Cryptography

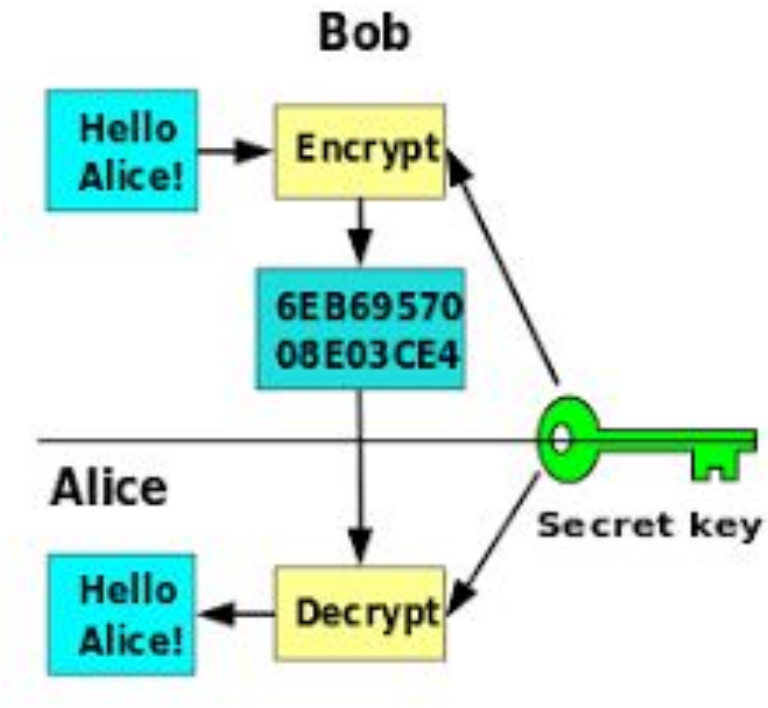
Elijah Charles

Good morning everyone. Today I am here to give a presentation about cryptography. Cryptography is the practice and study of techniques for secure communication in the presence of third parties. Cryptography is commonly used in computer security to protect data from unauthorized access, and it is used in connection with many protocols and applications.

What is Cryptography?

Cryptography is the practice of creating and deciphering codes for the purpose of protecting information. It is a very important tool used in many areas of life, from military operations to financial transactions. Cryptography is an ancient art, with its roots in the early days of civilization. Its use has grown exponentially in recent years, due to the increasing demand for secure communication.

Cont.



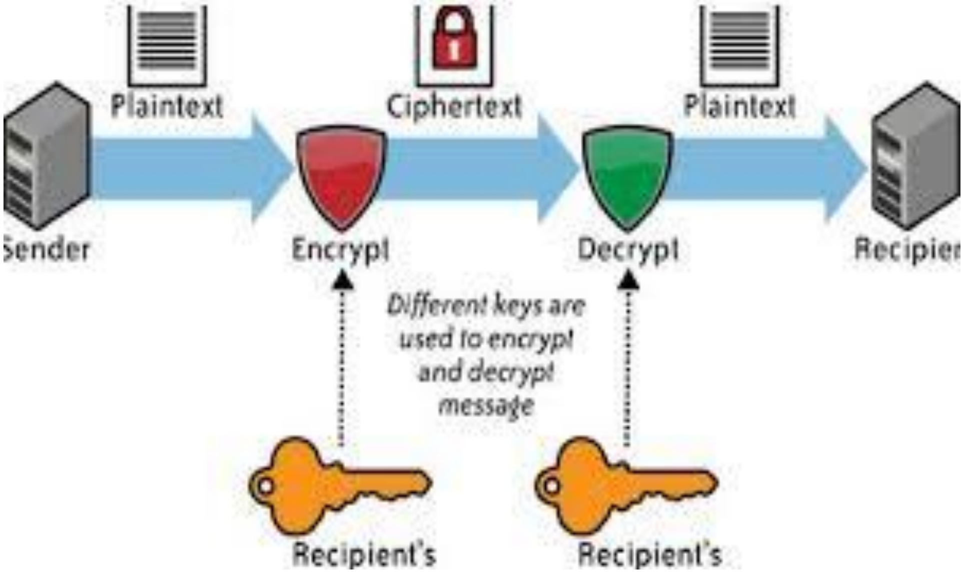
Cryptography works by using algorithms to transform plaintext into ciphertext, making it incomprehensible without a key. This key is usually a combination of numbers and/or letters that allow the user to decrypt the message. Cryptography is used in many areas, such as banking, military operations, and email communication. Banks use cryptography to protect their customers' financial information, while the military uses it to protect sensitive information from enemy forces. Email communication also uses cryptography to protect messages from being viewed by unwanted individuals.

Cont.

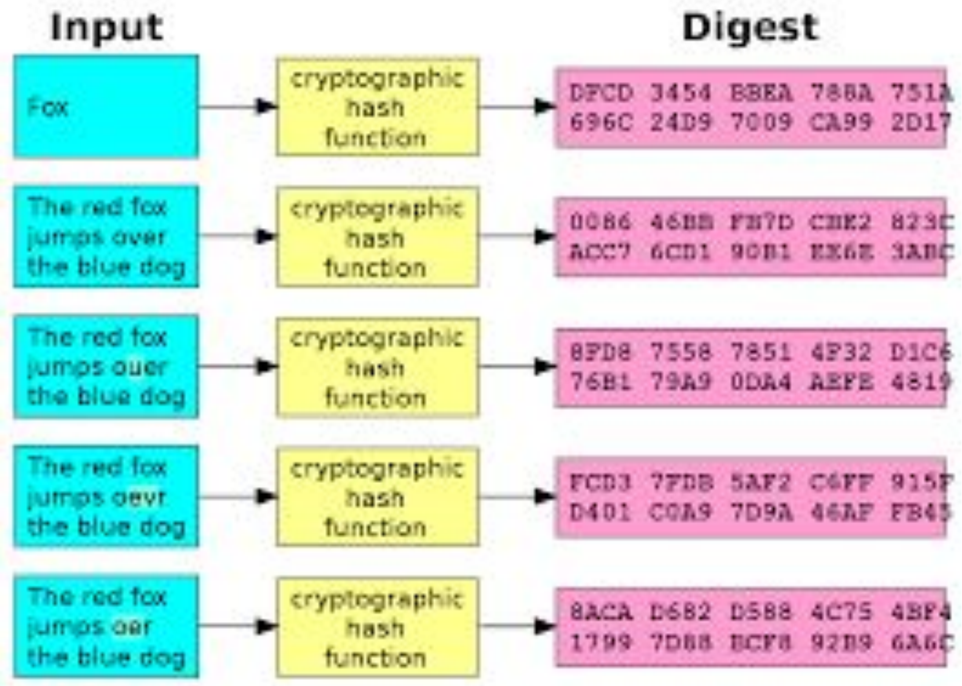
Cryptography can be divided into two main categories: symmetric and asymmetric. Symmetric cryptography uses a single key to both encrypt and decrypt messages. This means that both sender and receiver must have the same key to access the message. Asymmetric cryptography, relies on two different keys to perform these functions. The public key is used to encrypt data, and the private key is used to decrypt data.

What is encryption?

Encryption is a process of transforming information into an unreadable form using a cryptographic algorithm, usually called a cipher. It is a fundamental element of cryptology and is used to protect information from unauthorized access, modification, or disclosure. Encryption ensures that only authorized parties can access the data, and that the data is not altered in any way. Encryption can be used to secure data in transit or at rest, and is often used in combination with other security measures such as authentication, access control, and digital signatures.



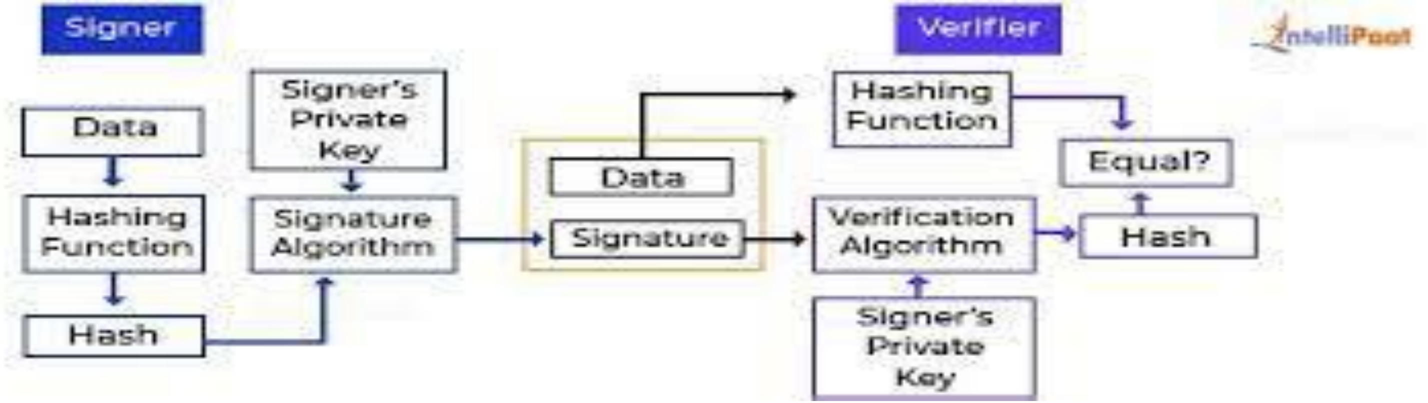
What are hash functions?


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Hash functions in cryptography are mathematical algorithms that take a variable-length input and produce a fixed-length output. They are used to provide a one-way transformation of data, meaning that it is not possible to reverse the process and retrieve the original data from the output. Hash functions are an important tool in cryptography, as they are used to create digital signatures, to verify the integrity of data, and to store passwords securely. The output of a hash function is known as a hash value or a message digest, and it should be unique for a given input.

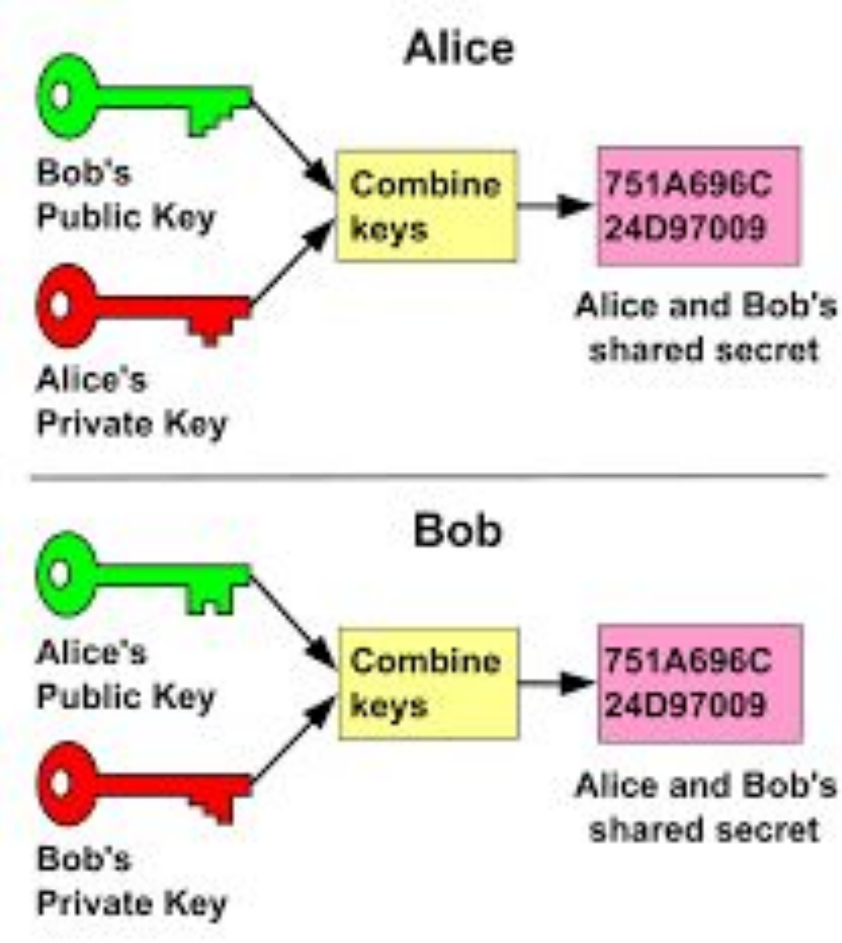
What are digital signatures?

A digital signature is an electronic form of a signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and also ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. Digital signatures use asymmetric cryptography, meaning a pair of keys, a public key and a private key, is used to authenticate the signature. The public key is available for anyone to use and verify the signature, while the private key is kept secret and is used to sign the message or document.

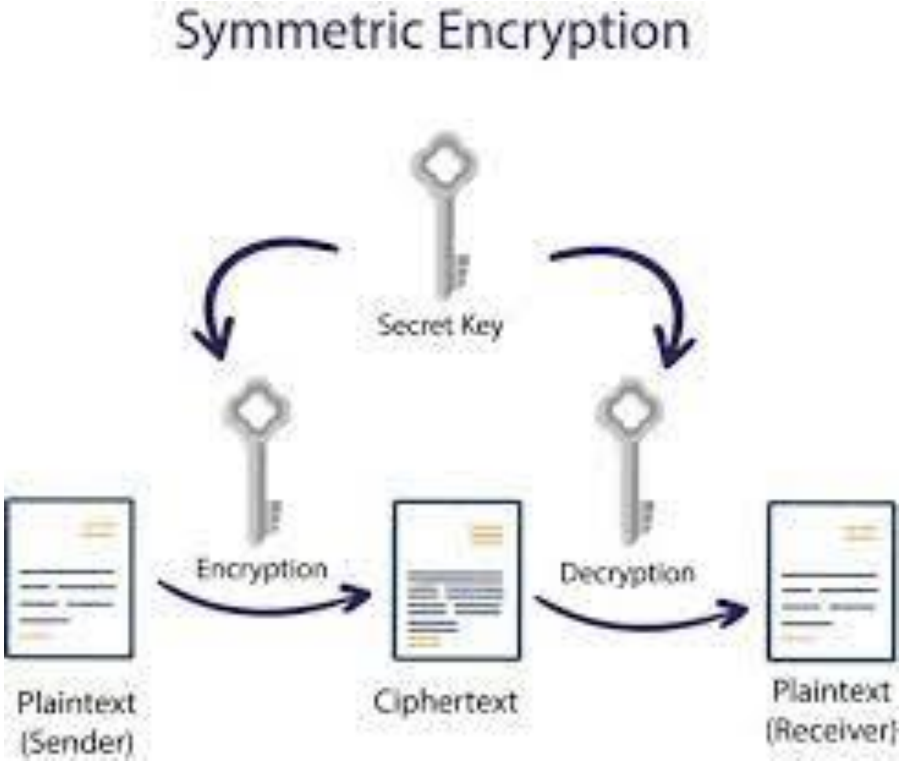


What is key exchange?

Key exchange is a method of securely exchanging cryptographic keys between two parties, usually over an insecure communications channel. It is an important part of creating secure communications on the Internet, as it allows two parties to share a secret key without the risk of it being intercepted by a third-party. The exchanged key can then be used for encryption and authentication purposes, such as for setting up a secure VPN connection. Key exchange protocols often involve the use of public-key cryptography, where each party generates a pair of keys, a public key and a private key, and then exchanges their public keys with the other party. This allows the two parties to securely communicate with each other without having to worry about the security of the channel.



What is key management?



Key management in cryptography is the process of generating, distributing, storing, and controlling access to cryptographic keys. Cryptographic keys are the core elements used to secure cryptographic operations, and proper management is critical to the security of any system involving cryptography. This includes the generation of secure keys, storage of secret keys, secure distribution of public keys, and the destruction of keys once they are no longer needed. Key management also includes the establishment of policies and procedures to ensure that keys are used only for authorized purposes and that access to keys is carefully controlled and monitored.

In conclusion...

These are just some of the ways cryptography is used to protect data. Cryptography is an important tool for many aspects of computer security, and its use is becoming increasingly common. Thank you.