Cryptography

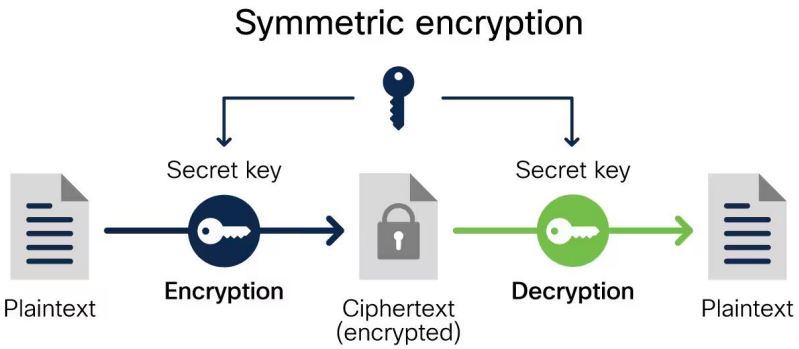
Cryptography

- Cryptography is technique of securing information and communications through use of codes so that only those for whom the information is intended can understand it and process it, thus preventing unauthorized access to information.
- It helps in providing confidentiality, authentication, data integrity, digital signature, etc.

Cryptography

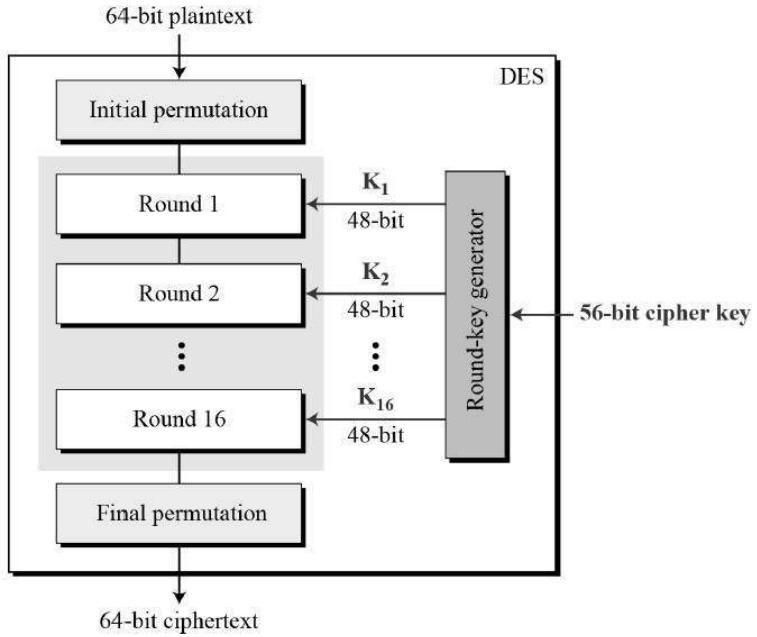
- Terminologies
  - **Plaintext:** the original message
  - **Ciphertext:** the scrambled message
  - **Encipher/encryption**: converting plaintext to cipher text
  - **Decipher/decryption**: recovering plaintext from ciphertext
  - **Cipher:** an algorithm for performing encryption and decryption
  - **Key:** secret information known only to sender/receiver
  - **Cryptanalysis** (code breaking): the study of principles/methods of deciphering ciphertext without knowing key
  - **Cryptology:** the field of both cryptography and cryptanalysis
- There are two types of cryptography
  - Symmetric/Secret Key Cryptography
  - Asymmetric/Public Key Cryptography

Symmetric Key Cryptography

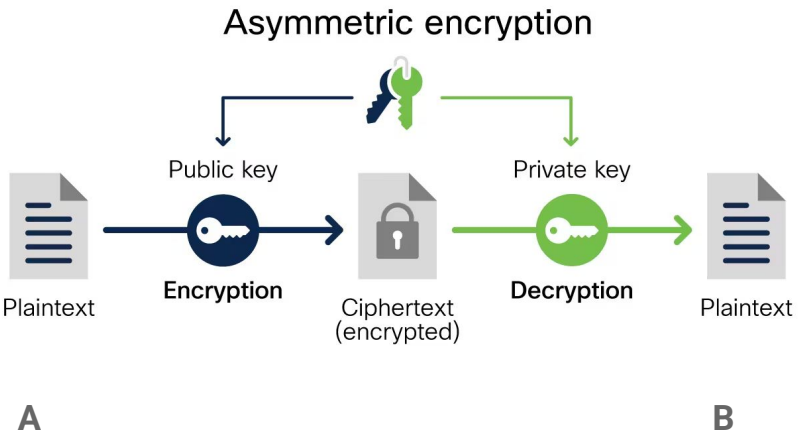


Symmetric Key Cryptography

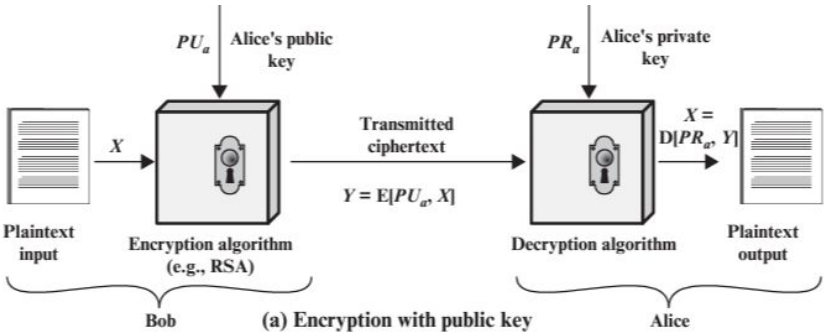
- **Data Encryption Standard (DES):** Developed by IBM (in collaboration with the NSA). Used 56-bits key. It is no longer secure.
- **Triple DES:** An improvement over DES. Has effective key length of 112-bits
- **Advanced Encryption Standard(AES):** Originally named Rijndael. Was chosen in 2001 as the winner of a 5-year-long contest.
  It is an iterated block cipher with 10, 12, or 14 rounds for key sizes 128, 192, and 256 bits, respectively.

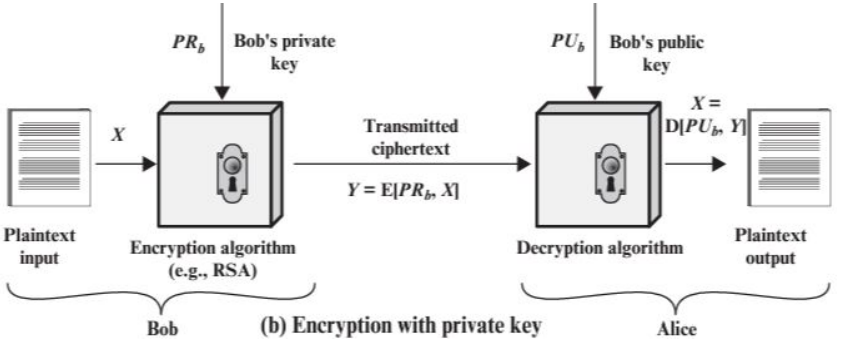


Asymmetric Key Cryptography

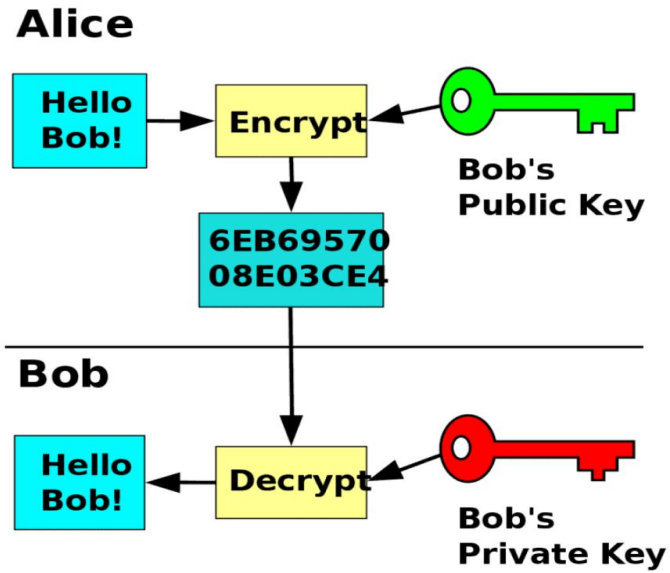


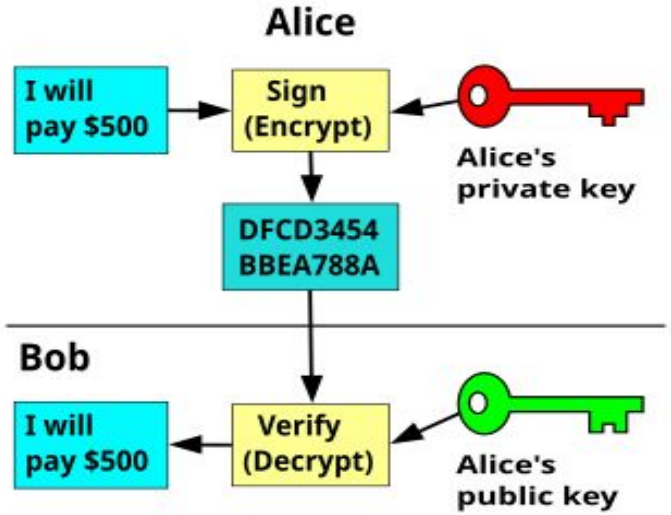
Asymmetric Key Cryptography





Asymmetric Key Cryptography





Asymmetric Key Cryptography

- Asymmetric Key Ciphers are based on mathematical hard problems. These are mathematical functions that are easy to perform but difficult to reverse.
- **RSA** : Developed by Rivest-Shamir-Adelman. Uses Prime Factorization and Discrete Log Problems.
- **Elliptic Curve Cryptography:** Uses Elliptic Curve Discrete Log Problem

Block Ciphers and Stream Ciphers

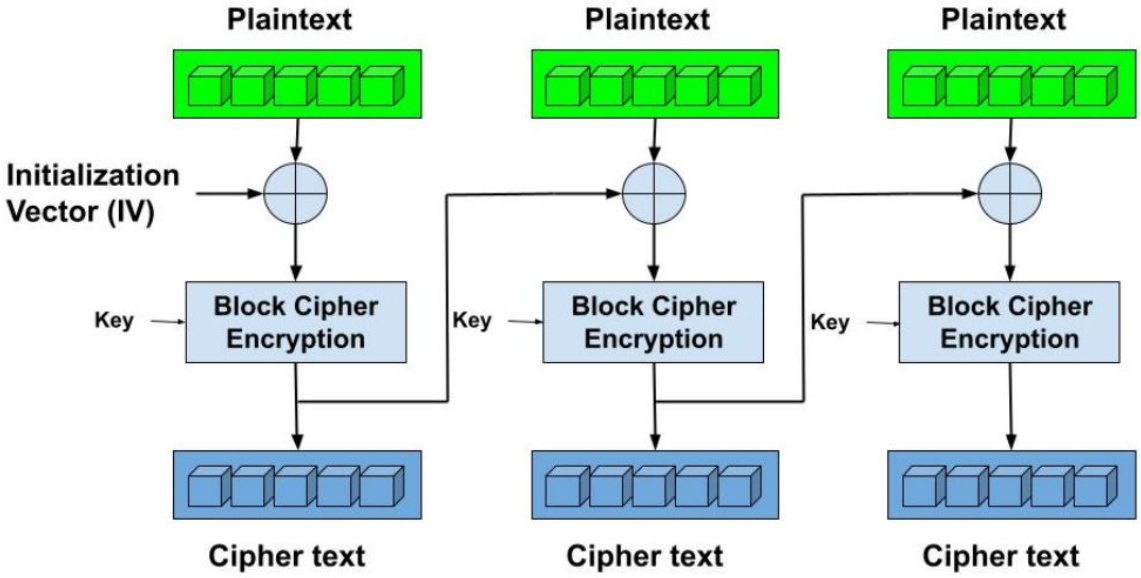
Block Ciphers

- In Block Ciphers, the plaintext is split into fixed size chunks called Blocks, and each block is encrypted separately
- Typically all blocks in the plaintext are encrypted using the same key
- Examples: DES, AES, RSA, ECC

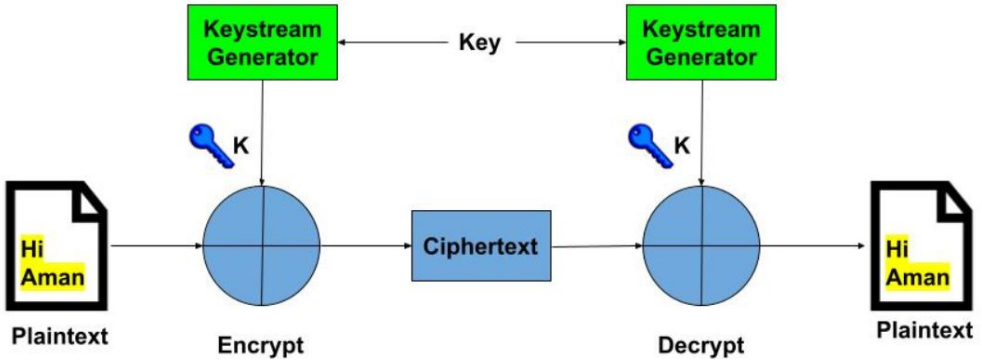
Stream Ciphers

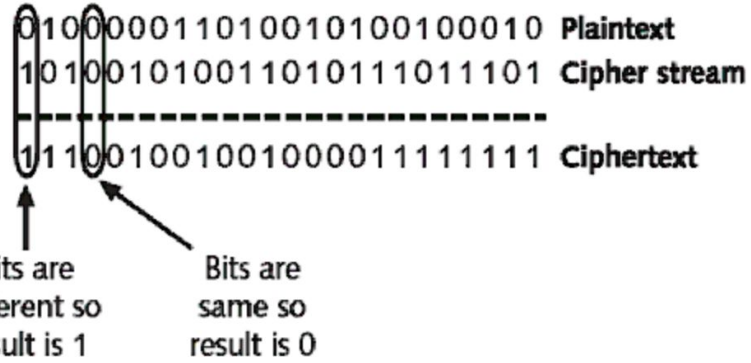
- Stream ciphers operate on bits
- Typically generate a pseudo-random keystream as a function of a fixed length key and per-message bit string
- Faster than block ciphers
- Example: RC4, ChaCha, Salsa20

Block Ciphers



Stream Ciphers





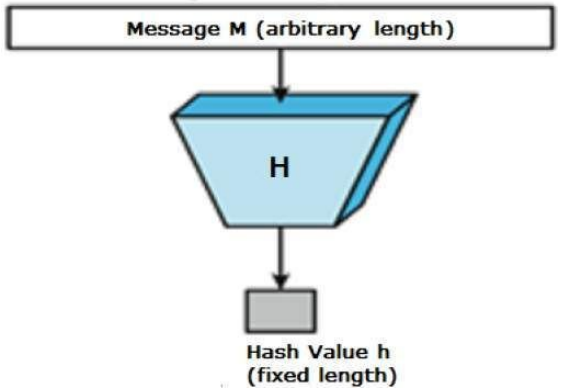
Attacks on Cryptographic Algorithms

- A Cryptanalyst may try to
    - Obtain the corresponding plaintext from a given ciphertext
    - Deduce the secret key or the private key

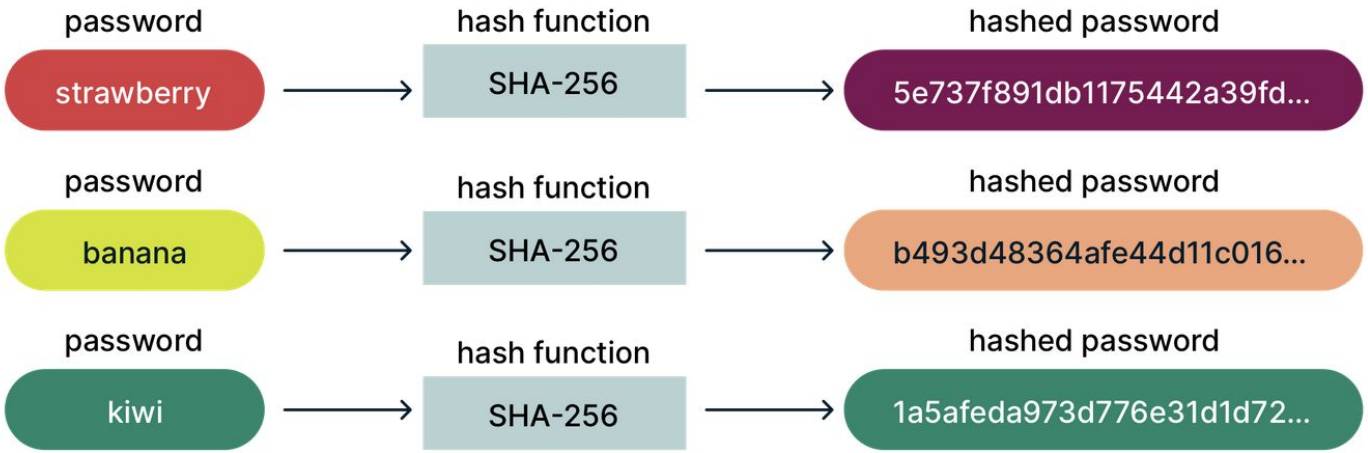
- Types of attacks
    - **Known Ciphertext Attacks:** Attacker collects large amounts of ciphertext and looks for pattern in an attempt to reconstruct some plaintext and/or deduce the key
    - **Known Plaintext Attacks:** Here attacker knows all or parts of the plaintext. Using the plaintext-ciphertext pairs, the attacker tries to deduce the key.
    - **Chosen Plaintext Attacks:** An attacker carefully choses a plaintext and obtains its ciphertext.

Hashing

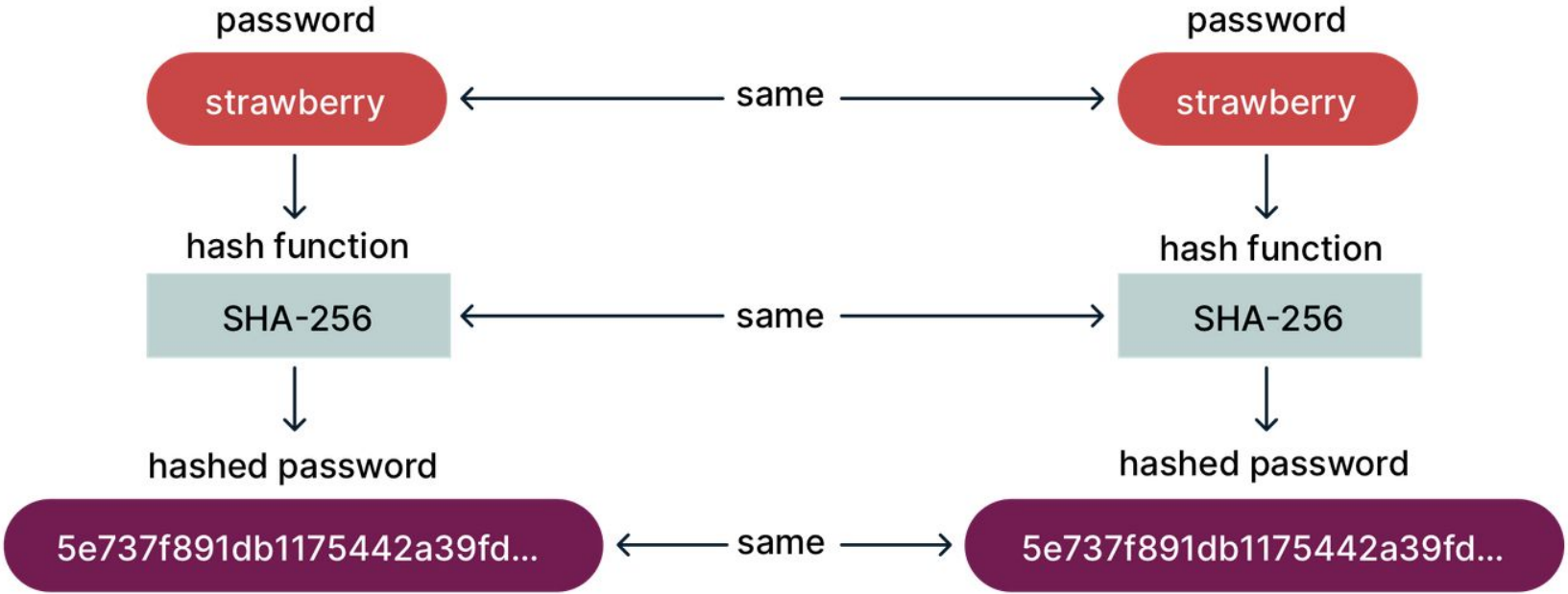
- Uses one-way functions.
- Examples: MD5, SHA-1, SHA-2
- Properties of Hash Functions
    - **Preimage Resistance**: It should be impossible to derive the original input from a given hash
    - **Second Preimage Resistance:** Given an input and its hash, it should be hard to find another input with the same hash
    - **Collision Resistance:** It should be hard to find two different inputs of any length that result in the same hash



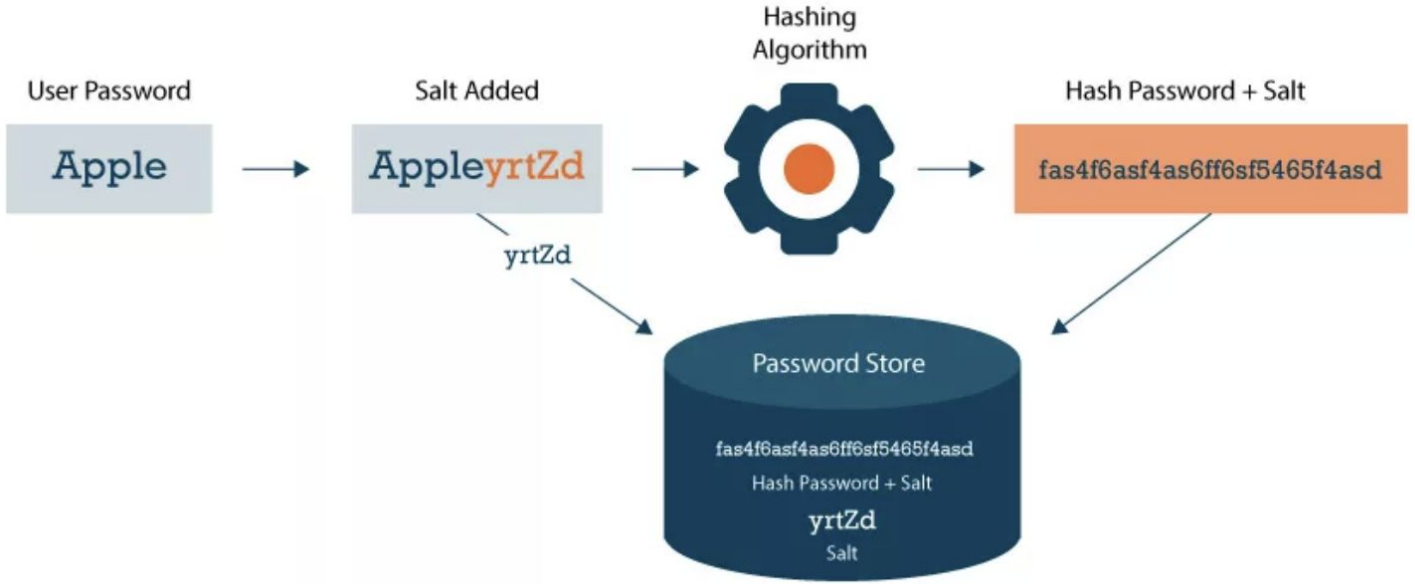
Hashing


password
hash function
hashed password
strawberry
SHA-256
5e737f891db1175442a39fd...
password
hash function
hashed password
banana
SHA-256
b493d48364afe44d11c016...
password
hash function
hashed password
kiwi
SHA-256
1a5afeda973d776e31d1d72...

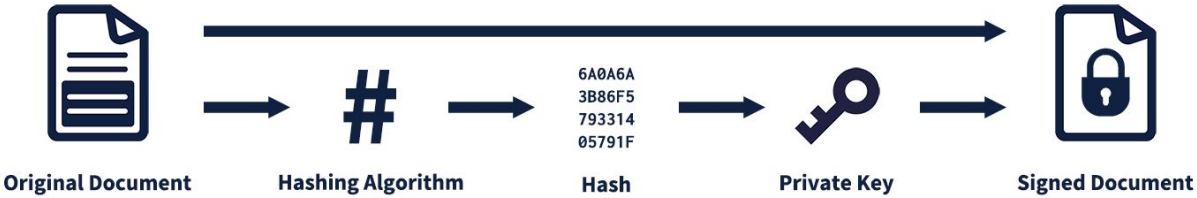
Hashing


password
strawberry
same
password
strawberry
hash function
SHA-256
same
hash function
SHA-256
hashed password
5e737f891db1175442a39fd...
same
hashed password
5e737f891db1175442a39fd...

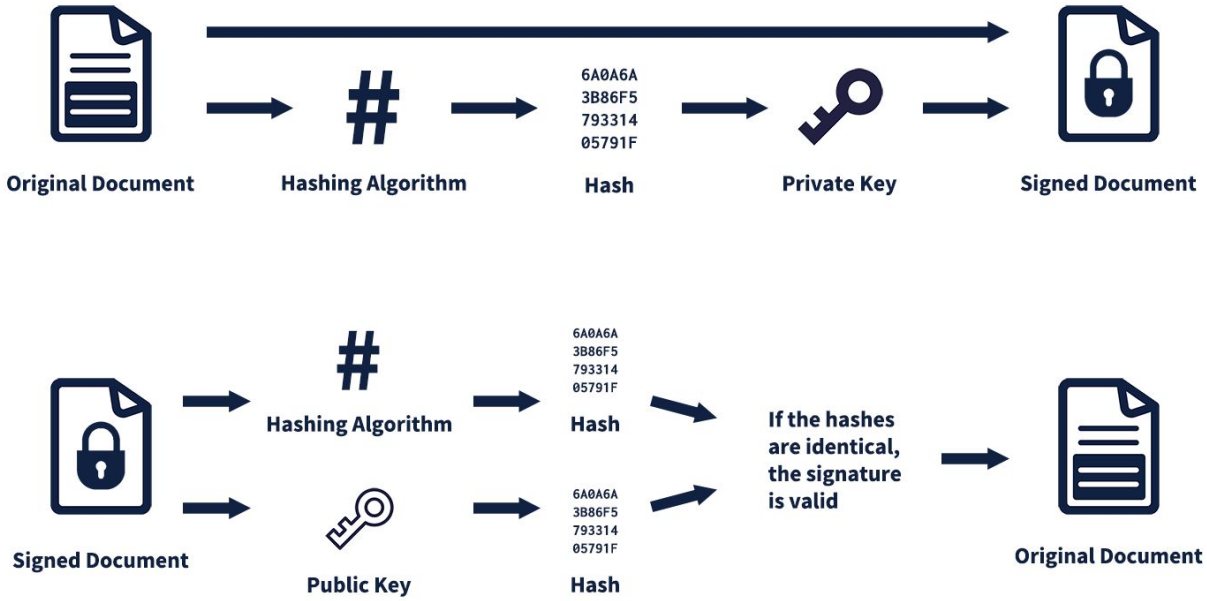
Hashing with Salt



Digital Signatures



Digital Signatures

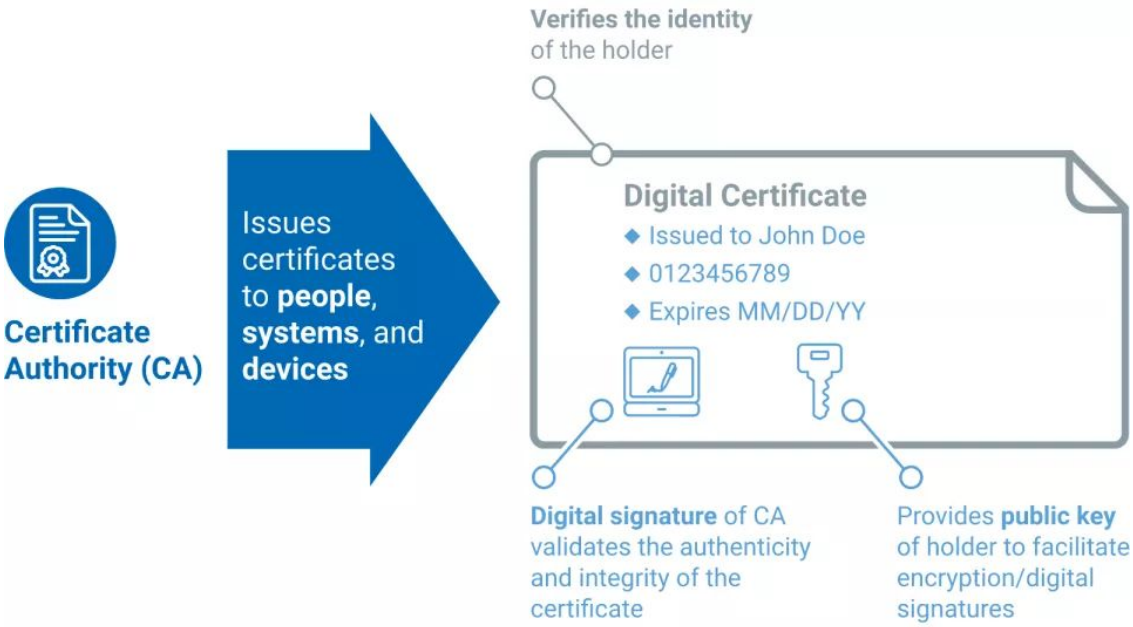


Digital Signatures

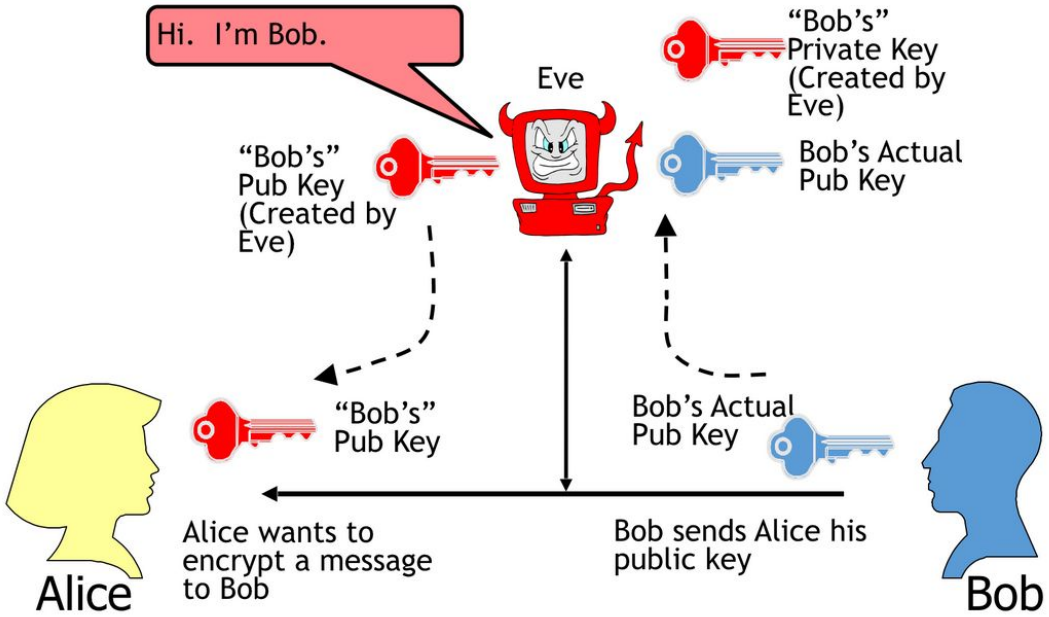
- Digital signatures make signature dependent on the document being signed
- Combines Hashing and Public-key Cryptography
- They provide
  - Data Integrity
  - Source Integrity (Authentication)
  - Non-repudiation

Digital Certificate

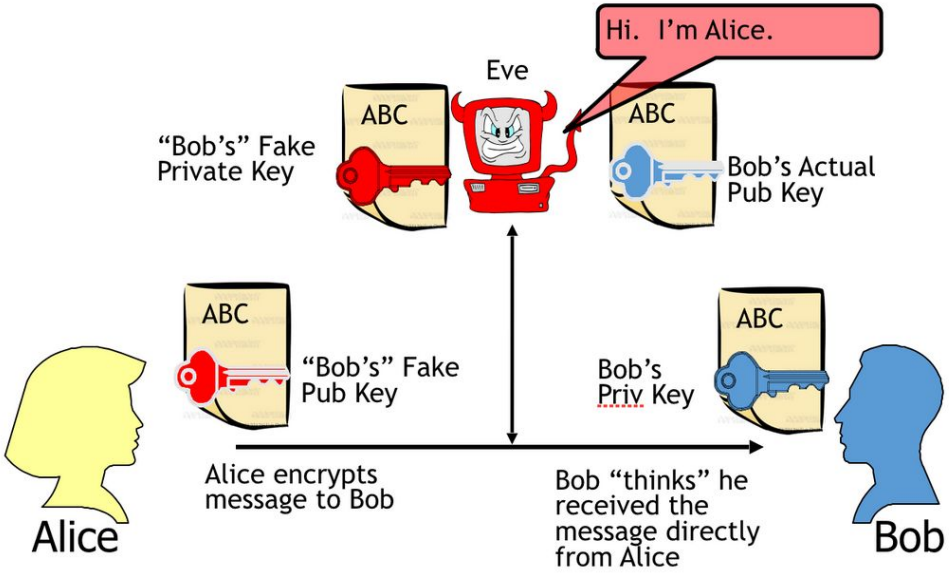
Digital Certificate



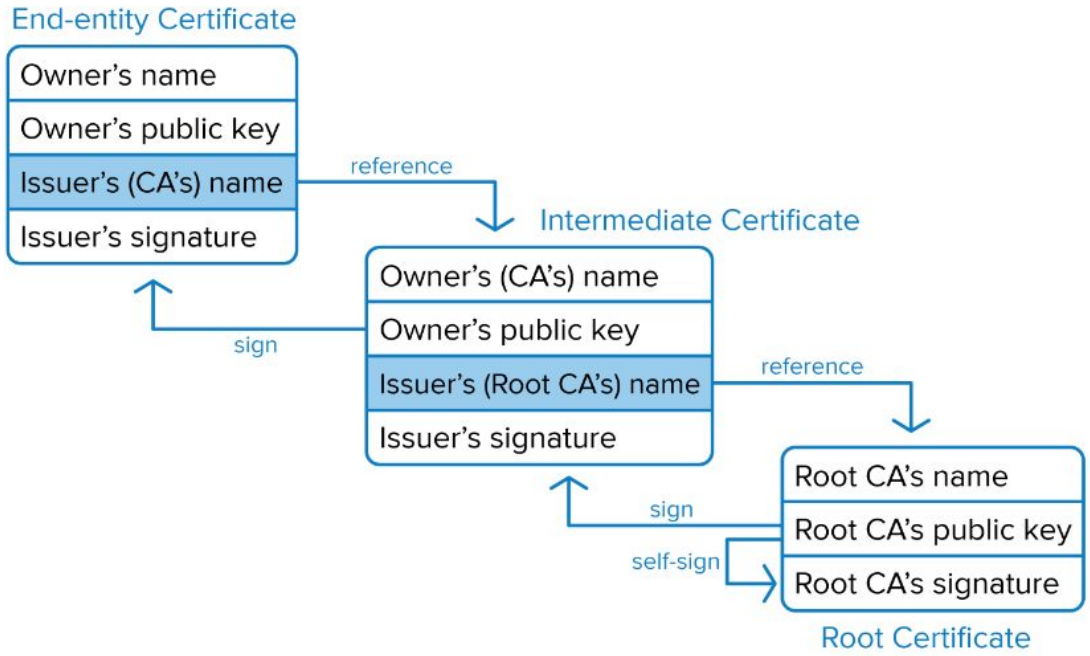
Man-in-the-middle Attack



Man-in-the-middle Attack

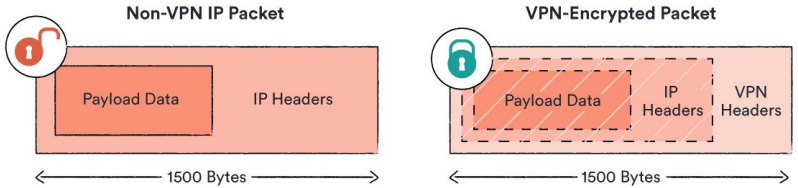


Digital Certificate Verification



Virtual Private Network (VPN)

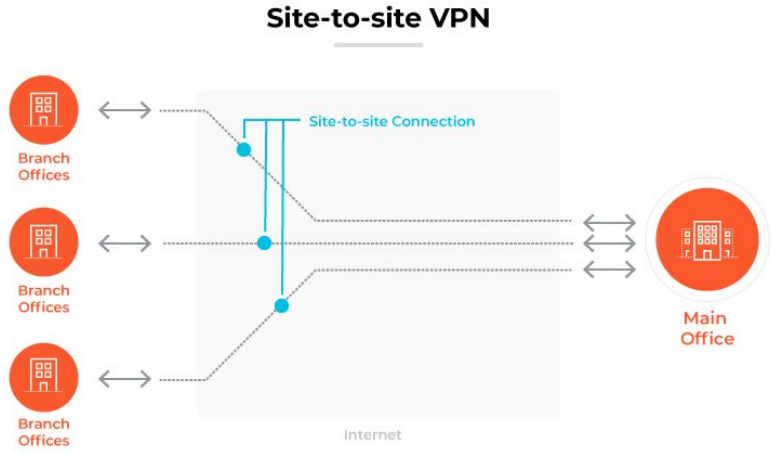
- A VPN creates a hidden tunnel within an unprotected network and secures user's internet activity
- Internet Protocol Security (IPSec) is a set of protocols that is generally used to set up VPNs

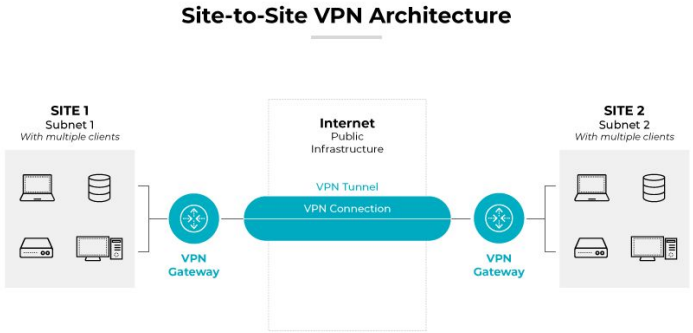


https://www.top10vpn.com/vpn-explained/

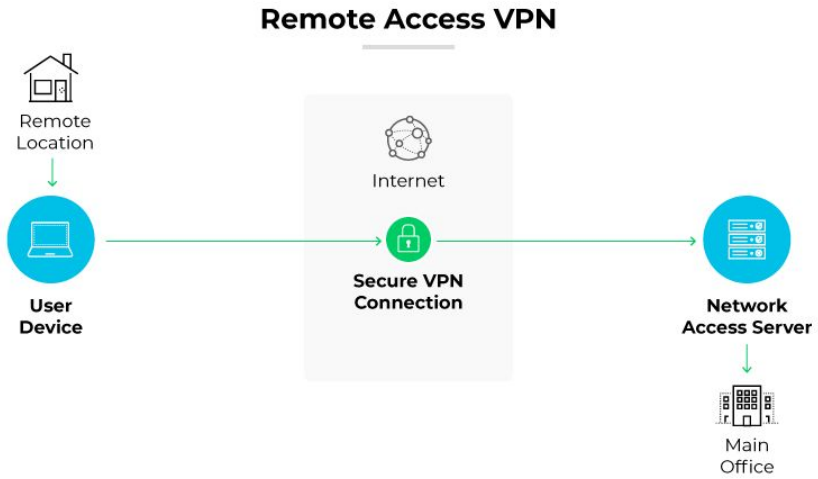
Site-to-site VPN

- Establishes a link between two or more networks

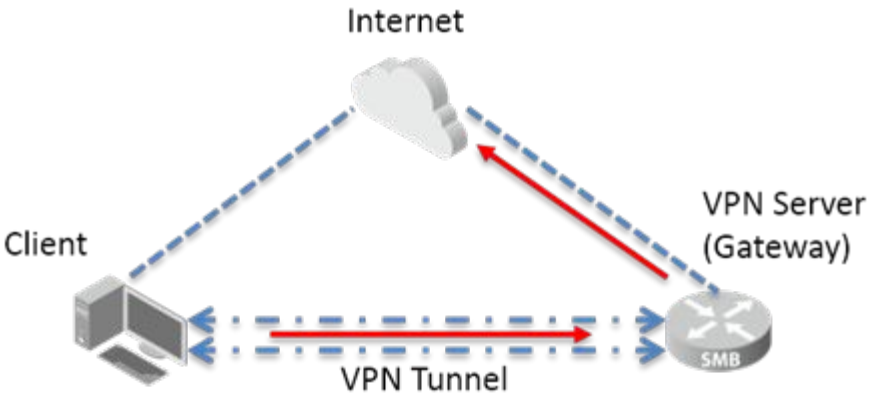




Client/Remote Access VPN

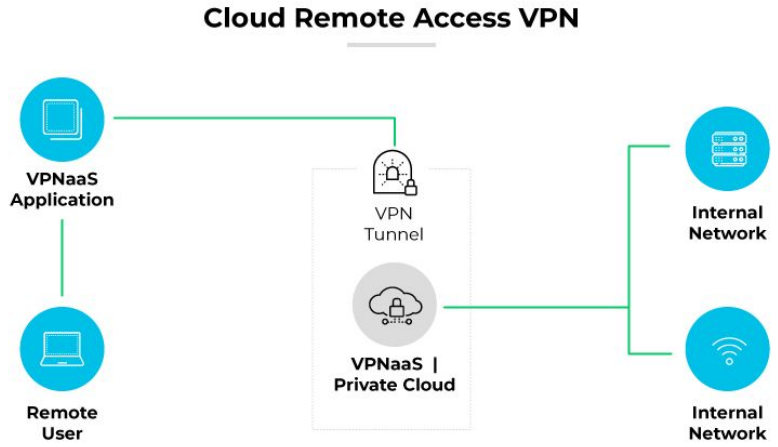


Server Access VPN



Cloud VPN

- Creates an encrypted VPN connection over the internet between a user and the company's network infrastructure hosted in the cloud



Virtual Private Network (VPN)

Types of VPN

- Site-to-site VPN
- Remote-site VPN
- Server Access VPN
- Cloud VPN

Advantages

- Enhances Security
- Convenience
    - Allows use of resources inside the private network
- Anonymity

References

1. https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c01.pdf
2. https://www.cisco.com/c/en/us/products/security/encryption-explained.html
3. https://www.cs.cornell.edu/courses/cs5430/2010sp/TL03.symmetric.html
4. https://learn.microsoft.com/en-us/azure/iot-hub/reference-x509-certificates
5. https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/