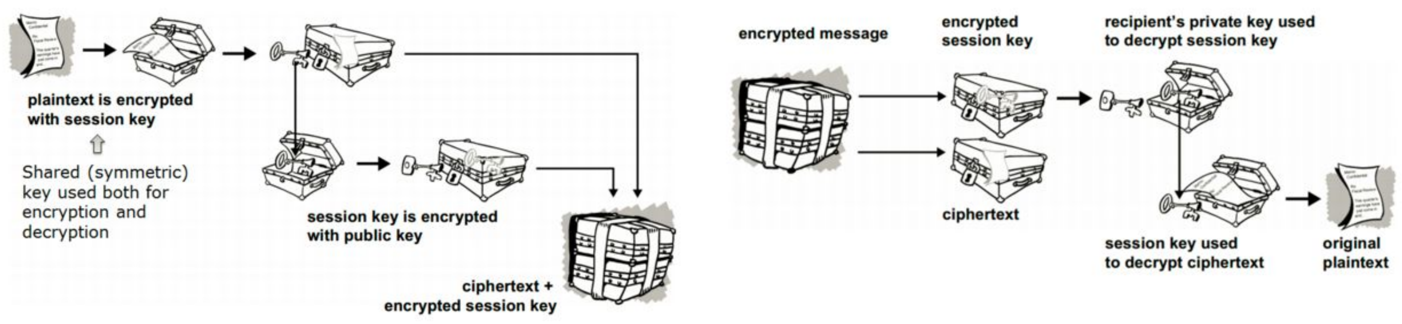
1. **Explain basic security terms like authentication, authorization, confidentiality, integrity, SSL/TLS and provide examples of how you have used them.**
    a. **Authentication** - Confirming the identity of a client (via some kind of login procedure)
    b. **Authorization -** Determining whether an authenticated client is allowed to receive a service or perform an operation
    c. **Confidentiality** - Protection from disclosure to unauthorised persons
    d. **Integrity** - Maintaining data consistency (data cannot be modified)
    e. **SSL/TLS -** the green chainlock in the browser
        i. ***Symmetric Key Encryption*** - An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. Contrast this with public-key cryptology, which utilizes two keys - a public key to encrypt messages and a private key to decrypt them. Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way. Public-key encryption avoids this problem because the public key can be distributed in a non-secure way, and the private key is never transmitted.
        ii. ***Public Key Encryption*** - A cryptographic system that uses two keys -- a public key known to everyone and a private or secret key known only to the recipient of the message. When John wants to send a secure message to Jane, he uses Jane's public key to encrypt the message. Jane then uses her private key to decrypt it.An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key.
            1. Public-key systems, such as Pretty Good Privacy (PGP), are becoming popular for transmitting information via the Internet.

Exemplified with Pretty Good Privacy (PGP)

Encryption

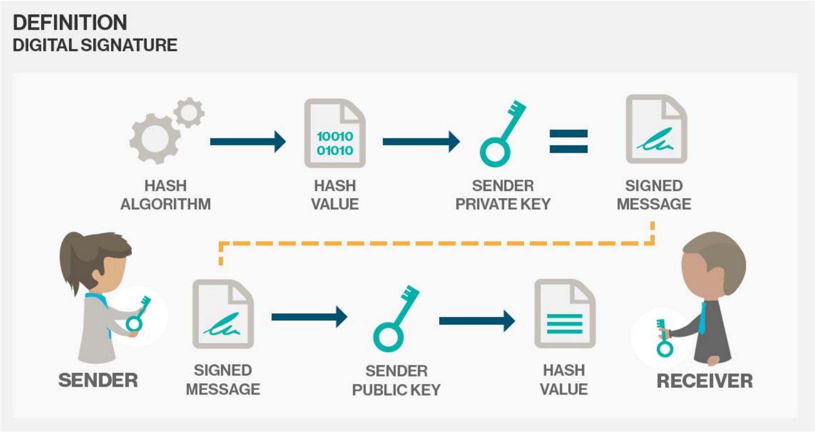
Decryption


plaintext is encrypted with session key
Shared (symmetric) key used both for encryption and decryption
session key is encrypted with public key
ciphertext + encrypted session key
encrypted message
encrypted session key
recipient's private key used to decrypt session key
ciphertext
session key used to decrypt ciphertext
original plaintext

They are extremely secure and relatively simple to use. The only difficulty with public-key systems is that you need to know the recipient's public key to encrypt a message for him or her. What's needed, therefore, is a global registry of public keys, which is one of the promises of the new LDAP technology.

iii. **Digital signature** - a mathematical technique used to validate the authenticity and integrity of a message, software or digital document

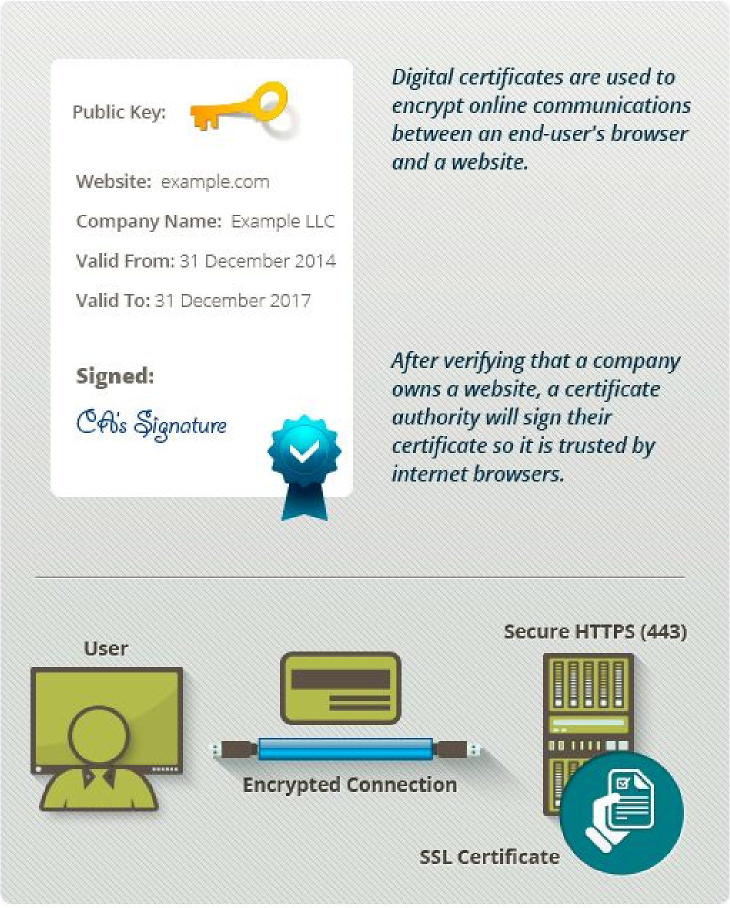
1. ***Signing a Digest*** - Signing the whole document is slow, and produces an enormous volume of data—at least double the size of the original information



   a. An improvement is to sign only a digest of the message using a one-way hash function in the process
   b. A one-way hash function takes variable-length input—in this case, a message of any length, even thousands or millions of bits—and produces a fixed-length output; say, 160-bits.
   c. The hash function ensures that, if the information is changed in any way—even by just one bit—an entirely different output value is produced

iv. **Digital certificate -** A digital certificate is data that functions much like a physical certificate. A digital certificate is information included with a person’s public key that helps others verify that a key is genuine or valid.A digital certificate consists of three things:

1. A public key.
2. Certificate information. (“Identity” information about the user, such as name, user ID, and so on.
3. One or more digital signatures



Public Key:

Website: example.com

Company Name: Example LLC

Valid From: 31 December 2014

Valid To: 31 December 2017

Signed:

CA's Signature

Digital certificates are used to encrypt online communications between an end-user's browser and a website.

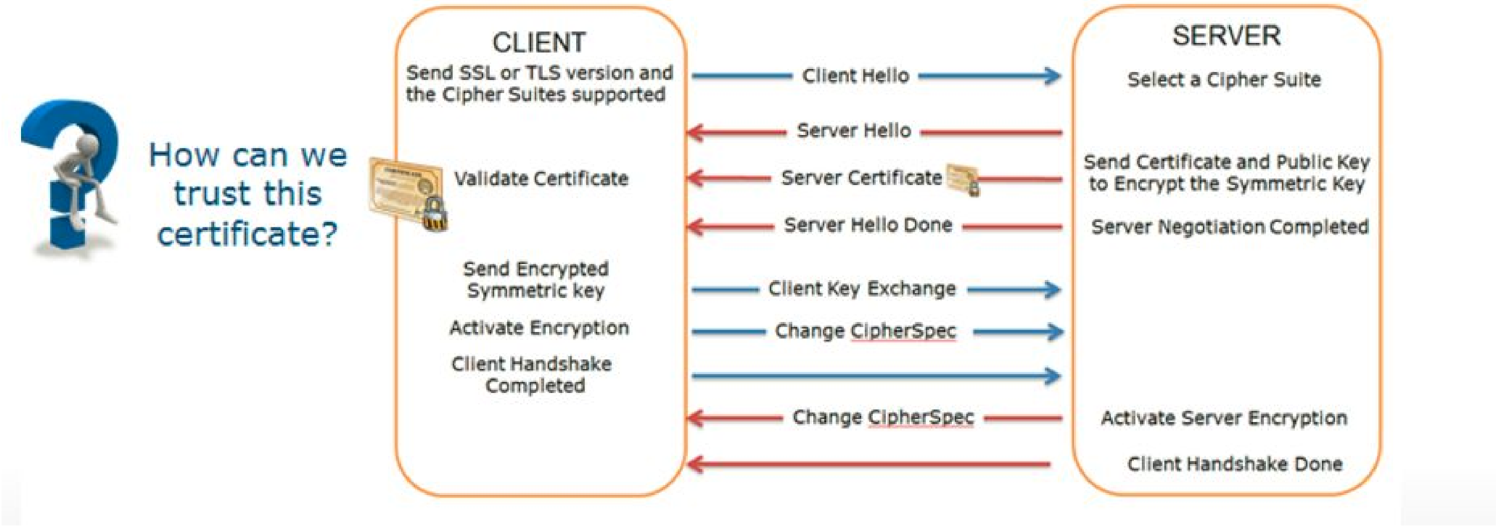
After verifying that a company owns a website, a certificate authority will sign their certificate so it is trusted by internet browsers.

v. **Public key Infrastructure - Hierarchical Trust**

1. A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates[1] and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.

vi. How it is all combined to provide a secure TLS connections

1. TLS includes two layers
   a. A Record Protocol and a Handshake Protocol, and these are layered above a transport protocol such as TCP/IP.
   b. They both use asymmetric and symmetric cryptography techniques



How can we trust this certificate?

CLIENT

Send SSL or TLS version and the Cipher Suites supported

Validate Certificate

Send Encrypted Symmetric key

Activate Encryption

Client Handshake Completed

Client Hello

Server Hello

Server Certificate

Server Hello Done

Client Key Exchange

Change CipherSpec

Change CipherSpec

SERVER

Select a Cipher Suite

Send Certificate and Public Key to Encrypt the Symmetric Key

Server Negotiation Completed

Activate Server Encryption

Client Handshake Done

vii.