Cryptography

Cryptography

Cryptography, or cryptology (from Ancient Greek: ???????, romanized: kryptós "hidden, secret"; and ??????? graphein, "to write", or -????? -logia, "study"

Cryptography, or cryptology (from Ancient Greek: ???????, romanized: 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...

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...

Outline of cryptography

and topical guide to cryptography: Cryptography (or cryptology) – practice and study of hiding information. Modern cryptography intersects the disciplines

The following outline is provided as an overview of and topical guide to cryptography:

Cryptography (or cryptology) – practice and study of hiding information. Modern cryptography intersects the disciplines of mathematics, computer science, and engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Bibliography of cryptography

Books on cryptography have been published sporadically and with variable quality for a long time. This is despite the paradox that secrecy is of the essence

Books on cryptography have been published sporadically and with variable quality for a long time. This is despite the paradox that secrecy is of the essence in sending confidential messages – see Kerckhoffs' principle.

In contrast, the revolutions in cryptography and secure communications since the 1970s are covered in the available literature.

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.

Export of cryptography

The export of cryptography is the transfer from one country to another of devices and technology related to cryptography. In the early days of the Cold

The export of cryptography is the transfer from one country to another of devices and technology related to cryptography.

In the early days of the Cold War, the United States and its allies developed an elaborate series of export control regulations designed to prevent a wide range of Western technology from falling into the hands of others, particularly the Eastern bloc. All export of technology classed as 'critical' required a license. CoCom was organized to coordinate Western export controls.

Many countries, notably those participating in the Wassenaar Arrangement, introduced restrictions. The Wassenaar restrictions were largely loosened in the late 2010s.

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 finite 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.

Strong cryptography

Strong cryptography or cryptographically strong are general terms used to designate the cryptographic algorithms that, when used correctly, provide a very

Strong cryptography or cryptographically strong are general terms used to designate the cryptographic algorithms that, when used correctly, provide a very high (usually insurmountable) level of protection against any eavesdropper, including the government agencies. There is no precise definition of the boundary line between the strong cryptography and (breakable) weak cryptography, as this border constantly shifts due to

improvements in hardware and cryptanalysis techniques. These improvements eventually place the capabilities once available only to the NSA within the reach of a skilled individual, so in practice there are only two levels of cryptographic security, "cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading...

Quantum cryptography

Quantum cryptography is the science of exploiting quantum mechanical properties such as quantum entanglement, measurement disturbance, no-cloning theorem

Quantum cryptography is the science of exploiting quantum mechanical properties such as quantum entanglement, measurement disturbance, no-cloning theorem, and the principle of superposition to perform various cryptographic tasks. Historically defined as the practice of encoding messages, a concept now referred to as encryption, quantum cryptography plays a crucial role in the secure processing, storage, and transmission of information across various domains. One aspect of quantum cryptography is quantum key distribution (QKD), 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...

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...