in a 1999 decision that printed source code for cryptographic algorithms and systems was protected as free speech by the United States Constitution.[74]

In 1996, thirty-nine countries signed the Wassenaar Arrangement, an arms control treaty that deals with the export of arms and "dual-use" technologies such as cryptography. The treaty stipulated that the use of cryptography with short key-lengths (56-bit for symmetric encryption, 512-bit for RSA) would no longer be export-controlled.[75] Cryptography exports from the US became less strictly regulated as a consequence of a major relaxation in 2000;[76] there are no longer very many restrictions on key sizes in US-exported mass-market software. Since this relaxation in US export restrictions, and because most personal computers connected to the Internet include US-sourced web browsers such as Firefox or Internet Explorer, almost every Internet user worldwide has potential access to quality cryptography via their browsers (e.g., via Transport Layer Security). The Mozilla Thunderbird and Microsoft Outlook E-mail client programs similarly can transmit and receive emails via TLS, and can send and receive email encrypted with S/MIME. Many Internet users don't realize that their basic application software contains such extensive cryptosystems. These browsers and email programs are so ubiquitous that even governments whose intent is to regulate civilian use of cryptography generally don't find it practical to do much to control distribution or use of cryptography of this quality, so even when such laws are in force, actual enforcement is often effectively impossible.

NSA involvement

Another contentious issue connected to cryptography in the United States is the influence of the National Security Agency on cipher development and policy.[10] The NSA was involved with the design of DES during its development at IBM and its consideration by the National Bureau of Standards as a possible Federal Standard for cryptography.[77] DES was designed to be resistant to differential cryptanalysis,[78] a powerful and general cryptanalytic technique known to the NSA and IBM, that became publicly known only when it was rediscovered in the late 1980s.[79] According to Steven Levy, IBM discovered differential cryptanalysis,[73] but kept the technique secret at the NSA's request. The technique became publicly known only when Biham

NSA headquarters in Fort Meade, Maryland

and Shamir re-discovered and announced it some years later. The entire affair illustrates the difficulty of determining what resources and knowledge an attacker might actually have.

Another instance of the NSA's involvement was the 1993 Clipper chip affair, an encryption microchip intended to be part of the Capstone cryptography-control initiative. Clipper was widely criticized by cryptographers for two reasons. The cipher algorithm (called Skipjack) was then classified (declassified in 1998, long after the Clipper initiative lapsed). The classified cipher caused concerns that the NSA had deliberately made the cipher weak in order to assist its intelligence efforts. The whole initiative was also criticized based on its violation of Kerckhoffs's Principle, as the scheme included a special escrow key held by the government for use by law enforcement (i.e. wiretapping).[73]

Digital rights management

Cryptography is central to digital rights management (DRM), a group of techniques for technologically controlling use of copyrighted material, being widely implemented and deployed at the behest of some copyright holders. In 1998, U.S. President Bill Clinton signed the Digital Millennium Copyright Act (DMCA), which criminalized all production, dissemination, and use of certain cryptanalytic techniques and technology (now known or later discovered); specifically, those that could be used to circumvent DRM technological schemes.[80] This had a noticeable impact on the cryptography research community since an argument can be made that any cryptanalytic research violated the DMCA. Similar statutes have since been enacted in several countries and regions, including the implementation in the EU Copyright Directive. Similar restrictions are called for by treaties signed by World Intellectual Property Organization member-states.

The United States Department of Justice and FBI have not enforced the DMCA as rigorously as had been feared by some, but the law, nonetheless, remains a controversial one. Niels Ferguson, a well-respected cryptography researcher, has publicly stated that he will not release some of his research into an Intel security design for fear of prosecution under the DMCA.[81] Cryptologist Bruce Schneier has argued that the DMCA encourages vendor lock-in, while inhibiting actual measures toward cyber-security.[82] Both Alan Cox (longtime Linux kernel developer) and Edward Felten (and some of his students at Princeton) have encountered problems related to the Act. Dmitry Sklyarov was arrested during a visit to the US from Russia, and jailed for five months pending trial for alleged violations of the DMCA arising from work he had done in Russia, where the work was legal. In 2007, the cryptographic keys responsible for Blu-ray and HD DVD content scrambling were discovered and released onto the Internet. In both cases, the Motion Picture Association of America sent out numerous DMCA takedown notices, and there was a massive Internet backlash[11] triggered by the perceived impact of such notices on fair use and free speech.

Forced disclosure of encryption keys

In the United Kingdom, the Regulation of Investigatory Powers Act gives UK police the powers to force suspects to decrypt files or hand over passwords that protect encryption keys. Failure to comply is an offense in its own right, punishable on conviction by a two-year jail sentence or up to five years in cases involving national security.[9] Successful prosecutions have occurred under the Act; the first, in 2009,[83] resulted in a term of 13 months' imprisonment.[84] Similar forced disclosure laws in Australia, Finland, France, and India compel individual suspects under investigation to hand over encryption keys or passwords during a criminal investigation.

In the United States, the federal criminal case of *United States v. Fricosu* addressed whether a search warrant can compel a person to reveal an encryption passphrase or password.[85] The Electronic Frontier Foundation (EFF) argued that this is a violation of the protection from self-incrimination given by the Fifth Amendment.[86] In 2012, the court ruled that under the All Writs Act, the defendant was required to produce an unencrypted hard drive for the court.[87]

In many jurisdictions, the legal status of forced disclosure remains unclear.

The 2016 FBI–Apple encryption dispute concerns the ability of courts in the United States to compel manufacturers' assistance in unlocking cell phones whose contents are cryptographically protected.

As a potential counter-measure to forced disclosure some cryptographic software supports plausible deniability, where the encrypted data is indistinguishable from unused random data (for example such as that of a drive which has been securely wiped).

See also

- Collision attack
- Comparison of cryptography libraries
- Crypto Wars – Attempts to limit access to strong cryptography
- Encyclopedia of Cryptography and Security – Book by Technische Universiteit Eindhoven
- Global surveillance – Mass surveillance across national borders
- Indistinguishability obfuscation – Type of cryptographic software obfuscation
- Information theory – Scientific study of digital information
- Outline of cryptography – Overview of and topical guide to cryptography

    - List of cryptographers
    - List of important publications in cryptography
    - List of multiple discoveries
    - List of unsolved problems in computer science
- Secure cryptoprocessor
- Strong cryptography – Term applied to cryptographic systems that are highly resistant to cryptanalysis
- Syllabical and Steganographical Table – Eighteenth-century work believed to be the first cryptography chart – first cryptography chart
- World Wide Web Consortium's Web Cryptography API – World Wide Web Consortium cryptography standard

References

1. Liddell, Henry George; Scott, Robert; Jones, Henry Stuart; McKenzie, Roderick (1984). *A Greek-English Lexicon*. Oxford University Press.
2. Rivest, Ronald L. (1990). "Cryptography". In J. Van Leeuwen (ed.). *Handbook of Theoretical Computer Science*. Vol. 1. Elsevier.
3. Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". *Introduction to Modern Cryptography*. p. 10.
4. Sadkhan, Sattar B. (December 2013). "Key note lecture multidisciplinary in cryptology and information security" (https://ieeexplore.ieee.org/abstract/document/6998773). *2013 International Conference on Electrical Communication, Computer, Power, and Control Engineering (ICECCPCE)*: 1–2. doi:10.1109/ICECCPCE.2013.6998773 (https://doi.org/10.1109%2FICECCPCE.2013.6998773).
5. "Crypto FAQ: What is cryptography & how does it work?" (https://cryptographyworks.com/faq/what-is-cryptography.html). *Cryptography Works™*. Retrieved 27 August 2022.
6. Menezes, A.J.; van Oorschot, P.C.; Vanstone, S.A. (1997). *Handbook of Applied Cryptography* (https://archive.org/details/handbookofapplie0000mene). ISBN 978-0-8493-8523-0.
7. Biggs, Norman (2008). *Codes: An introduction to Information Communication and Cryptography* (https://archive.org/details/codesintroductio00bigg_911). Springer. p. 171 (https://archive.org/details/codesintroductio00bigg_911/page/n176).
8. "Overview per country" (http://www.cryptolaw.org/cls2.htm). *Crypto Law Survey*. February 2013. Retrieved 26 March 2015.

9. "UK Data Encryption Disclosure Law Takes Effect" (https://web.archive.org/web/201201201 35135/http://www.pcworld.com/article/137881/uk_data_encryption_disclosure_law_takes_ef fect.html). *PC World*. 1 October 2007. Archived from the original (http://www.pcworld.com/arti cle/137881/uk_data_encryption_disclosure_law_takes_effect.html) on 20 January 2012. Retrieved 26 March 2015.

10. Ranger, Steve (24 March 2015). "The undercover war on your internet secrets: How online surveillance cracked our trust in the web" (https://web.archive.org/web/20160612190952/htt p://www.techrepublic.com/article/the-undercover-war-on-your-internet-secrets-how-online-su rveillance-cracked-our-trust-in-the-web/). TechRepublic. Archived from the original (https://w ww.techrepublic.com/article/the-undercover-war-on-your-internet-secrets-how-online-surveill ance-cracked-our-trust-in-the-web/) on 12 June 2016. Retrieved 12 June 2016.

11. Doctorow, Cory (2 May 2007). "Digg users revolt over AACS key" (https://boingboing.net/200 7/05/02/digg-users-revolt-ov.html). *Boing Boing*. Retrieved 26 March 2015.

12. Whalen, Terence (1994). "The Code for Gold: Edgar Allan Poe and Cryptography". *Representations*. University of California Press. **46** (46): 35–57. doi:10.2307/2928778 (http s://doi.org/10.2307%2F2928778). JSTOR 2928778 (https://www.jstor.org/stable/2928778).

13. Rosenheim 1997, p. 20

14. Kahn, David (1967). *The Codebreakers*. ISBN 978-0-684-83130-5.

15. "An Introduction to Modern Cryptosystems" (https://www.giac.org/paper/gsec/2604/introducti on-modern-cryptosystems/104482).

16. Sharbaf, M.S. (1 November 2011). "Quantum cryptography: An emerging technology in network security". *2011 IEEE International Conference on Technologies for Homeland Security (HST)*: 13–19. doi:10.1109/THS.2011.6107841 (https://doi.org/10.1109%2FTHS.20 11.6107841). ISBN 978-1-4577-1376-7. S2CID 17915038 (https://api.semanticscholar.org/C orpusID:17915038).

17. "cryptology | Britannica" (https://www.britannica.com/topic/cryptology). *www.britannica.com*. Retrieved 22 June 2022.

18. Oded Goldreich, *Foundations of Cryptography, Volume 1: Basic Tools*, Cambridge University Press, 2001, ISBN 0-521-79172-3

19. "Cryptology (definition)" (http://www.merriam-webster.com/dictionary/cryptology). *Merriam-Webster's Collegiate Dictionary* (11th ed.). Merriam-Webster. Retrieved 26 March 2015.

20. Shirey, Rob (May 2000). "Internet Security Glossary" (https://tools.ietf.org/html/rfc2828). *Internet Engineering Task Force*. RFC 2828 (https://tools.ietf.org/html/rfc2828). Retrieved 26 March 2015.

21. Saltzman, Benjamin A. (1 October 2018). "Vt hkskdkxt: Early Medieval Cryptography, Textual Errors, and Scribal Agency" (https://www.journals.uchicago.edu/doi/10.1086/69886 1). *Speculum*. **93** (4): 975–1009. doi:10.1086/698861 (https://doi.org/10.1086%2F698861). ISSN 0038-7134 (https://www.worldcat.org/issn/0038-7134). S2CID 165362817 (https://api.s emanticscholar.org/CorpusID:165362817).

22. I͡Ashchenko, V.V. (2002). *Cryptography: an introduction* (https://books.google.com/books?id= cH-NGrpcIMcC&pg=PA6). AMS Bookstore. p. 6. ISBN 978-0-8218-2986-8.

23. electricpulp.com. "CODES – Encyclopaedia Iranica" (http://www.iranicaonline.org/articles/co des-romuz-sg). *www.iranicaonline.org*.

24. Kahn, David (1996). *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* (https://books.google.com/books?id=3S8r hOEmDIIC&q=david+kahn+the+codebreakers). Simon and Schuster. ISBN 9781439103555.

25. 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 (http s://doi.org/10.1198%2Ftas.2011.10191). S2CID 123537702 (https://api.semanticscholar.org/ CorpusID:123537702).

26. Singh, Simon (2000). *The Code Book*. New York: Anchor Books. pp. 14–20. ISBN 978-0-385-49532-5.

27. Al-Kadi, Ibrahim A. (April 1992). "The origins of cryptology: The Arab contributions". *Cryptologia*. **16** (2): 97–126. doi:10.1080/0161-119291866801 (https://doi.org/10.1080%2F0 161-119291866801).

28. Schrödel, Tobias (October 2008). "Breaking Short Vigenère Ciphers". *Cryptologia*. **32** (4): 334–337. doi:10.1080/01611190802336097 (https://doi.org/10.1080%2F016111908023360 97). S2CID 21812933 (https://api.semanticscholar.org/CorpusID:21812933).

29. Hakim, Joy (1995). *A History of US: War, Peace and all that Jazz*. New York: Oxford University Press. ISBN 978-0-19-509514-2.

30. Gannon, James (2001). *Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century* (https://archive.org/details/stealingsecretst00gann). Washington, D.C.: Brassey's. ISBN 978-1-57488-367-1.

31. "The Legacy of DES - Schneier on Security" (https://www.schneier.com/blog/archives/2004/ 10/the_legacy_of_d.html). *www.schneier.com*. Retrieved 26 January 2022.

32. Diffie, Whitfield; Hellman, Martin (November 1976). "New Directions in Cryptography" (http:// www-ee.stanford.edu/~hellman/publications/24.pdf) (PDF). *IEEE Transactions on Information Theory*. IT-22 (6): 644–654. CiteSeerX 10.1.1.37.9720 (https://citeseerx.ist.psu.e du/viewdoc/summary?doi=10.1.1.37.9720). doi:10.1109/tit.1976.1055638 (https://doi.org/10. 1109%2Ftit.1976.1055638).

33. Singh, Simon (1999). *The Code Book: The Science of Secrecy From Ancient Egypt To Quantum Cryptography* (https://archive.org/details/codebook00simo/page/278) (First Anchor Books ed.). New York: Anchor Books. pp. 278 (https://archive.org/details/codebook00simo/p age/278). ISBN 978-0-385-49532-5.

34. *Cryptography: Theory and Practice*, Third Edition (Discrete Mathematics and Its Applications), 2005, by Douglas R. Stinson, Chapman and Hall/CRC

35. Blaze, Matt; Diffie, Whitefield; Rivest, Ronald L.; Schneier, Bruce; Shimomura, Tsutomu; Thompson, Eric; Wiener, Michael (January 1996). "Minimal key lengths for symmetric ciphers to provide adequate commercial security" (http://www.fortify.net/related/cryptographe rs.html). Fortify. Retrieved 26 March 2015.

36. Diffie, W.; Hellman, M. (1 September 2006). "New directions in cryptography" (https://dl.acm. org/doi/10.1109/TIT.1976.1055638). *IEEE Transactions on Information Theory*. **22** (6): 644–654. doi:10.1109/TIT.1976.1055638 (https://doi.org/10.1109%2FTIT.1976.1055638).

37. "FIPS PUB 197: The official Advanced Encryption Standard" (https://web.archive.org/web/2 0150407153905/http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf) (PDF). *Computer Security Resource Center*. National Institute of Standards and Technology. Archived from the original (http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf) (PDF) on 7 April 2015. Retrieved 26 March 2015.

38. "NCUA letter to credit unions" (https://www.ncua.gov/Resources/Documents/LCU2004-09.p df) (PDF). *National Credit Union Administration*. July 2004. Retrieved 26 March 2015.

39. Finney, Hal; Thayer, Rodney L.; Donnerhacke, Lutz; Callas, Jon (November 1998). "Open PGP Message Format" (https://tools.ietf.org/html/rfc2440). *Internet Engineering Task Force*. RFC 2440 (https://tools.ietf.org/html/rfc2440). Retrieved 26 March 2015.

40. Golen, Pawel (19 July 2002). "SSH" (http://www.windowsecurity.com/articles/SSH.html). *WindowSecurity*. Retrieved 26 March 2015.

41. Schneier, Bruce (1996). *Applied Cryptography* (https://archive.org/details/Applied_Cryptogra phy_2nd_ed._B._Schneier) (2nd ed.). Wiley. ISBN 978-0-471-11709-4.

42. Paar, Christof (2009). *Understanding cryptography : a textbook for students and practitioners* (https://www.worldcat.org/oclc/567365751). Jan Pelzl. Berlin: Springer. p. 123. ISBN 978-3-642-04101-3. OCLC 567365751 (https://www.worldcat.org/oclc/567365751).

43. Bernstein, Daniel J.; Lange, Tanja (14 September 2017). "Post-quantum cryptography" (htt p://www.nature.com/articles/nature23461). *Nature*. **549** (7671): 188–194. doi:10.1038/nature23461 (https://doi.org/10.1038%2Fnature23461). ISSN 0028-0836 (http s://www.worldcat.org/issn/0028-0836).

44. "Notices". *Federal Register*. **72** (212). 2 November 2007. "Archived copy" (https://web.archive.org/web/20080228075550/http://csrc.nist.gov/groups/S T/hash/documents/FR_Notice_Nov07.pdf) (PDF). Archived from the original on 28 February 2008. Retrieved 27 January 2009.

45. "NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition" (https://www.nist.go v/itl/csd/sha-100212.cfm). *Tech Beat*. National Institute of Standards and Technology. 2 October 2012. Retrieved 26 March 2015.

46. Diffie, Whitfield; Hellman, Martin (8 June 1976). "Multi-user cryptographic techniques". *AFIPS Proceedings*. **45**: 109–112. doi:10.1145/1499799.1499815 (https://doi.org/10.1145% 2F1499799.1499815). S2CID 13210741 (https://api.semanticscholar.org/CorpusID:1321074 1).

47. Ralph Merkle was working on similar ideas at the time and encountered publication delays, and Hellman has suggested that the term used should be Diffie–Hellman–Merkle aysmmetric key cryptography.

48. Kahn, David (Fall 1979). "Cryptology Goes Public". *Foreign Affairs*. **58** (1): 141–159. doi:10.2307/20040343 (https://doi.org/10.2307%2F20040343). JSTOR 20040343 (https://w ww.jstor.org/stable/20040343).

49. "Using Client-Certificate based authentication with NGINX on Ubuntu - SSLTrust" (https://w ww.ssltrust.com.au/help/setup-guides/client-certificate-authentication). *SSLTrust*. Retrieved 13 June 2019.

50. Rivest, Ronald L.; Shamir, A.; Adleman, L. (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". *Communications of the ACM*. **21** (2): 120–126. CiteSeerX 10.1.1.607.2677 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.607. 2677). doi:10.1145/359340.359342 (https://doi.org/10.1145%2F359340.359342). S2CID 2873616 (https://api.semanticscholar.org/CorpusID:2873616). "Archived copy" (https://web.archive.org/web/20011116122233/http://theory.lcs.mit.edu/~rive st/rsapaper.pdf) (PDF). Archived from the original (http://theory.lcs.mit.edu/~rivest/rsapaper.p df) (PDF) on 16 November 2001. Retrieved 20 April 2006. Previously released as an MIT "Technical Memo" in April 1977, and published in Martin Gardner's *Scientific American* Mathematical recreations column

51. Wayner, Peter (24 December 1997). "British Document Outlines Early Encryption Discovery" (https://www.nytimes.com/library/cyber/week/122497encrypt.html). *The New York Times*. Retrieved 26 March 2015.

52. Cocks, Clifford (20 November 1973). "A Note on 'Non-Secret Encryption' " (http://www.fi.mun i.cz/usr/matyas/lecture/paper2.pdf) (PDF). *CESG Research Report*.

53. Singh, Simon (1999). *The Code Book* (https://archive.org/details/codebookevolutio00sing). Doubleday. pp. 279–292 (https://archive.org/details/codebookevolutio00sing/page/279). ISBN 9780385495318.

54. Shannon, Claude; Weaver, Warren (1963). *The Mathematical Theory of Communication*. University of Illinois Press. ISBN 978-0-252-72548-7.

55. "An Example of a Man-in-the-middle Attack Against Server Authenticated SSL-sessions" (http://www8.cs.umu.se/education/examina/Rapporter/MattiasEriksson.pdf) (PDF).

56. Junod, Pascal (2001). *On the Complexity of Matsui's Attack* (http://citeseer.ist.psu.edu/cache/papers/cs/22094/http:zSzzSzeprint.iacr.orgzSz2001zSz056.pdf/junod01complexity.pdf) (PDF). *Selected Areas in Cryptography*. Lecture Notes in Computer Science. Vol. 2259. pp. 199–211. doi:10.1007/3-540-45537-X_16 (https://doi.org/10.1007%2F3-540-45537-X_16). ISBN 978-3-540-43066-7.

57. Song, Dawn; Wagner, David A.; Tian, Xuqing (2001). "Timing Analysis of Keystrokes and Timing Attacks on SSH" (http://citeseer.ist.psu.edu/cache/papers/cs/22094/http:zSzzSzeprint.iacr.orgzSz2001zSz056.pdf/junod01complexity.pdf) (PDF). *Tenth USENIX Security Symposium*.

58. Brands, S. (1994). "Untraceable Off-line Cash in Wallet with Observers". *Untraceable Off-line Cash in Wallets with Observers* (https://web.archive.org/web/20110726214409/http://ftp.se.kde.org/pub/security/docs/ecash/crypto93.ps.gz). *Advances in Cryptology—Proceedings of CRYPTO*. Lecture Notes in Computer Science. Vol. 773. pp. 302–318. doi:10.1007/3-540-48329-2_26 (https://doi.org/10.1007%2F3-540-48329-2_26). ISBN 978-3-540-57766-9. Archived from the original (http://ftp.se.kde.org/pub/security/docs/ecash/crypto93.ps.gz) on 26 July 2011.

59. Babai, László (1985). "Trading group theory for randomness". *Proceedings of the seventeenth annual ACM symposium on Theory of computing - STOC '85* (http://portal.acm.org/citation.cfm?id=22192). *Proceedings of the Seventeenth Annual Symposium on the Theory of Computing*. Stoc '85. pp. 421–429. CiteSeerX 10.1.1.130.3397 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.130.3397). doi:10.1145/22145.22192 (https://doi.org/10.1145%2F22145.22192). ISBN 978-0-89791-151-1. S2CID 17981195 (https://api.semanticscholar.org/CorpusID:17981195).

60. Goldwasser, S.; Micali, S.; Rackoff, C. (1989). "The Knowledge Complexity of Interactive Proof Systems". *SIAM Journal on Computing*. **18** (1): 186–208. CiteSeerX 10.1.1.397.4002 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.397.4002). doi:10.1137/0218012 (https://doi.org/10.1137%2F0218012).

61. Blakley, G. (June 1979). "Safeguarding cryptographic keys". *Proceedings of AFIPS 1979*. **48**: 313–317.

62. Shamir, A. (1979). "How to share a secret". *Communications of the ACM*. **22** (11): 612–613. doi:10.1145/359168.359176 (https://doi.org/10.1145%2F359168.359176). S2CID 16321225 (https://api.semanticscholar.org/CorpusID:16321225).

63. Gunathilake, Nilupulee A.; Al-Dubai, Ahmed; Buchana, William J. (2 November 2020). "Recent Advances and Trends in Lightweight Cryptography for IoT Security" (https://ieeexplore.ieee.org/document/9269083). *2020 16th International Conference on Network and Service Management (CNSM)*. Izmir, Turkey: IEEE: 1–5. doi:10.23919/CNSM50824.2020.9269083 (https://doi.org/10.23919%2FCNSM50824.2020.9269083). ISBN 978-3-903176-31-7. S2CID 227277538 (https://api.semanticscholar.org/CorpusID:227277538).

64. Thakor, Vishal A.; Razzaque, Mohammad Abdur; Khandaker, Muhammad R. A. (2021). "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities" (https://doi.org/10.1109%2FACCESS.2021.3052867). *IEEE Access*. **9**: 28177–28193. doi:10.1109/ACCESS.2021.3052867 (https://doi.org/10.1109%2FACCESS.2021.3052867). ISSN 2169-3536 (https://www.worldcat.org/issn/2169-3536). S2CID 232042514 (https://api.semanticscholar.org/CorpusID:232042514).

65. Cohen, Fred (1995). "2.4 - Applications of Cryptography" (http://all.net/edu/curr/ip/Chap2-4.html). *all.net*. Archived (https://web.archive.org/web/19990824044441/http://all.net/edu/curr/ip/Chap2-4.html) from the original on 24 August 1999. Retrieved 21 December 2021.

66. "4 Common Encryption Methods to Shield Sensitive Data From Prying Eyes" (https://www.g etapp.com/resources/common-encryption-methods/). *GetApp*. Retrieved 14 May 2022.

67. Chamberlain, Austin (12 March 2017). "Applications of Cryptography | UCL Risky Business" (https://blogs.ucl.ac.uk/infosec/2017/03/12/applications-of-cryptography/). *blogs.ucl.ac.uk*. Archived (https://web.archive.org/web/20180226185448/https://blogs.ucl.ac.uk/infosec/2017/ 03/12/applications-of-cryptography/) from the original on 26 February 2018. Retrieved 21 December 2021.

68. "Crypto FAQ: What is cryptocurrency?" (https://cryptocurrencyworks.com/faq//faq/what-is-cry ptocurrency.html). *CryptoCurrency Works™*. Retrieved 27 August 2022.

69. "Crypto FAQ: What is cryptoeconomics & how does it work?" (https://cryptoeconworks.com/f aq/what-is-cryptoeconomics.html). *cryptoeconworks.com*. Retrieved 27 August 2022.

70. "6.5.1 What Are the Cryptographic Policies of Some Countries?" (http://www.emc.com/emc-p lus/rsa-labs/standards-initiatives/cryptographic-policies-countries.htm). RSA Laboratories. Retrieved 26 March 2015.

71. Rosenoer, Jonathan (1995). "Cryptography & Speech". *CyberLaw*. "Archived copy" (https://web.archive.org/web/20051201184530/http://www.cyberlaw.com/cyl w1095.html). Archived from the original (http://www.cyberlaw.com/cylw1095.html) on 1 December 2005. Retrieved 23 June 2006.

72. "Case Closed on Zimmermann PGP Investigation" (http://www.ieee-security.org/Cipher/New sbriefs/1996/960214.zimmerman.html). *IEEE Computer Society's Technical Committee on Security and Privacy*. 14 February 1996. Retrieved 26 March 2015.

73. Levy, Steven (2001). *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age*. Penguin Books. p. 56. ISBN 978-0-14-024432-8. OCLC 244148644 (http s://www.worldcat.org/oclc/244148644).

74. "Bernstein v USDOJ" (http://www.epic.org/crypto/export_controls/bernstein_decision_9_cir.h tml). *Electronic Privacy Information Center*. United States Court of Appeals for the Ninth Circuit. 6 May 1999. Retrieved 26 March 2015.

75. "Dual-use List – Category 5 – Part 2 – "Information Security" " (https://www.bis.doc.gov/inde x.php/documents/regulations-docs/445-category-5-part-2-information-security/file) (PDF). *Wassenaar Arrangement*. Retrieved 26 March 2015.

76. ".4 United States Cryptography Export/Import Laws" (http://www.emc.com/emc-plus/rsa-labs/ standards-initiatives/united-states-cryptography-export-import.htm). *RSA Laboratories*. Retrieved 26 March 2015.

77. Schneier, Bruce (15 June 2000). "The Data Encryption Standard (DES)" (http://www.schneie r.com/crypto-gram-0006.html#DES). *Crypto-Gram*. Retrieved 26 March 2015.

78. Coppersmith, D. (May 1994). "The Data Encryption Standard (DES) and its strength against attacks" (http://domino.watson.ibm.com/tchjr/journalindex.nsf/0/94f78816c77fc77885256bfa0 067fb98?OpenDocument) (PDF). *IBM Journal of Research and Development*. **38** (3): 243– 250. doi:10.1147/rd.383.0243 (https://doi.org/10.1147%2Frd.383.0243). Retrieved 26 March 2015.

79. Biham, E.; Shamir, A. (1991). "Differential cryptanalysis of DES-like cryptosystems". *Journal of Cryptology*. **4** (1): 3–72. doi:10.1007/bf00630563 (https://doi.org/10.1007%2Fbf00630563). S2CID 206783462 (https://api.semanticscholar.or g/CorpusID:206783462).

80. "The Digital Millennium Copyright Act of 1998" (http://www.copyright.gov/legislation/dmca.p df) (PDF). *United States Copyright Office*. Retrieved 26 March 2015.

81. Ferguson, Niels (15 August 2001). "Censorship in action: why I don't publish my HDCP results" (https://web.archive.org/web/20011201184919/http://www.macfergus.com/niels/dmc a/cia.html). Archived from the original (http://www.macfergus.com/niels/dmca/cia.html) on 1 December 2001. Retrieved 16 February 2009.

82. Schneier, Bruce (6 August 2001). "Arrest of Computer Researcher Is Arrest of First Amendment Rights" (https://www.schneier.com/essays/archives/2001/08/arrest_of_computer _r.html). InternetWeek. Retrieved 7 March 2017.

83. Williams, Christopher (11 August 2009). "Two convicted for refusal to decrypt data" (https://w ww.theregister.co.uk/2009/08/11/ripa_iii_figures/). *The Register*. Retrieved 26 March 2015.

84. Williams, Christopher (24 November 2009). "UK jails schizophrenic for refusal to decrypt files" (https://www.theregister.co.uk/2009/11/24/ripa_jfl/). *The Register*. Retrieved 26 March 2015.

85. Ingold, John (4 January 2012). "Password case reframes Fifth Amendment rights in context of digital world" (http://www.denverpost.com/news/ci_19669803). *The Denver Post*. Retrieved 26 March 2015.

86. Leyden, John (13 July 2011). "US court test for rights not to hand over crypto keys" (https://w ww.theregister.co.uk/2011/07/13/eff_piles_in_against_forced_decryption/). *The Register*. Retrieved 26 March 2015.

87. "Order Granting Application under the All Writs Act Requiring Defendant Fricosu to Assist in the Execution of Previously Issued Search Warrants" (https://www.wired.com/images_blogs/t hreatlevel/2012/01/decrypt.pdf) (PDF). United States District Court for the District of Colorado. Retrieved 26 March 2015.

Further reading

- Arbib, Jonathan; Dwyer, John (31 January 2011). *Discrete Mathematics for Cryptography* (1 ed.). Algana Publishing. ISBN 978-1-907934-01-8.

- Becket, B (1988). *Introduction to Cryptology*. Blackwell Scientific Publications. ISBN 978-0-632-01836-9. OCLC 16832704 (https://www.worldcat.org/oclc/16832704). Excellent coverage of many classical ciphers and cryptography concepts and of the "modern" DES and RSA systems.

- *Cryptography and Mathematics* by Bernhard Esslinger, 200 pages, part of the free open-source package CrypTool, "PDF download" (https://web.archive.org/web/20110722183013/ http://www.cryptool.org/download/CrypToolScript-en.pdf) (PDF). Archived from the original on 22 July 2011. Retrieved 23 December 2013.. CrypTool is the most widespread e-learning program about cryptography and cryptanalysis, open source.

- *In Code: A Mathematical Journey* by Sarah Flannery (with David Flannery). Popular account of Sarah's award-winning project on public-key cryptography, co-written with her father.

- James Gannon, *Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century*, Washington, D.C., Brassey's, 2001, ISBN 1-57488-367-4.

- Oded Goldreich, *Foundations of Cryptography* (http://www.wisdom.weizmann.ac.il/~oded/foc -book.html), in two volumes, Cambridge University Press, 2001 and 2004.

- *Alvin's Secret Code* by Clifford B. Hicks (children's novel that introduces some basic cryptography and cryptanalysis).

- *Introduction to Modern Cryptography (http://www.cs.umd.edu/~jkatz/imc.html)* by Jonathan Katz and Yehuda Lindell.

- Ibrahim A. Al-Kadi, "The Origins of Cryptology: the Arab Contributions," Cryptologia, vol. 16, no. 2 (April 1992), pp. 97–126.

- Christof Paar (https://web.archive.org/web/20060709111152/http://www.crypto.rub.de/en_paar.html), Jan Pelzl, *Understanding Cryptography, A Textbook for Students and Practitioners*. (http://www.cryptography-textbook.com/) Archived (https://web.archive.org/web/20201031190651/http://cryptography-textbook.com/) 31 October 2020 at the Wayback Machine Springer, 2009. (Slides, online cryptography lectures and other information are available on the companion web site.) Very accessible introduction to practical cryptography for non-mathematicians.
- "Max Planck Encyclopedia of Public International Law" (http://www.mpepil.com)., giving an overview of international law issues regarding cryptography.
- *Introduction to Modern Cryptography* by Phillip Rogaway and Mihir Bellare, a mathematical introduction to theoretical cryptography including reduction-based security proofs. PDF download (http://www.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf).
- Stallings, William (March 2013). *Cryptography and Network Security: Principles and Practice* (6th ed.). Prentice Hall. ISBN 978-0-13-335469-0.
- Tenzer, Theo (2021): *SUPER SECRETO – The Third Epoch of Cryptography: Multiple, exponential, quantum-secure and above all, simple and practical Encryption for Everyone*, Norderstedt, ISBN 9783755761174.
- Johann-Christoph Woltag, 'Coded Communications (Encryption)' in Rüdiger Wolfrum (ed) *Max Planck Encyclopedia of Public International Law* (Oxford University Press 2009).

External links

- The dictionary definition of *cryptography* at Wiktionary
- Media related to Cryptography at Wikimedia Commons
- Cryptography (https://www.bbc.co.uk/programmes/p004y272) on *In Our Time* at the BBC
- Cryptography Works - web information portal (https://cryptographyworks.com)
- Crypto Glossary and Dictionary of Technical Cryptography (https://ciphersbyritter.com/GLOSSARY.HTM)
- A Course in Cryptography (https://www.cs.cornell.edu/courses/cs4830/2010fa/lecnotes.pdf) by Raphael Pass & Abhi Shelat – offered at Cornell in the form of lecture notes.
- For more on the use of cryptographic elements in fiction, see: Dooley, John F., William and Marilyn Ingersoll Professor of Computer Science, Knox College (23 August 2012). "Cryptology in Fiction" (https://web.archive.org/web/20200729044734/http://faculty.knox.edu/jdooley/Crypto/CryptoFiction.htm). Archived from the original (http://faculty.knox.edu/jdooley/Crypto/CryptoFiction.htm) on 29 July 2020. Retrieved 20 February 2015.
- The George Fabyan Collection (https://www.loc.gov/rr/rarebook/coll/073.html) at the Library of Congress has early editions of works of seventeenth-century English literature, publications relating to cryptography.