What is Cryptography?

Cryptography is a method to secure communication from unauthorized party. Cryptography allows the following 3 goals to be achieved:

Confidentiality

Integrity

Authenticity

Cryptography ensures the information sent is from intended and not fake sender. This done using digital certificate, digital signature and Public Key Infrastructure (PKI).

Cryptography can be further divided into:

1. Symmetric (or Secret Key) Cryptography
2. Asymmetric (or Public Key) Cryptography

What is Symmetric Cryptography?

In symmetric cryptography, both sender and receiver use the same secret key to encrypt and decrypt a message.
Some of the algorithms includes Blowfish, AES, RC4, DES, RC5, and RC6. The most widely used symmetric algorithm is AES-128, AES-192, and AES-256. All AES algorithms uses the block size of 128-bit but different size of key lengths (128, 192, 256).

What is Asymmetric Cryptography?

Asymmetric cryptography uses a key pairs — public and private key. It works in a way, message encrypted with either public or private key can only be decrypted using the other key of the pair. That is public key to encrypt, private key to decrypt and private key to encrypt, public key to decrypt. Public keys are disseminated in public network whereas private keys are only known to the owners. This key pair cryptography differs from symmetric cryptography which uses one secret key.

Some of the algortihms includes RSA, ELC, Diffie-Helman key exchange, etc.

Asymmetric Cryptography has 2 usages, data encryption and digital signature.

Data Encryption

For data encryption, a sender encryptes an information with receiver's public key. The message can only be decrypted using receiver's public key which is only known to the receiver.

Encrypting a Message

1. Sender encrypts a document with one time symmetric key. This is typically AES or DES Session Key.
2. Sender encrypts the symmetric key with receiver's public key
3. Sender sends both encrypted document and key.

Decrypting a Message

1. Receiver decrypts the session key using own private key.
2. Receiver uses decrypted session key to decrypt the message.

Digital Signature

Digital signatures are like electronic "fingerprints". A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents.

Performing a Digital Signature

1. Sender hashes the original message. A hash function (also called a "hash") is a fixed-length string of numbers and letters generated from a mathematical algorithm and an arbitrarily sized file such as an email, document, picture, or other type of data.
2. Sender ciphers the hashed message with own private key to produce a signature.
3. Sender sends the original message together with signature.

Verifying a Digital Signature

1. Receiver uses the sender public key to decrypt the signature. The outcome is the hashed message.
2. Receiver hashes the original message.
3. Receiver compares the hashes from step 1 and 2.

What is hashing?

Hashing converts input data to output random data of fixed size. This is a one way function, hence the original input data cannot be derived from the output. One usage of hashing is instead of storing password in clear text, we store the hashed password. Even if the hashed passwords were to be compromised, the nature of hashing makes it difficult to retrieve the clear password.

Some of the commonly used hashing algorithms include MD5, SHA-1, bcrypt, Whirlpool, SHA-2 and SHA-3.

Hash Function

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

Features of Hash Functions

The typical features of hash functions are –

- Fixed Length Output (Hash Value)
  - Hash function coverts data of arbitrary length to a fixed length. This process is often referred to as hashing the data.
  - In general, the hash is much smaller than the input data, hence hash functions are sometimes called compression functions.
  - Since a hash is a smaller representation of a larger data, it is also referred to as a digest.
  - Hash function with n bit output is referred to as an n-bit hash function. Popular hash functions generate values between 160 and 512 bits.
- Efficiency of Operation
  - Generally for any hash function h with input x, computation of h(x) is a fast operation.
  - Computationally hash functions are much faster than a symmetric encryption.

Properties of Hash Functions

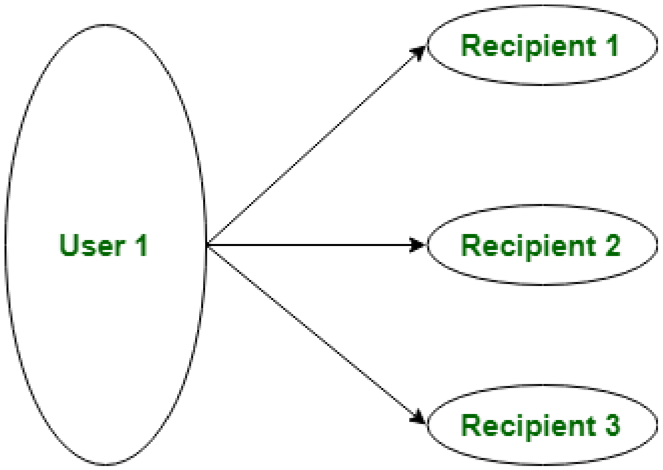
In order to be an effective cryptographic tool, the hash function is desired to possess following properties –

- **Pre-Image Resistance**
  - This property means that it should be computationally hard to reverse a hash function.
  - In other words, if a hash function h produced a hash value z, then it should be a difficult process to find any input value x that hashes to z.
  - This property protects against an attacker who only has a hash value and is trying to find the input.
- **Second Pre-Image Resistance**
  - This property means given an input and its hash, it should be hard to find a different input with the same hash.
  - In other words, if a hash function h for an input x produces hash value h(x), then it should be difficult to find any other input value y such that h(y) = h(x).
  - This property of hash function protects against an attacker who has an input value and its hash, and wants to substitute different value as legitimate value in place of original input value.
- **Collision Resistance**
  - This property means it should be hard to find two different inputs of any length that result in the same hash. This property is also referred to as collision free hash function.
  - In other words, for a hash function h, it is hard to find any two different inputs x and y such that h(x) = h(y).
  - Since, hash function is compressing function with fixed hash length, it is impossible for a hash function not to have collisions. This property of collision free only confirms that these collisions should be hard to find.
  - This property makes it very difficult for an attacker to find two input values with the same hash.
  - Also, if a hash function is collision-resistant then it is second pre-image resistant.

Public Key Distribution

The public key can be distributed in four ways:

1. **Public Announcement:** Here the public key is broadcasted to everyone. The major weakness of this method is a forgery. Anyone can create a key claiming to be someone else and broadcast it. Until forgery is discovered can masquerade as claimed user.



Public Key Announcement

2. Publicly Available Directory: In this type, the public key is stored in a public directory. Directories are trusted here, with properties like Participant Registration, access and allow to modify values at any time, contains entries like {name, public-key}. Directories can be accessed electronically still vulnerable to forgery or tampering.

3. Public Key Authority: It is similar to the directory but, improves security by tightening control over the distribution of keys from the directory. It requires users to know the public key for the directory. Whenever the keys are needed, real-time access to the directory is made by the user to obtain any desired public key securely.

4. Public Certification: This time authority provides a certificate (which binds an identity to the public key) to allow key exchange without real-time access to the public authority each time. The certificate is accompanied by some other info such as period of validity, rights of use, etc. All of this content is signed by the private key of the certificate authority and it can be verified by anyone possessing the authority's public key.
First sender and receiver both request CA for a certificate which contains a public key and other information and then they can exchange these certificates and can start communication.

Real World protocols in cryptography

The typical cryptographic protocols include the Secure Socket Layer Protocol (SSL) and its variant, Transport Layer Security Protocol (TLS), the Internet Key Exchange Protocol (IKE) and the Kerberos Authentication Protocol.

1. **SSL Protocol :**
   - SSL Protocol stands for Secure Sockets Layer protocol, which is an encryption-based Internet security protocol that protects confidentiality and integrity of data.
   - SSL is used to ensure the privacy and authenticity of data over the internet.
   - SSL is located between the application and transport layers.
   - At first, SSL contained security flaws and was quickly replaced by the first version of TLS that's why SSL is the predecessor of the modern TLS encryption.
   - TLS/SSL website has "HTTPS" in its URL rather than "HTTP".
   - SSL is divided into three sub-protocols: the Handshake Protocol, the Record Protocol, and the Alert Protocol.
2. **TLS Protocol :**
   - Same as SSL, TLS which stands for Transport Layer Security is widely used for the privacy and security of data over the internet.
   - TLS uses a pseudo-random algorithm to generate the master secret which is a key used for the encryption between the protocol client and protocol server.
   - TLS is basically used for encrypting communication between online servers like a web browser loading a web page in the online server.
   - TLS also has three sub-protocols the same as SSL protocol – Handshake Protocol, Record Protocol, and Alert Protocol.
3. **SHTTP :**
   - SHTTP stands for Secure HyperText Transfer Protocol, which is a collection of security measures like Establishing strong passwords, setting up a firewall, thinking of antivirus protection, and so on designed to secure internet communication.
   - SHTTP includes data entry forms that are used to input data, which has previously been collected into a database. As well as internet-based transactions.
   - SHTTP's services are quite comparable to those of the SSL protocol.
   - Secure HyperText Transfer Protocol works at the application layer (that defines the shared communications protocols and interface methods used by hosts in a network) and is thus closely linked with HTTP.
   - SHTTP can authenticate and encrypt HTTP traffic between the client and the server.
   - SHTTP operates on a message-by-message basis. It can encrypt and sign individual messages.
4. **Set Protocol :**
   - Secure Electronic Transaction (SET) is a method that assures the security and integrity of electronic transactions made using credit cards.
   - SET is not a payment system; rather, it is a secure transaction protocol that is used via the internet.
   - The SET protocol provides the following services:
     - It establishes a safe channel of communication between all parties engaged in an e-commerce transaction.
     - It provides confidentiality since the information is only available to the parties engaged in a transaction when and when it is needed.

- The SET protocol includes the following participants:
    - **Cardholder**
    - **Merchant**
    - **Issuer**
    - **Acquire**
    - **Payment Gateway**
    - **Certification Authority**

5. **PEM Protocol :**
    - PEM Protocol stands for privacy-enhanced mail and is used for email security over the internet.
    - RFC 1421, RFC 1422, RFC 1423, and RFC 1424 are the four particular papers that explain the Privacy Enhanced Mail protocol.
    - It is capable of performing cryptographic operations such as encryption, nonrepudiation, and message integrity.

6. **PGP Protocol :**
    - PGP Protocol stands for Pretty Good Privacy, and it is simple to use and free, including its source code documentation.
    - It also meets the fundamental criteria of cryptography.
    - When compared to the PEM protocol, the PGP protocol has grown in popularity and use.
    - The PGP protocol includes cryptographic features such as encryption, non-repudiation, and message integrity.

What is Public Key Infrastructure (PKI)?

PKI is a framework that uses public key cryptography to provide authentication and confidentiality. A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates 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.

Basic Terminology of Cryptography:

The important terms in cryptography are:
Plaintext: original message
Cipher text: encrypted or coded message
Encryption: convert from plaintext to cipher text (enciphering)
Decryption: restore the plaintext from cipher text (deciphering)
Key: information used in cipher known only to sender/receiver
Cipher: a particular algorithm (cryptographic system)
Cryptography: study of algorithms used for encryption
Cryptanalysis: study of techniques for decryption without knowledge of plaintext
Cryptology: areas of cryptography and cryptanalysis

Email Security Certificates: Email certificates, also known as SMIME certificates, are digital certificates that can be used to sign and encrypt email messages. When you encrypt an email using an email certificate, only the person that you sent it to can decrypt and read the email. The recipient can also be sure that the email hasn't been changed in any way.

Why do I need email certificates?

If you don't use an email certificate, your emails can be read by anyone, or any server, that is used to pass the emails to the recipient. This can be a lot people. This would be like sending a postcard through the mail so that all of the postal workers and anyone who really wants to can read it. With an email certificate, you are 100% guaranteed to have secure email while it is being transmitted.

Some email servers use a different kind of certificate called a server authentication SSL certificate. This secures all email transmissions from the server to your local computer, but once you send an email to another email account on another email server, it leaves that safe haven and travels to the unprotected lines of the Internet where anyone can read it. An SMIME certificate ensures end-to-end security.

How does an SMIME Email Certificate work?

Once you install the SMIME (Secure / Multipurpose Internet Mail Extensions) certificate in your email client, you will send a signed email to people that need to send encrypted emails to you. Your contacts' email client should automatically download your certificate add it the address book. From then on, your contacts can send you encrypted emails by clicking the "Encrypt" button when creating a new email. Different email clients handle this differently than others so make sure to check the documentation of the email client that you use.

TLS (Transport Layer Security): The transport layer provides a logical communication between application processes running on different hosts. Transport Layer Securities (TLS) are designed to provide security at the transport layer. TLS was derived from a security protocol called Secure Socket Layer (SSL). TLS ensures that no third party may eavesdrop or tampers with any message.

There are several benefits of TLS:

- **Encryption:** TLS/SSL can help to secure transmitted data using encryption.
- **Interoperability:** TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.
- **Algorithm flexibility:** TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.
- **Ease of Deployment:** Many applications TLS/SSL temporarily on a windows server 2003 operating systems.
- **Ease of Use:** Because we implement TLS/SSL beneath the application layer, most of its operations are completely invisible to client.

IP security (IPSec): The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

Uses of IP Security –

IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

What is DNS security?

DNS security is the practice of protecting DNS infrastructure from cyber attacks in order to keep it performing quickly and reliably. An effective DNS security strategy incorporates a number of overlapping defenses, including establishing redundant DNS servers, applying security protocols like DNSSEC, and requiring rigorous DNS logging. DNS Security Extensions (DNSSEC) is a security protocol created to mitigate this problem. DNSSEC protects against attacks by digitally signing data to help ensure its validity. In order to ensure a secure lookup, the signing must happen at every level in the DNS lookup process.

What are some common attacks involving DNS?

Attackers have found a number of ways to target and exploit DNS servers. Here are some of the most common:

DNS spoofing/cache poisoning: Instead of going to the correct website, traffic can be diverted to a malicious machine or anywhere else the attacker desires; often this will be a replica of the original site.

DNS tunneling, DNS hijacking, NXDOMAIN attack, Phantom domain attack, Random sub domain attack, Domain lock-up attack, Botnet-based CPE attack