Cryptography and Network Programming

Suren Hakobyan

AUA

March 17, 2025

Outline

1. Introduction
2. Symmetric Ciphers
3. Asymmetric Ciphers
4. Digital Certificates
5. SSL

Introduction

Definition

Cryptography is a technique of securing information and communications through the use of codes so that only those persons for whom the information is intended can understand and process it.

There are four main goals of cryptography:

- Confidentiality
- Data Integrity
- Authentication
- Non-Repudiation

Terminology

- **plaintext** - the original message
- **ciphertext** - the coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering plaintext from ciphertext

Symmetric Ciphers

Definition

Symmetric Cipher (Single-Key Encryption) is a cipher which only uses one key for the process of both the encryption and decryption of data.

Examples:

- **Substitution Ciphers** (Ceasar Cipher)
- **Transposition Ciphers** (Row Transposition Cipher)

Modern secure symmetric cipher: **AES**

Assymetric Ciphers

Definition

Asymmetric Cipher (public-key cryptography) is a type of cipher that uses a pair of keys to encrypt and decrypt data. The pair of keys includes a **public key**, which can be shared with anyone, and a **private key**, which is kept secret by the owner.

- **public key** - used to **encrypt messages**, and **verify signatures**.
- **private key** - used to **decrypt messages**, and **sign signatures**.

Very popular and secure assymetric cipher: **RSA**

RSA - Setup

Procedure

1. Take two large prime random numbers p and q.
2. Compute the system modulus $N = p \times q$.
3. Compute $\phi(N) = (p-1) \times (q-1)$.
4. Choose a random e such that $1 < e < \phi(N)$ and $\gcd(e, \phi(N)) = 1$.
5. Solve $e \times d = 1 \mod \phi(N), 0 \leq d \leq N$.

Result:

- **public key**: $K_{pu} = \{e, N\}$, provide this to others.
- **private key**: $K_{pr} = \{d, p, q\}$, keep this a secret.

RSA - Usage

Procedure

Given a message M and public key information $\{e, N\}$, the cipher C is determined by:

$$C = M^e \mod N$$

Given a cipher C, private key information d and system modulus N, the message M is determined by:

$$M = C^d \mod N$$

So, one uses the recipient's public key to encrypt data and the recipient uses their own private key to decrypt the data.

RSA - Proof

Why RSA works?

Proof

$$\left(C^d = (M^e)^d = M^{e \times d} = M^{1+k \times \phi(N)} = M\right) \mod N$$

Notes:

- Remember that $e \times d = 1 \mod \phi(N)$.
- Remember a result from Euler's Theorem: $a^{\phi(N)+1} = a \mod N, \forall a$.

RSA - Key Considerations

- RSA is based on the fact that it is trivially easy to calculate N but very hard to factorize it.
- p and q have to be sufficiently large so that it is infeasible to determine them from N.

Digital Signatures

Definition

A **Digital Signature** is a mathematical technique used to validate the authenticity and integrity of a message.

Very popular and secure digital signature: **DSA**

DSA - Setup

Procedure - Universal

1. Choose a random prime number q.
2. Choose a prime p such that $p-1$ is a multiple of q.
3. Calculate $g = h^{\frac{p-1}{q}} \mod p$, where h is a random number.

Procedure - Individual

1. Generate a random integer x such that $0 < x < q$.
2. Compute $y = g^x \mod q$.

Result:

- Universally known constants in the system: (p, g, q).
- **public key**: y, provide this to others.
- **private key**: x, keep this a secret.

DSA - Usage

Procedure - Signing

Given a message M:

1. Generate a random $k < q$.
2. Compute $r = \left(g^k \mod p\right) \mod q$.
3. Compute $s = \left(k^{-1} \times (H(M) + x \times r)\right) \mod q$.
4. Send the pair (r, s) alongside M.

Procedure - Verifying

Given message M and the pair (r, s):

1. Compute $w = s^{-1} \mod q$.
2. Compute $u_1 = (H(M) \times w) \mod q$.
3. Compute $u_2 = (r \times w) \mod q$.
4. Compute $v = (a^{u_1} \times y^{u_2} \mod p) \mod q$.
5. The signature is valid iff $v = r$.

DSA - Proof

Why DSA works?

Proof

$$\begin{aligned}((g^{u_1} \times y^{u_2} &= g^{H(M)\times s^{-1}} \times g^{x\times r\times s^{-1}} \\ &= g^{(H(M)+x\times r)\times s^{-1}} \\ &= g^k = r) \mod p) \mod q\end{aligned}$$

Notes:

- $(k^{-1} \times (H(M) + x \times r) = s) \mod p$

DSA - Key Considerations

- DSA is a tool for authentication, while RSA is a tool for encryption.
- RSA and DSA can be used together to provide both secrecy and identification mechanisms. This is achieved by first signing the message, and then encrypting both the message and the signature.
- RSA alone can also act as a authentication mechanism $(H(M)^d)$.

Digital Certificates

Definition

Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender. A digital certificate is a certificate issued by a **Certificate Authority** (CA) to verify the identity of the certificate holder. Digital certificate is used to attach public key with a particular individual or an entity.

SSL

Definition

Secure Sockets Layer (SSL) is an Internet security service that encrypts data to keep it safe. It subsequently became Internet standard known as **TLS (Transport Layer Security)**.

SSL has four main protocols:

- **Handshake Protocol** - used to establish connections.
- **Record Protocol** - used to process and send data.
- **Change-Cipher Protocol** - used to notify that the handshake is done.
- **Alert Protocol** - used to inform about unexpected events.

SSL - Architecture

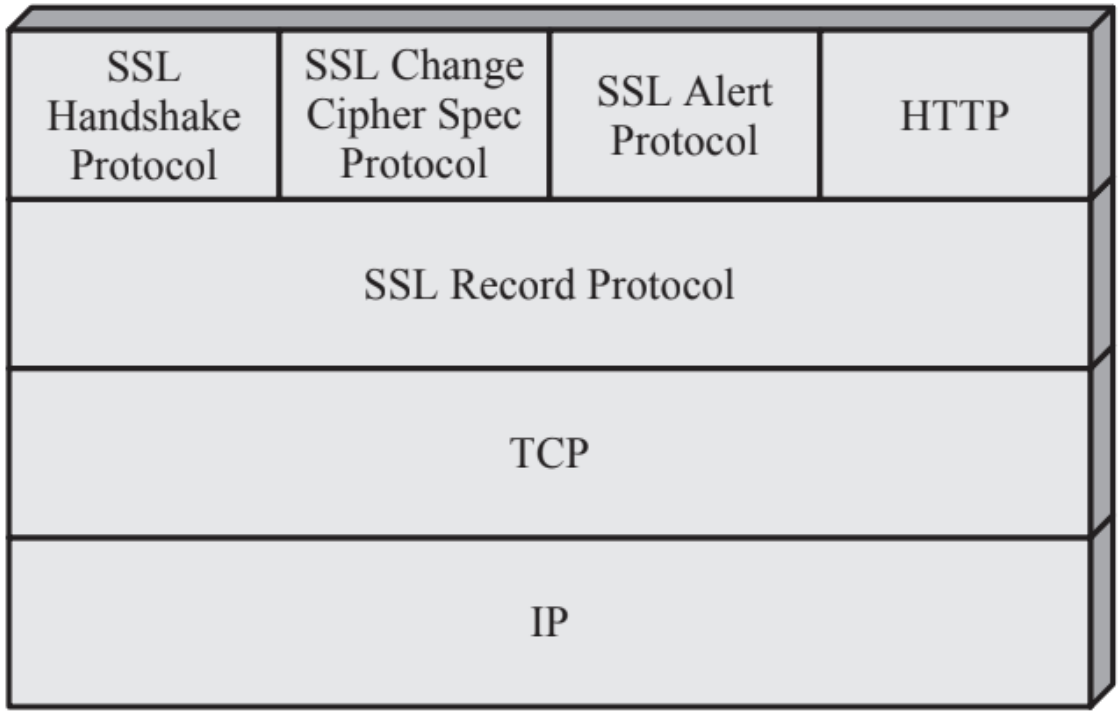

Figure: SSL Architecture

SSL - Handshake Protocol

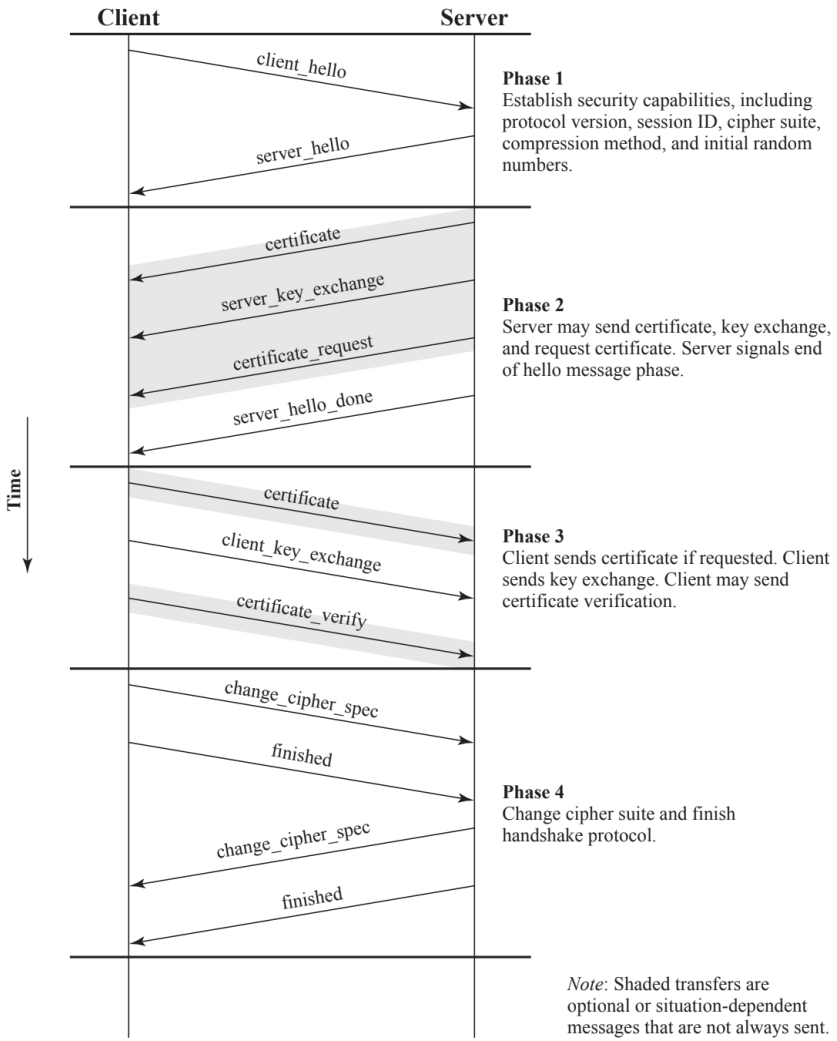

Figure: SSL Handshake Protocol

SSL - Record Protocol

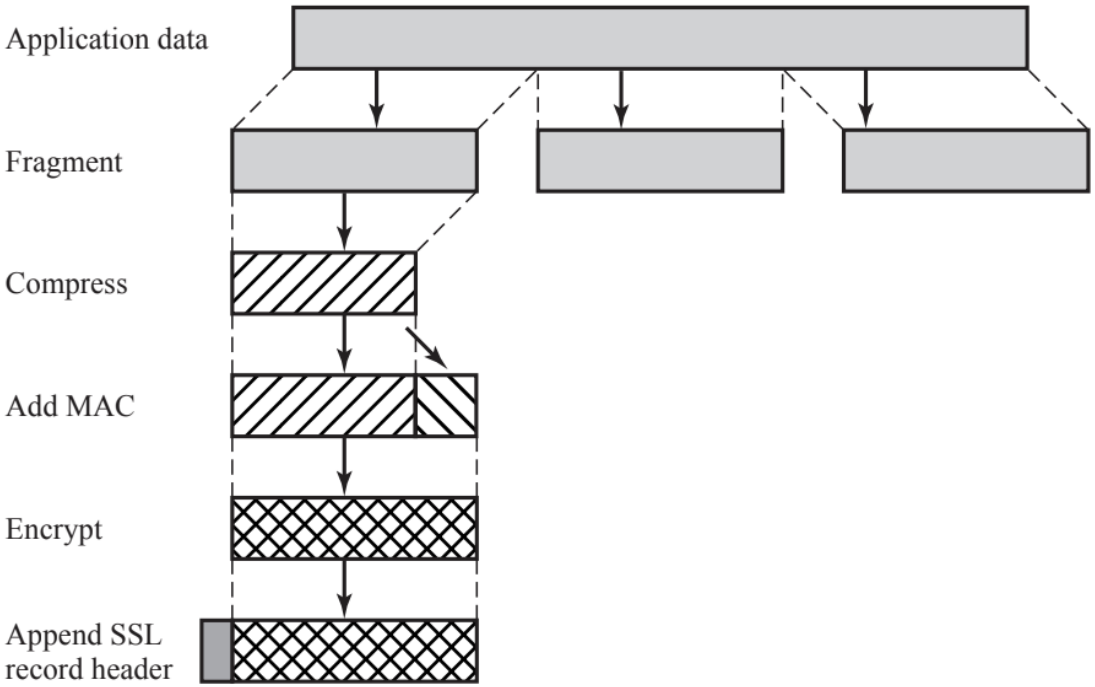

Figure: SSL Record Protocol

SSL - Key Considerations

- SSL uses asymmetric ciphers to establish connection, authenticate and exchange keys, afterwards a symmetric cipher is being used.
- The SSL protocols do not have any fixed order of execution between themselves.
- **HTTPS** incorporates SSL and TLS for secure data transmission.

Outro

Thank you!