**Cryptography** (or *cryptology*; from [Greek](http://en.wikipedia.org/wiki/Ancient_Greek) [κρυπτός](http://en.wiktionary.org/wiki/en:%CE%BA%CF%81%CF%85%CF%80%CF%84%CF%8C%CF%82), "hidden, secret"; and [γράφειν](http://en.wiktionary.org/wiki/en:%CE%B3%CF%81%CE%AC%CF%86%CF%89#Ancient_Greek), *graphein*, "writing", or [-λογία](http://en.wiktionary.org/wiki/en:-%CE%BB%CE%BF%CE%B3%CE%AF%CE%B1#Greek), [*-logia*](http://en.wikipedia.org/wiki/-logy), "study", respectively)[1] is the practice and study of techniques for secure communication in the presence of third parties (called [adversaries](http://en.wikipedia.org/wiki/Adversary_(cryptography))).[2] More generally, it is about constructing and analyzing [protocols](http://en.wikipedia.org/wiki/Communications_protocol) that overcome the influence of adversaries[3] and which are related to various aspects in [information security](http://en.wikipedia.org/wiki/Information_security) such as data [confidentiality](http://en.wikipedia.org/wiki/Confidentiality), [data integrity](http://en.wikipedia.org/wiki/Data_integrity), and [authentication](http://en.wikipedia.org/wiki/Authentication).[4] Modern cryptography intersects the disciplines of [mathematics](http://en.wikipedia.org/wiki/Mathematics), [computer science](http://en.wikipedia.org/wiki/Computer_science), and [electrical engineering](http://en.wikipedia.org/wiki/Electrical_engineering). Applications of cryptography include [ATM cards](http://en.wikipedia.org/wiki/Automated_teller_machine), [computer passwords](http://en.wikipedia.org/wiki/Password), and [electronic commerce](http://en.wikipedia.org/wiki/Electronic_commerce).

Cryptography prior to the modern age was effectively synonymous with [*encryption*](http://en.wikipedia.org/wiki/Encryption), the conversion of information from a readable state to apparent [nonsense](http://en.wikipedia.org/wiki/Nonsense). The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same. Since [World War I](http://en.wikipedia.org/wiki/World_War_I) and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around [computational hardness assumptions](http://en.wikipedia.org/wiki/Computational_hardness_assumption), making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances (e.g., improvements in [integer factorization](http://en.wikipedia.org/wiki/Integer_factorization) algorithms) and faster computing technology require these solutions to be continually adapted. There exist [information-theoretically secure](http://en.wikipedia.org/wiki/Information_theoretic_security) schemes that provably cannot be broken even with unlimited computing power—an example is the [one-time pad](http://en.wikipedia.org/wiki/One-time_pad)—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.

Before the modern era, cryptography was concerned solely with message confidentiality (i.e., encryption)—conversion of [messages](http://en.wikipedia.org/wiki/Information) 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 was used to (attempt to) ensure [secrecy](http://en.wikipedia.org/wiki/Secrecy) in [communications](http://en.wikipedia.org/wiki/Communications), such as those of [spies](http://en.wikipedia.org/wiki/Spy), military leaders, and [diplomats](http://en.wikipedia.org/wiki/Diplomat). In recent decades, the field has expanded beyond confidentiality concerns to include techniques for message integrity checking, sender/receiver identity [authentication](http://en.wikipedia.org/wiki/Authentication), [digital signatures](http://en.wikipedia.org/wiki/Digital_signature), [interactive proofs](http://en.wikipedia.org/wiki/Interactive_proof_system) and [secure computation](http://en.wikipedia.org/wiki/Secure_multiparty_computation), among others.

The earliest forms of secret writing required little more than local pen and paper analogs, as most people could not read. More literacy, or literate opponents, required actual cryptography. An early substitution cipher was the [Caesar cipher](http://en.wikipedia.org/wiki/Caesar_cipher), in which each letter in the plaintext was replaced by a letter some fixed number of positions further down the alphabet. [Suetonius](http://en.wikipedia.org/wiki/Suetonius) reports that [Julius Caesar](http://en.wikipedia.org/wiki/Julius_Caesar) used it with a shift of three to communicate with his generals.

Many mechanical encryption/decryption devices were invented early in the 20th century, and several patented, among them [rotor machines](http://en.wikipedia.org/wiki/Rotor_machine)—famously including the [Enigma machine](http://en.wikipedia.org/wiki/Enigma_machine) used by the German government and military from the late '20s and during [World War II](http://en.wikipedia.org/wiki/World_War_II).[16] The ciphers implemented by better quality examples of these machine designs brought about a substantial increase in cryptanalytic difficulty after WWI.[17]

Essentially, prior to the early 20th century, cryptography was chiefly concerned with [linguistic](http://en.wikipedia.org/wiki/Language) and [lexicographic](http://en.wikipedia.org/wiki/Lexicographic_code) patterns. Since then the emphasis has shifted, and cryptography now makes extensive use of mathematics, including aspects of [information theory](http://en.wikipedia.org/wiki/Information_theory), [computational complexity](http://en.wikipedia.org/wiki/Computational_complexity_theory), [statistics](http://en.wikipedia.org/wiki/Statistics), [combinatorics](http://en.wikipedia.org/wiki/Combinatorics), [abstract algebra](http://en.wikipedia.org/wiki/Abstract_algebra), [number theory](http://en.wikipedia.org/wiki/Number_theory), and finite mathematics generally.

An asymmetric-key cryptosystem was published in 1976 by [Whitfield Diffie](http://en.wikipedia.org/wiki/Whitfield_Diffie) and [Martin Hellman](http://en.wikipedia.org/wiki/Martin_Hellman), who, influenced by [Ralph Merkle](http://en.wikipedia.org/wiki/Ralph_Merkle)'s work on public-key distribution, disclosed a method of public-key agreement. This method of key exchange, which uses [exponentiation in a finite field](http://en.wikipedia.org/wiki/Finite_field#Applications), came to be known as [Diffie–Hellman key exchange](http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange). This was the first published practical method for establishing a shared secret-key over an authenticated (but not private) communications channel without using a prior shared secret.

Since the 1970s, a large number and variety of encryption, digital signature, key agreement, and other techniques have been developed in the field of public-key cryptography. The [ElGamal cryptosystem](http://en.wikipedia.org/wiki/ElGamal_encryption) (invented by [Taher ElGamal](http://en.wikipedia.org/wiki/Taher_ElGamal)) relies on the (similar, and related) difficulty of the [discrete logarithm problem](http://en.wikipedia.org/wiki/Discrete_logarithm_problem).

1. Liddell and Scott's Greek-English Lexicon. Oxford University Press. (1984)
2. Rivest, Ronald L. (1990). "Cryptology". In J. Van Leeuwen. *Handbook of Theoretical Computer Science*. **1**. Elsevier.
3. Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". *Introduction to Modern Cryptography*. p. 10.
4. AJ Menezes, PC van Oorschot, and SA Vanstone, [Handbook of Applied Cryptography](http://web.archive.org/web/20050307081354/www.cacr.math.uwaterloo.ca/hac/) [ISBN 0-8493-8523-7](http://en.wikipedia.org/wiki/Special:BookSources/0849385237).
5. ["UK Data Encryption Disclosure Law Takes Effect"](http://www.pcworld.com/article/137881/uk_data_encryption_disclosure_law_takes_effect.html). Pcworld.com. 2007-10-01. Retrieved 2012-01-28.
6. Leyden, John (2011-07-13). ["US court test for rights not to hand over crypto keys"](http://www.theregister.co.uk/2011/07/13/eff_piles_in_against_forced_decryption/). Theregister.co.uk. Retrieved 2012-01-28.

14.[Ibrahim A. Al-Kadi](http://en.wikipedia.org/w/index.php?title=Ibrahim_A._Al-Kadi&action=edit&redlink=1) (April 1992), "The origins of cryptology: The Arab contributions”, [*Cryptologia*](http://en.wikipedia.org/wiki/Cryptologia) **16** (2): 97–126

15. Schrödel, Tobias (October 2008). "Breaking Short Vigenère Ciphers". *Cryptologia* **32** (4): 334–337. [doi](http://en.wikipedia.org/wiki/Digital_object_identifier):[10.1080/01611190802336097](http://dx.doi.org/10.1080%2F01611190802336097).

16. Hakim, Joy (1995). *A History of Us: War, Peace and all that Jazz*. New York: Oxford University Press. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [0-19-509514-6](http://en.wikipedia.org/wiki/Special:BookSources/0-19-509514-6).

17. [James Gannon](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Special:BookSources/1574883674).

Wide