

CS801D: Cryptography & Network Security

Name: Mayukh Datta
Roll no.: 16800116065
Reg. no.: 161680110032
Year: 4th
Dept: CSE



What is cryptography?

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. The prefix "crypt-" means "hidden" or "vault" -- and the suffix "-graphy" stands for "writing."



What is encryption?

Encryption is a process that encodes a message or file so that it can be only be read by certain people.

Encryption uses an algorithm to scramble, or encrypt, data and then uses a key for the receiving party to unscramble, or decrypt, the information. The message contained in an encrypted message is referred to as plaintext. In its encrypted, unreadable form it is referred to as ciphertext.



What is decryption?

Decryption is the process of converting encrypted or encoded data or text back to its original plain format that people computer applications can easily read and comprehend. This is the opposite of encryption which involves coding data to make it unreadable by everyone but only by those with matching decryption keys.

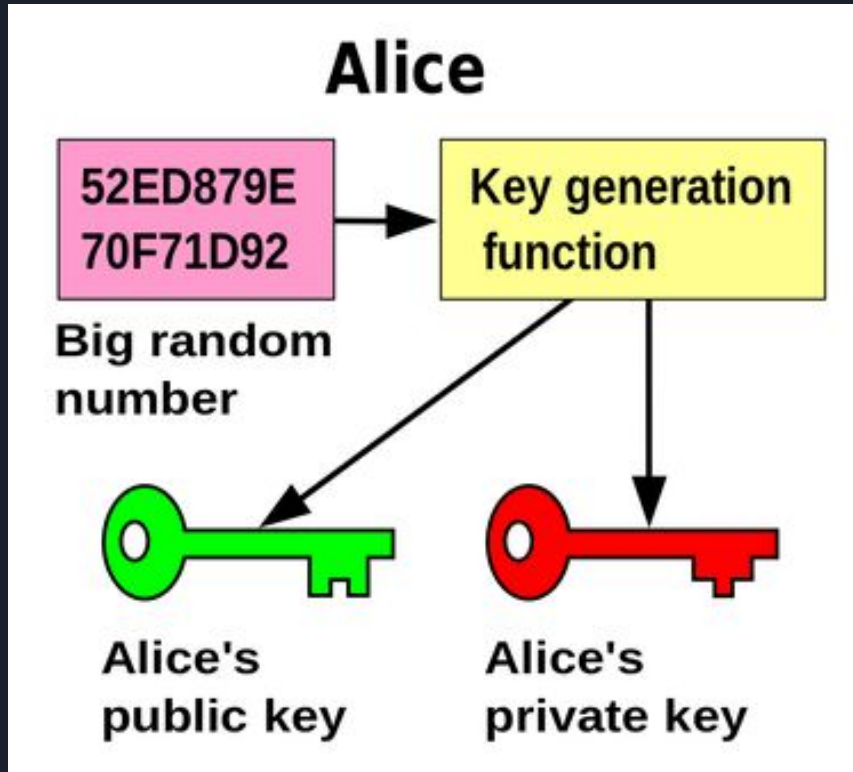


What is public key cryptography?

Public key cryptography is a cryptographic system that uses private/public keys. The advantage of this approach is in not requiring some sort of secure channel for the initial exchange of secret keys between communicators. This makes secure communication with strangers on open networks possible.

The private key is a random hexadecimal number that must be kept private by the account holder.

A public key is another hexadecimal number which can be shared publicly.




In most common encryption systems, the public and private keys are both generated at the same time. In others, the public key is generated from the private key. The public and private keys are associated with each other through a mathematical relationship. However, there is no way use the public key to figure out the private key.



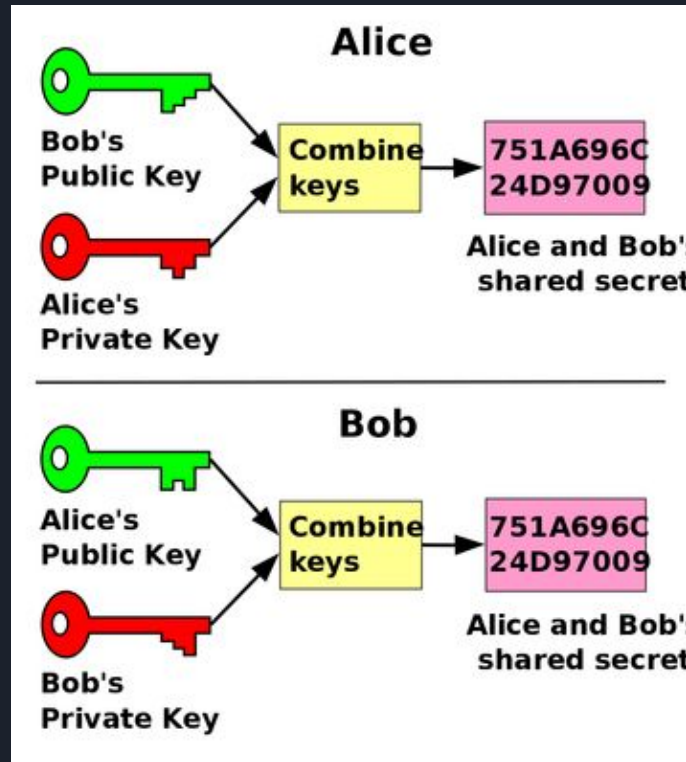
What are digital signatures?

Digital signatures are like electronic “fingerprints.” In the form of a coded message, the digital signature securely associates a signer with a document in a recorded transaction. Digital signatures use a standard, accepted format, called Public Key Infrastructure (PKI), to provide the highest levels of security and universal acceptance. They are a specific signature technology implementation of electronic signature.

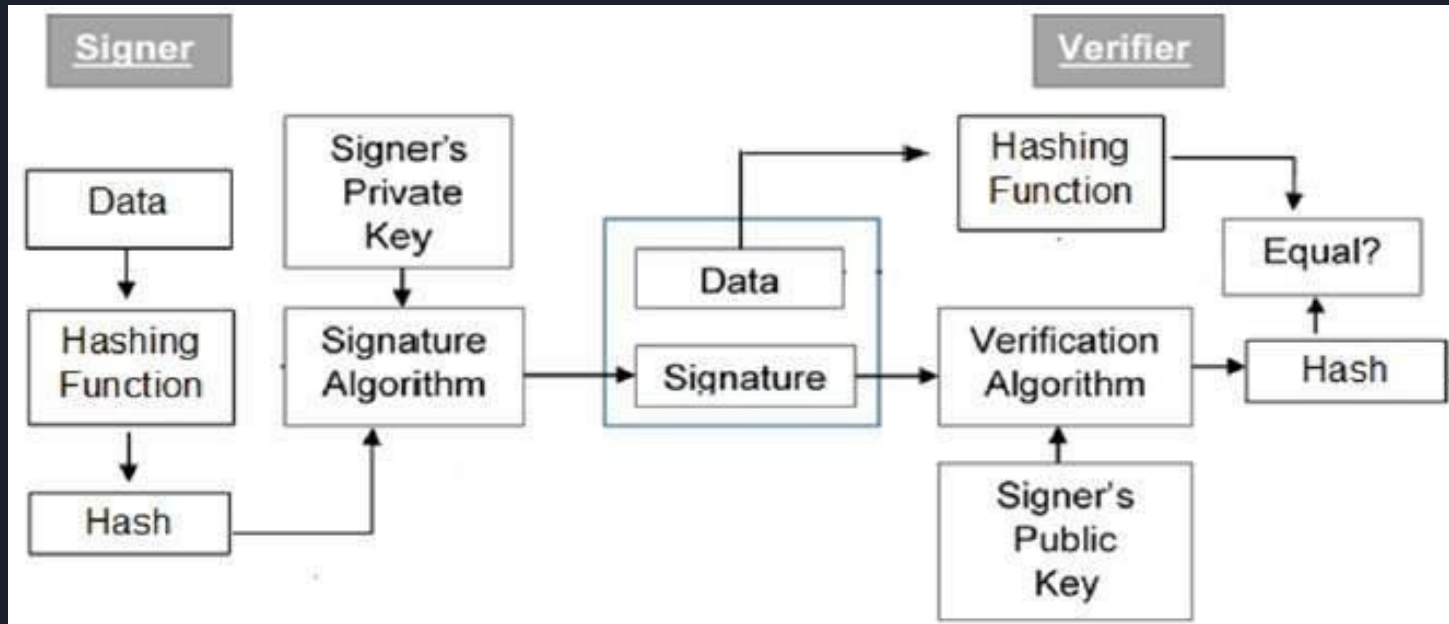


Public key cryptography with digital signatures


A digital signature with public-key cryptography securing a message is created in the following way. First, the message is digitally signed like explained above. Then, this bundle is encrypted with the sender's private key, and again with the receiver's public key



`public_key_of_recipient(private_key(message_hashing(message) + message + type of hashing algorithm))`



Model of Digital Signature: the digital signature scheme is based on public key cryptography.



How addition of digital signature changes the process of public key cryptography

By adding digital signature to public key cryptography, we can create a cryptosystem that can provide the four essential elements of security namely – Privacy, Authentication, Integrity, and Non-repudiation

The background features three overlapping circles of varying shades of gray, creating a layered effect. The circles are positioned on the right side of the frame, with the largest circle being the darkest and the smallest being the lightest. The text "The End" is written in a bold, white, sans-serif font on the left side of the image.

The End