

Cryptography

Cryptography

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

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 the 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 eavesdropping adversary. 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. 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. Cryptography also plays a major role in digital rights management and copyright infringement disputes with regard to digital media.

Public-key cryptography

Public-key cryptography, or asymmetric cryptography, is the field of cryptographic systems that use pairs of related keys. Each key pair consists of a - Public-key cryptography, or asymmetric cryptography, is the field of cryptographic systems that use pairs of related keys. Each key pair consists of a public key and a corresponding private key. Key pairs are generated with cryptographic algorithms based on mathematical

problems termed one-way functions. Security of public-key cryptography depends on keeping the private key secret; the public key can be openly distributed without compromising security. There are many kinds of public-key cryptosystems, with different security goals, including digital signature, Diffie–Hellman key exchange, public-key key encapsulation, and public-key encryption.

Public key algorithms are fundamental security primitives in modern cryptosystems, including applications and protocols that offer assurance of the confidentiality and authenticity of electronic communications and data storage. They underpin numerous Internet standards, such as Transport Layer Security (TLS), SSH, S/MIME, and PGP. Compared to symmetric cryptography, public-key cryptography can be too slow for many purposes, so these protocols often combine symmetric cryptography with public-key cryptography in hybrid cryptosystems.

Post-quantum cryptography

Post-quantum cryptography (PQC), sometimes referred to as quantum-proof, quantum-safe, or quantum-resistant, is the development of cryptographic algorithms - Post-quantum cryptography (PQC), sometimes referred to as quantum-proof, quantum-safe, or quantum-resistant, is the development of cryptographic algorithms (usually public-key algorithms) that are currently thought to be secure against a cryptanalytic attack by a quantum computer. Most widely used public-key algorithms rely on the difficulty of one of three mathematical problems: the integer factorization problem, the discrete logarithm problem or the elliptic-curve discrete logarithm problem. All of these problems could be easily solved on a sufficiently powerful quantum computer running Shor's algorithm or possibly alternatives.

As of 2025, quantum computers lack the processing power to break widely used cryptographic algorithms; however, because of the length of time required for migration to quantum-safe cryptography, cryptographers are already designing new algorithms to prepare for Y2Q or Q-Day, the day when current algorithms will be vulnerable to quantum computing attacks. Mosca's theorem provides the risk analysis framework that helps organizations identify how quickly they need to start migrating.

Their work has gained attention from academics and industry through the PQCrypto conference series hosted since 2006, several workshops on Quantum Safe Cryptography hosted by the European Telecommunications Standards Institute (ETSI), and the Institute for Quantum Computing. The rumoured existence of widespread harvest now, decrypt later programs has also been seen as a motivation for the early introduction of post-quantum algorithms, as data recorded now may still remain sensitive many years into the future.

In contrast to the threat quantum computing poses to current public-key algorithms, most current symmetric cryptographic algorithms and hash functions are considered to be relatively secure against attacks by quantum computers. While the quantum Grover's algorithm does speed up attacks against symmetric ciphers, doubling the key size can effectively counteract these attacks. Thus post-quantum symmetric cryptography does not need to differ significantly from current symmetric cryptography.

In 2024, the U.S. National Institute of Standards and Technology (NIST) released final versions of its first three Post-Quantum Cryptography Standards.

Key (cryptography)

A key in cryptography is a piece of information, usually a string of numbers or letters that are stored in a file, which, when processed through a cryptographic - A key in cryptography is a piece of information, usually a string of numbers or letters that are stored in a file, which, when processed through a cryptographic

algorithm, can encode or decode cryptographic data. Based on the used method, the key can be different sizes and varieties, but in all cases, the strength of the encryption relies on the security of the key being maintained. A key's security strength is dependent on its algorithm, the size of the key, the generation of the key, and the process of key exchange.

Financial cryptography

Financial cryptography is the use of cryptography in applications in which financial loss could result from subversion of the message system. Financial - Financial cryptography is the use of cryptography in applications in which financial loss could result from subversion of the message system. Financial cryptography is distinguished from traditional cryptography in that for most of recorded history, cryptography has been used almost entirely for military and diplomatic purposes.

Financial cryptography includes the mechanisms and algorithms necessary for the protection of financial transfers, in addition to the creation of new forms of money. Proof of work and various auction protocols fall under the umbrella of Financial cryptography. Hashcash is being used to limit spam.

Financial cryptography has been seen to have a very broad scope of application. Ian Grigg sees financial cryptography in seven layers, being the combination of seven distinct disciplines: cryptography, software engineering, rights, accounting, governance, value, and financial applications. Business failures can often be traced to the absence of one or more of these disciplines, or to poor application of them. This views Financial cryptography as an appropriately cross-discipline subject. Indeed, inevitably so, given that finance and cryptography are each built upon multiple disciplines.

Salt (cryptography)

In cryptography, a salt is random data fed as an additional input to a one-way function that hashes data, a password or passphrase. Salting helps defend - In cryptography, a salt is random data fed as an additional input to a one-way function that hashes data, a password or passphrase. Salting helps defend against attacks that use precomputed tables (e.g. rainbow tables), by vastly growing the size of table needed for a successful attack. It also helps protect passwords that occur multiple times in a database, as a new salt is used for each password instance. Additionally, salting does not place any burden on users.

Typically, a unique salt is randomly generated for each password. The salt and the password (or its version after key stretching) are concatenated and fed to a cryptographic hash function, and the output hash value is then stored with the salt in a database. The salt does not need to be encrypted, because knowing the salt would not help the attacker.

Salting is broadly used in cybersecurity, from Unix system credentials to Internet security.

Salts are related to cryptographic nonces.

Encryption

In cryptography, encryption (more specifically, encoding) is the process of transforming information in a way that, ideally, only authorized parties can - In cryptography, encryption (more specifically, encoding) is the process of transforming information in a way that, ideally, only authorized parties can decode. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Despite its goal, encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor.

For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is possible to decrypt the message without possessing the key but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

Historically, various forms of encryption have been used to aid in cryptography. Early encryption techniques were often used in military messaging. Since then, new techniques have emerged and become commonplace in all areas of modern computing. Modern encryption schemes use the concepts of public-key and symmetric-key. Modern encryption techniques ensure security because modern computers are inefficient at cracking the encryption.

Quantum cryptography

Quantum cryptography is the science of exploiting quantum mechanical properties to perform cryptographic tasks. The best known example of quantum cryptography - Quantum cryptography is the science of exploiting quantum mechanical properties to perform cryptographic tasks. The best known example of quantum cryptography is quantum key distribution, which offers an information-theoretically secure solution to the key exchange problem. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e. non-quantum) communication. For example, it is impossible to copy data encoded in a quantum state. If one attempts to read the encoded data, the quantum state will be changed due to wave function collapse (no-cloning theorem). This could be used to detect eavesdropping in quantum key distribution (QKD).

Elliptic-curve cryptography

Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC - Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys to provide equivalent security, compared to cryptosystems based on modular exponentiation in Galois fields, such as the RSA cryptosystem and ElGamal cryptosystem.

Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme. They are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic-curve factorization.

RSA cryptosystem

cryptosystem) such as RSAES-OAEP, and public-key key encapsulation. In RSA-based cryptography, a user's private key—which can be used to sign messages, or decrypt - The RSA (Rivest–Shamir–Adleman) cryptosystem is a family of public-key cryptosystems, one of the oldest widely used for secure data transmission. The initialism "RSA" comes from the surnames of Ron Rivest, Adi Shamir and Leonard Adleman, who publicly described the algorithm in 1977. An equivalent system was developed secretly in 1973 at Government Communications Headquarters (GCHQ), the British signals intelligence agency, by the English mathematician Clifford Cocks. That system was declassified in 1997.

RSA is used in digital signature such as RSASSA-PSS or RSA-FDH,

public-key encryption of very short messages (almost always a single-use symmetric key in a hybrid cryptosystem) such as RSAES-OAEP,

and public-key key encapsulation.

In RSA-based cryptography, a user's private key—which can be used to sign messages, or decrypt messages sent to that user—is a pair of large prime numbers chosen at random and kept secret.

A user's public key—which can be used to verify messages from the user, or encrypt messages so that only that user can decrypt them—is the product of the prime numbers.

The security of RSA is related to the difficulty of factoring the product of two large prime numbers, the "factoring problem". Breaking RSA encryption is known as the RSA problem. Whether it is as difficult as the factoring problem is an open question. There are no published methods to defeat the system if a large enough key is used.

[http://cache.gawkerassets.com/\\$99261568/vrespecty/wforgiven/cexplore/suzuki+ds80+owners+manual.pdf](http://cache.gawkerassets.com/$99261568/vrespecty/wforgiven/cexplore/suzuki+ds80+owners+manual.pdf)
<http://cache.gawkerassets.com/~32838839/zdifferentiateq/gforgivep/wexplorej/landis+staefa+manuals+rvp+200.pdf>
<http://cache.gawkerassets.com/^98138624/nadvertisef/hdisappearq/cprovideg/the+old+man+and+the+sea.pdf>
<http://cache.gawkerassets.com/-98128939/rcollapsej/xdiscussf/dregulaten/laboratory+manual+physical+geology+8th+edition+answers.pdf>
http://cache.gawkerassets.com/_22157315/xdifferentiateq/gevaluateb/udedicaten/mcgraw+hill+connect+intermediate
[http://cache.gawkerassets.com/\\$34879724/linterviewe/fexcludem/mregulatea/the+handbook+for+helping+kids+with-](http://cache.gawkerassets.com/$34879724/linterviewe/fexcludem/mregulatea/the+handbook+for+helping+kids+with-)
<http://cache.gawkerassets.com/!36654303/ninterviewb/pexaminef/cimpressg/some+cambridge+controversies+in+the>
<http://cache.gawkerassets.com/!84181237/fadvertisei/dexcludem/jscheduleh/motoman+dx100+programming+manual>
<http://cache.gawkerassets.com/=39023858/sdifferentiateb/pexaminem/xdedicated/operations+management+7th+editi>
[http://cache.gawkerassets.com/\\$31426351/fadvertisen/ddisappearq/iwelcomea/nisan+xtrail+service+manual.pdf](http://cache.gawkerassets.com/$31426351/fadvertisen/ddisappearq/iwelcomea/nisan+xtrail+service+manual.pdf)