14 November 2021

Clustering

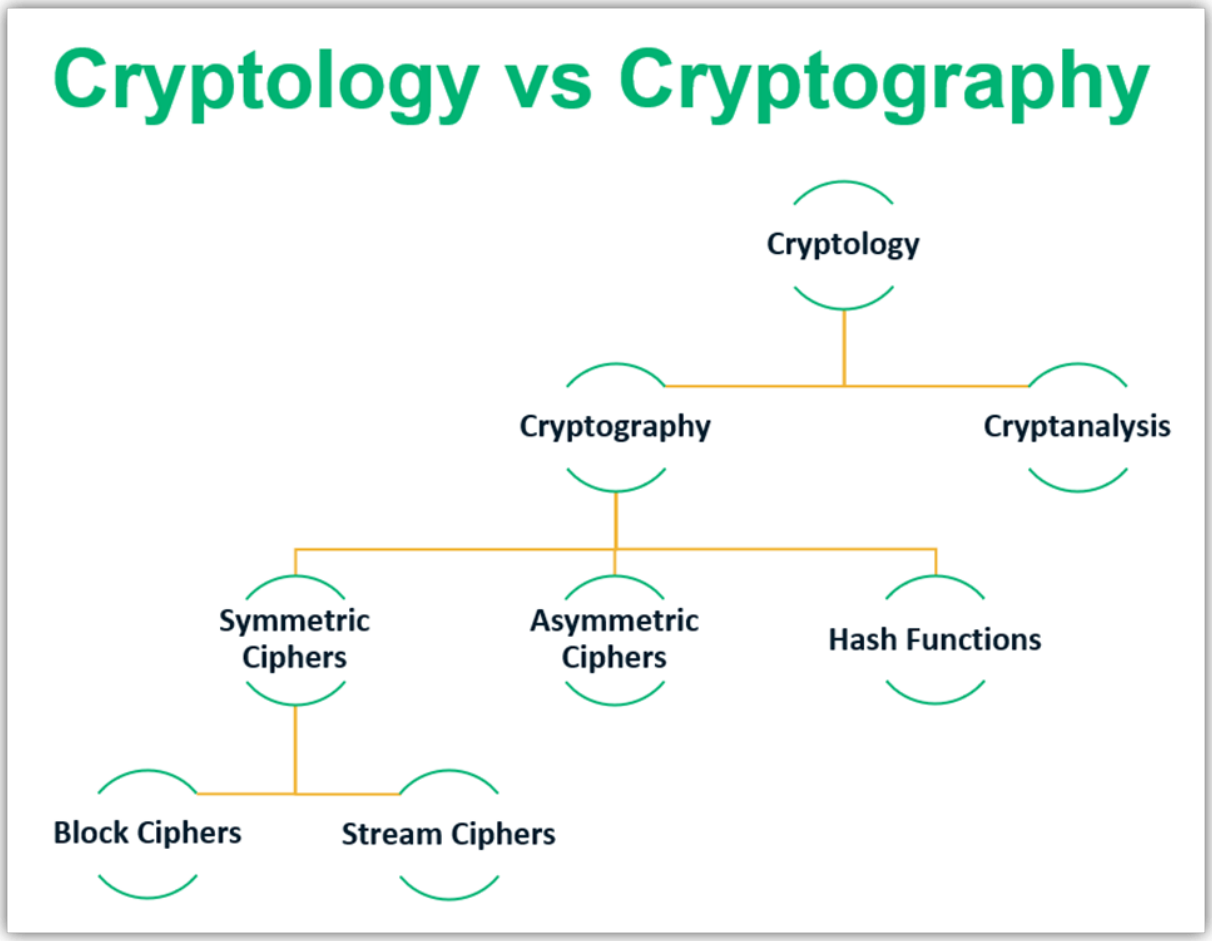
A weakness in cryptography is where a plain-text message generates identical cipher-text messages using the same algorithm but different keys.

Codes

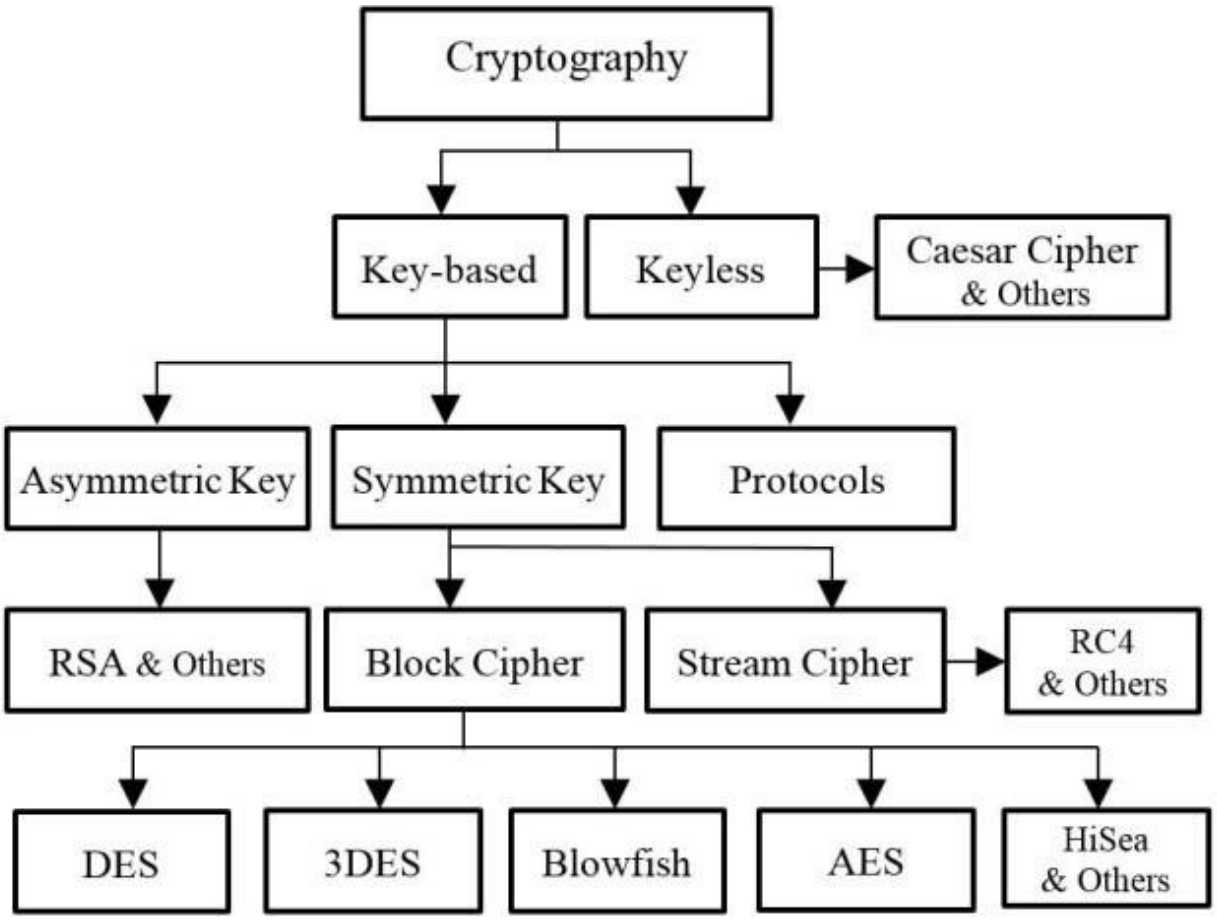
In cryptology, a **code** is a method used to encrypt a message that operates at the level of meaning; that is, words or phrases are converted into something else. A code might transform "change" into "CVGDK" or "cocktail lounge". The U.S. National Security Agency defined a code as "A substitution cryptosystem in which the plaintext elements are primarily words, phrases, or sentences, and the code equivalents (called "code groups") typically consist of letters or digits (or both) in otherwise meaningless combinations of identical length."[1]:Vol I, p. 12 A *codebook* is needed to encrypt, and decrypt the phrases or words.

Cryptoanalysis

Cryptanalysis (from the Greek *kryptós*, "hidden", and *analýein*, "to analyze") refers to the process of analyzing information systems in order to understand hidden aspects of the systems.[1] Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

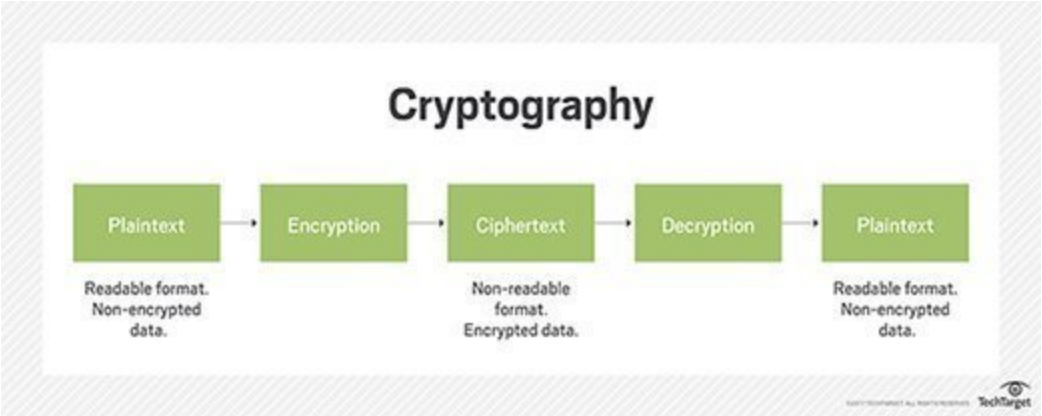


Cryptographic algorithm



Cryptography

Cryptography is the **study of secure communications techniques** that allow only the sender and intended recipient of a message to view its contents. ... Here, data is encrypted using a secret key, and then both the encoded message and secret key are sent to the recipient for decryption.



Cryptology

cryptology, **science concerned with data communication and storage in a secure and usually secret form**. It encompasses both cryptography and cryptanalysis. ... Security obtains from legitimate users being able to transform information by virtue of a secret key or keys—i.e., information known only to them.

Cryptosystem

A cryptosystem is **a structure or scheme consisting of a set of algorithms that converts plaintext to the ciphertext to encode or decode messages securely**. ... To help keep data secure, cryptosystems incorporate the algorithms for key generation, encryption, and decryption techniques.

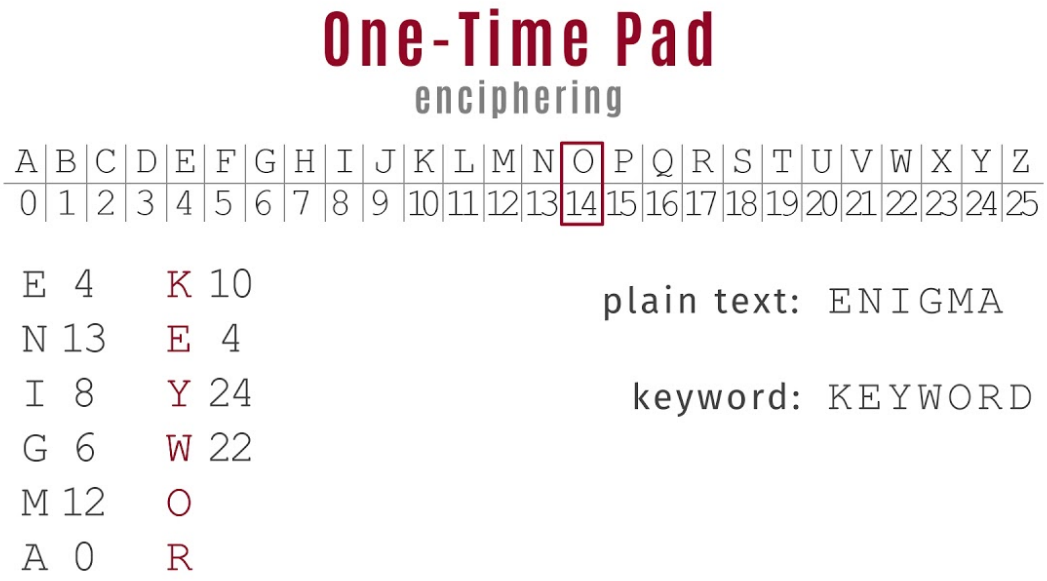
End to end Encryption

End-to-end encryption is a system of communication where only the communicating users can read the messages. In principle, it prevents potential eavesdroppers – including telecom providers, Internet providers, and even the provider of the communication service – from being able to access the cryptographic keys needed to decrypt the conversation.

Link encryption

Link Encryption is a **technique in which communication traveling along a network is encrypted and decrypted at every stage**, or node. It is used to prevent traffic analysis and avoid human error. With link encryption, communication is encrypted at each node such as devices and network switches.

One time pad



Crypto-variable

crypto variables (plural crypto variables) (cryptography) **The key used for encryption and decryption**.

Phishing

Phishing is **a type of social engineering attack often used to steal user data**, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

Black,blue,gray,white box

http://ijiet.com/wp-content/uploads/2017/05/31.pdf

Phreakers

Phreakers are **people who specialize in attacks on the telephone system**. The word, which became popular in the mid-1980s, is probably a combination of the words phone

and freak. ... Modern phreaking involves breaking into and manipulating the phone company's computer system, making it a specialized kind of hacking.

Zero-knowledge proof

In cryptography, a **zero-knowledge proof** or **zero-knowledge protocol** is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true. The essence of zero-knowledge proofs is that it is trivial to prove that one possesses knowledge of certain information by simply revealing it; the challenge is to prove such possession without revealing the information itself or any additional information.

Split knowledge

The PCI DSS explains split knowledge as, “Split knowledge is **a method in which two or more people separately have key components**, where each person knows only their own key component, and the individual key components convey no knowledge of the original cryptographic key.”

Skipjack

In cryptography, **Skipjack** is a block cipher—an algorithm for encryption—developed by the U.S. National Security Agency (NSA). Initially classified, it was originally intended for use in the controversial Clipper chip. Subsequently, the algorithm was declassified.

Skipjack operats 64-bit blocks of text. It uses an 80-bit key and supports the same four modes of operation supported by Des.