Cryptography

Symmetric Cryptography

Symmetric Cryptography Algorithms use the same key for encryption and decryption.

This key is generated and sent alongside the data to the receiver. We use techniques like **confusion** and **diffusion** to make the key more complex.

Most common symmetric cryptography algorithms are **AES**, **DES**, **Blowfish** and **ChaCha**.

Asymmetric Cryptography

Asymmetric Cryptography Algorithms use two different keys that are mathematically related where one is used for encryption and the other is used for decryption.

The two keys generated are a **public key** (which is shared with the receiver) and a **private key** (which is kept safely at the sender).

Popular asymmetric cryptography algorithms are **RSA**, **ECC**, **DSA** and **Diffie-Hellman**. All of these algorithms work on the concept of **One-Way** or **Trap-Door** where it becomes impossible for someone to crack the Private Key due to math.

RSA Algorithm

RSA (Rivest-Shamir-Adleman) is the most used asymmetric cryptography algorithm. It is based on the fact that it veyr difficult to brute-force very large prime numbers.

It works like this

1. Choose two large random prime numbers.
2. Calculate $n = p \times q$
3. Calculate $\phi(n) = (p-1)(q-1)$
4. Choose a value e such that
   $e > 1$
   $e < \phi$
   $hcf(e, \phi) = 1$
5. Calculate d such that
   $d \times e \equiv 1 \pmod{\phi(n)}$

d can be calculated by solving for

$$d = \frac{1 + k \times \phi(n)}{e}$$

where we ignore decimal answers and only consider the first answer that we get in whole numbers.

So now we get the two keys where encryption done using one of the keys requires decryption using the other key. The encryption/decryption is done this way by converting Cipher/Plaintext into numbers and then applying this transformation.

$$CT = PT^e \pmod{n}$$
$$PT = CT^d \pmod{n}$$

El Gamal Algorithm

It is another asymmetric algorithm that is based on the **Diffie Hellman Algorithm** that works on the fact that it is difficult to calculate logarithms in a finite field.

ECC (Elliptic Curve Cryptosystems)

It is another asymmetric algorithm that uses elliptic curves which are notoriously difficult to brute-force. It is much more efficient compared to RSA and generates shorter keys. It works on this equation.

$$y^2 = x^3 + ax + b$$

This equation generates an elliptic curve where any non-vertical line crosses the curve in atleast a single point.

PKI (Public Key Infrastructure)

Public Key Infrastructure is any infrastructure for distributing public encryption or signing keys. It consists of programs, data formats, procedures, communication protocols, security policies, and public key cryptographic mechanisms working in a comprehensive manner to enable a wide range of dispersed people to communicate in a secure and predictable fashion.

The **public key** is shared over the network but this approach is liable to attacks. Also, If you just get sent a public key though the same channels as you send the messages you can not make sure who you are communicating with.

SSL and TLS solves this by requiring that a private key is sent with a certificate which is signed by a trusted third parties called **Certificate Authorities**. That certificate can again have a certificate for its authenticity so you may end up with a chain of certificates. In the end you have to have a certificate from someone the other party have already approved, a root certificate.

Certificates

It is like the identification card for the machine and has the Public Key of that device in it. It is created and signed by a trusted third party → **Certificate Authority**. The

person's identity is verified by another trusted third party → **Registration Authority**. They are created on the basis of the X.205 protocol.

Most browsers come with a number of different root certificates. If a request doesn't have a certificate that matches with one that it recognizes then the browser throws an *alert* that the request might be malicious.

CRL (Certificate Revocation List)

The **Certificate Authority** can also revoke/remove certificates of suspicious/bad people. The revoked certificate's is stored in the **CRL**. The CRL contains all the revoked certificate's information.

This approach is really difficult to implement in the PKI because it becomes difficult to keep track of it.

OCSP (Online Certificate Status Protocol)

This is used instead of the CRL Approach. When using CRL the browser has to continually check for if a Certificate is revoked or not. OCSP does all of this automatically in the background.

Digital Signature → A hash value that has been encrypted with the sender's private key.

Key Management

Even though the encryption makes the text secure; The keys could get stolen, modified or corrupted. One of the most famous ways to enter an Asymmetric Cryptography system is to inject your own public key as someone else's.

Kerberos

Kerberos is a computer-network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

Encryption Methods

Link Encryption

An approach to communications security that encrypts and decrypts all network traffic at each network routing point (e.g. network switch, or node through which it passes) until arrival at its final destination.

It happens at the Network Access layer of the TCP/IP Model; headers and trailers are encrypted.

End-to-End Encryption

Another approach to communications security where the data is encrypted at the sender's device and only gets decrypted at the reciever's device.

It happens at the Application layer of the TCP/IP Model; headers and trailers are NOT encrypted.

Email Standards

They are standards which tell us what is necessary as to be **encrypted** and what is to be left **un-ecrypted**.

MIME (Multipurpose Internet Mail Extension)

A technical specification that tells how multimedia data and e-mail attachments are to be transferred.

When a file is sent, then the client also sends a MIME type which tells what type of file it is (audio? video? image? ...) and also the subtype (jpg? aac? mp4? ...)

S/MIME (Secure MIME)

Secure MIME (S/MIME) is a standard for encrypting and digitally signing electronic mail and for providing secure data transmissions.

PEM (Privacy-Enhanced Mail)

It is an Internet standard to provide secure e-mail over the Internet and for inhouse communication infrastructures.

MSP (Message Security Protocol) → Military's PEM. It was developed by the NSA and is X.400 compatible.

PGP (Pretty Good Privacy)

A free and the first email security program that is a complete cryptographic system.

It is very flexible and can use different types of algorithms; **RSA Asymmetric Algorithm** for PK Encryption, **IDEA Symmetric Cipher** for Bulk Data Encryption and the **MD5 Hashing Algorithm** for Security.

Firewalls

A firewall is either a piece of software or a physical device that protects an network or a PC/Server from unauthorized access.

They identify what is safe for the internal network and block everything else from the external network.

Types of Firewalls

There are many types of firewalls that can be installed with each being for different purposes.

Packet Filter Firewall

It operates at the **network layer** (Layer 3) of the OSI model and filters packets based on rules such as the source/destination IP addresses, ports, and protocols. It checks each packet passing through and if a packet doesn't match the rules then it drops it.

Stateful Packet Filter

It operates at the **network layer** (Layer 3) or **transport layer** (Layer 4) of the OSI model. They monitor the state of active connections and make decisions based on the context of the traffic.

Application Level Gateway (Proxy)

It operates at the **application layer** (Layer 7) of the OSI model. Instead of allowing direct connections between networks, it acts as a middleman for requests. It checks and filters traffic at the application level, providing more control over applications and content.

Circuit Level Gateway

It operates at the **session layer** (Layer 5) of the OSI model. Unlike packet filtering or application layer proxies, circuit-level gateways don’t inspect individual packets or the application data. Instead, they create a proxy connection between two endpoints, acting as a relay for TCP connections.

Bastion Host

It is a highly secured server or computer system located on a network perimeter. It is designed and configured to withstand attacks and is typically used to provide controlled access from an untrusted network (such as the internet) to a private network or a more secure part of the network.

Host-Based Firewall

It is installed directly on individual devices, such as computers, servers, or mobile devices. It monitors and controls incoming and outgoing network traffic based on a set of predefined rules.

Personal Firewalls

Personal firewalls are a specific type of host-based firewall designed for individual users, often installed on personal computers or laptops. They provide protection for end-users against various network threats.

Firewall Configurations

Screened-Host (Single-Homed Bastion Host)

Screened-Host (Double-Homed Bastion Host)

Screened Subnet Firewall

A screened subnet firewall, also known as a **three-legged firewall** or a **triple-homed firewall**, is a network security architecture that incorporates a DMZ (Demilitarized Zone) to provide enhanced protection for internal networks from external threats. It typically consists of three network segments: the internet (untrusted), the DMZ (semi-trusted), and the internal network (trusted).

DMZ (De-Militarized Zone) → a network segment that acts as a buffer zone between a trusted internal network (like a company's intranet) and an untrusted external network (like the internet).