Encryption

Cyber Security Foundation Course

AGENDA

- Definition
- Encryption types
- Symmetric Encryption
- Asymmetric Encryption
- Asymmetric Vs symmetric
- Digital Certificate
- How HTTPS/SSL Works

Definition

“encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information” wikipedia.org

Encryption Types

There are two types of encryption: symmetric and asymmetric encryption.

Symmetric Encryption: use one key for Both encryption and Decryption.

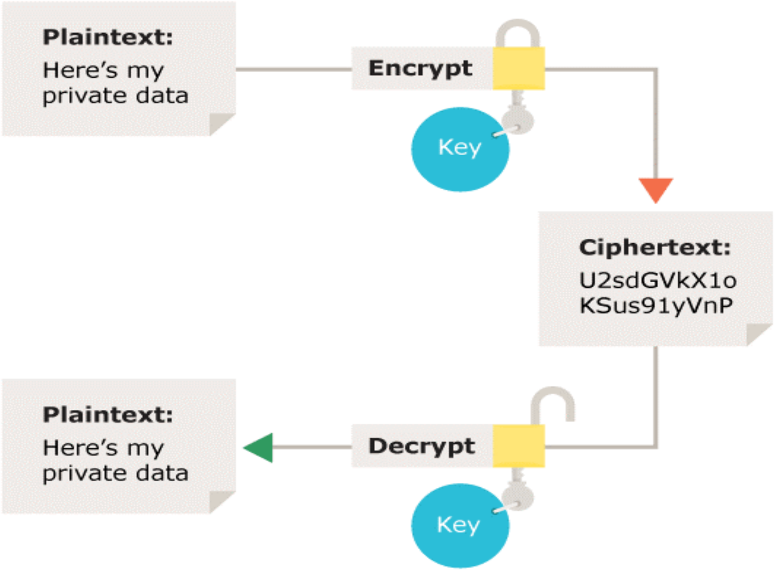
Asymmetric Encryption: Use Two Keys on known as the private key and the other is known as the public key, The private key is kept secret by it’s owner and the public key is shared with the other side. So Data encrypted with the recipient’s public key can only be decrypted with the recipient’s private key.

Symmetric Encryption

As previously shown the Symmetric Encryption is a one key for both Encryption and Decryption, which mean the both sides must Exchange the Secret Key through insecure Channel !

Examples:

AES (Advanced Encryption Standard): The most commonly symmetric algorithm in use, the AES cipher has a block size of 128 bits, but can have three different key lengths : AES-128, AES-192 and AES-256.

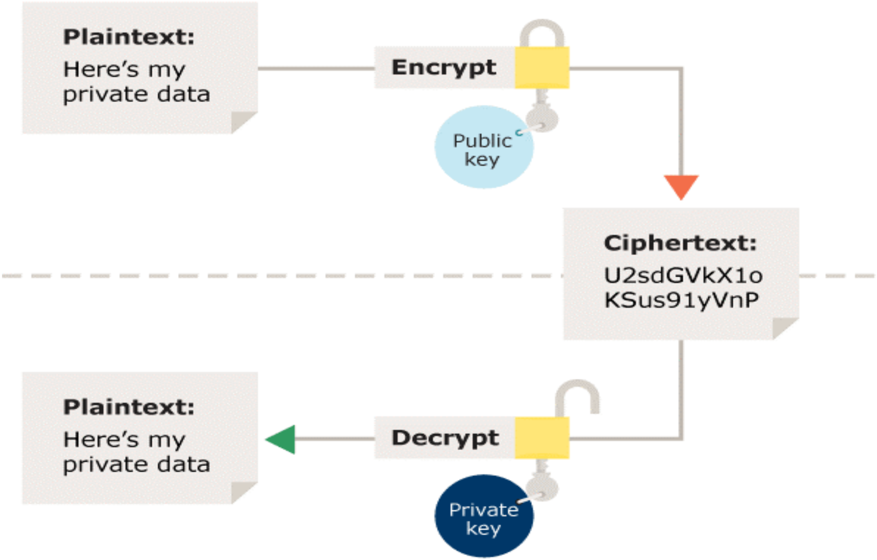


Asymmetric Encryption

Mostafa want to send a message to Menna, so Menna will send her Public Key to Mostafa to Encrypt the Message and only Menna's Private Key can decrypt its.

Examples:

RSA (Asymmetric Encryption Algorithm): The most commonly Asymmetric algorithm in use, encryption key lengths such as 768-bit, 1024-bit, 2048-bit, 4096-bit.



Asymmetric Vs Symmetric

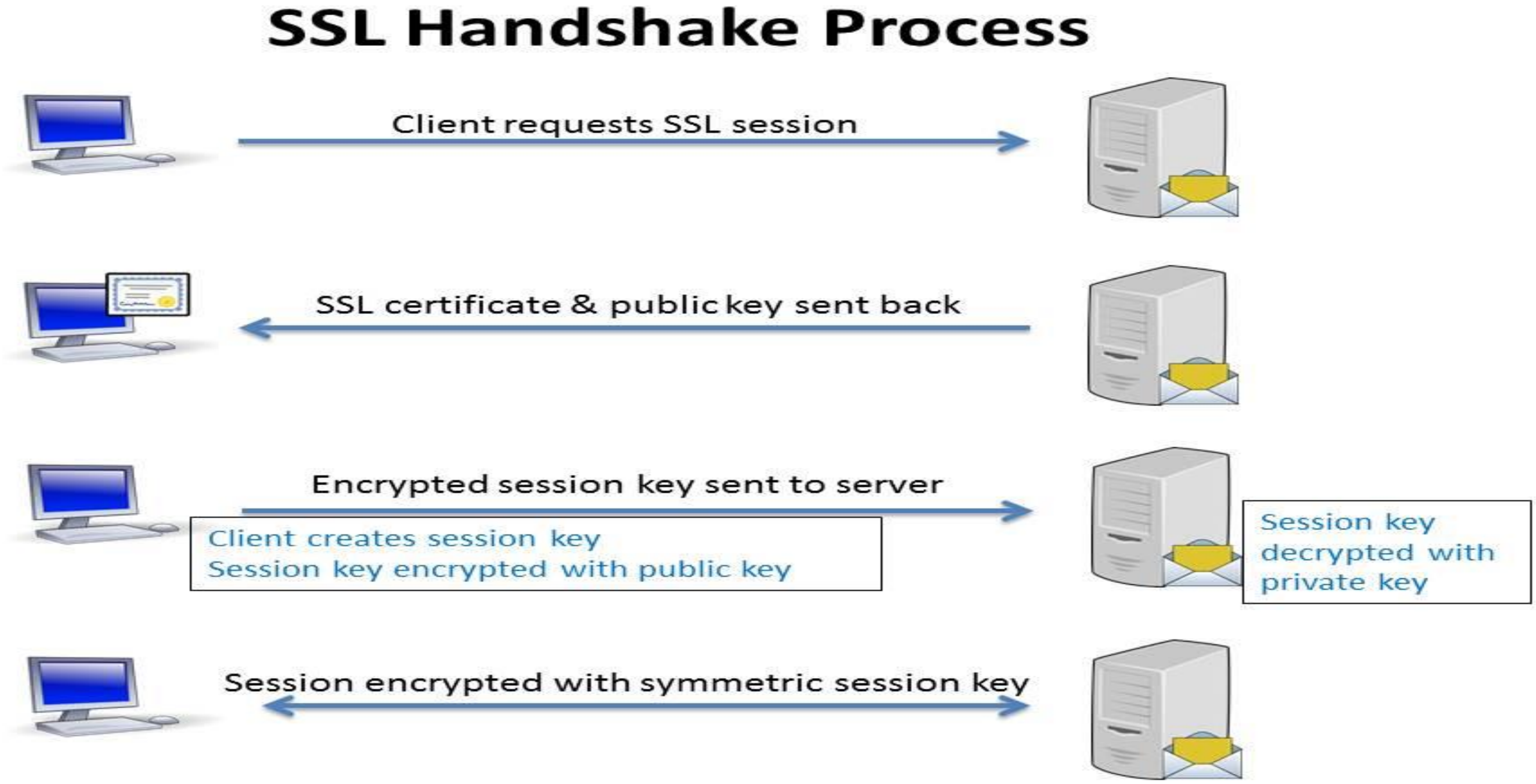
Symmetric	Asymmetric
A single key is used to encrypt and decrypt data.	pair of keys are used to encrypt and decrypt data.
faster and requires less computational power	slower and requires higher computational power
Smaller key lengths	longer keys lengths
RC4, AES, DES, 3DES, and QUAD.	RSA, Diffie-Hellman, ECC, El Gamal, and DSA.

Digital Certificate

“used to prove the ownership of a public key. The certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer)” wikipedia.org

Certificate Authority CA: is an Organization that issues and Validate the digital **certificates**

Hybrid Encryption: How HTTPS/SSL Works



SSL Handshake Process

Client requests SSL session

SSL certificate & public key sent back

Encrypted session key sent to server

Client creates session key
Session key encrypted with public key

Session key decrypted with private key

Session encrypted with symmetric session key

Thanks!

Any questions?