CRYPTO M1 (part-1)

techworldthink • March 18, 2022

Introduction to Cryptography

The word "cryptography" is derived from the Greek *kryptos*, meaning hidden. The prefix "crypt-" means "hidden" or "vault," and the suffix "-graphy" stands for "writing."

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. It includes techniques such as microdots, merging words with images and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

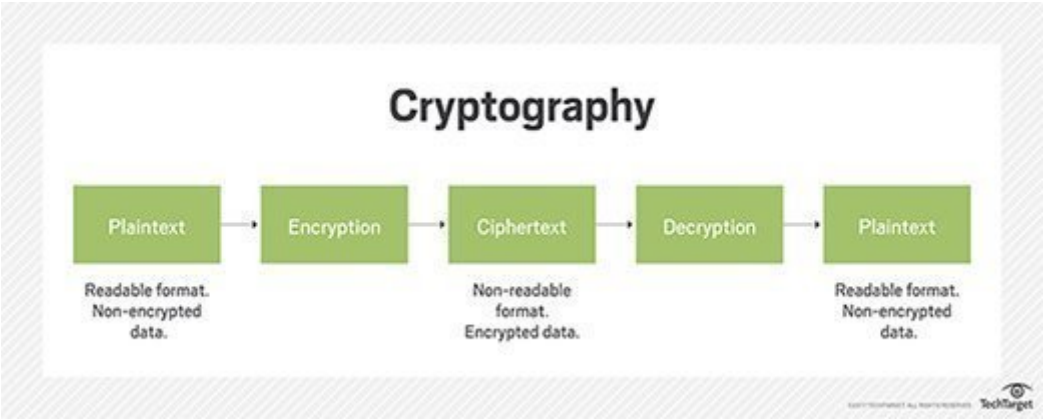


Image displaying cryptography steps and functions.

What problems does cryptography solve?

A secure system should provide several assurances such as confidentiality, integrity, and availability of data as well as authenticity and non-repudiation. When used correctly, crypto helps to provide these assurances. Cryptography can ensure the confidentiality and integrity of both data in transit as well as data at rest. It can also authenticate senders and recipients to one another and protect against repudiation.

Software systems often have multiple endpoints, typically multiple clients, and one or more back-end servers. These client/server communications take place over networks that cannot be trusted. Communication occurs over open, public networks such as the Internet, or private networks which may be compromised by external attackers or malicious insiders.

It can protect communications that traverse untrusted networks. There are two main types of attacks that an adversary may attempt to carry out on a network. Passive attacks involve an attacker simply listening on a network segment and attempting to read sensitive information as it travels. Passive attacks may be online (in which an attacker reads traffic in real-time) or offline (in which an attacker simply captures traffic in real-time and views it later—perhaps after spending some time decrypting it). Active attacks involve an attacker impersonating a client or server, intercepting communications in transit, and viewing and/or modifying the contents before passing them on to their intended destination (or dropping them entirely).

The confidentiality and integrity protections offered by cryptographic protocols such as SSL/TLS can protect communications from malicious eavesdropping and tampering. Authenticity protections provide assurance that users are actually communicating with the systems as intended. For example, are you sending your online banking password to your bank or someone else?

It can also be used to protect data at rest. Data on a removable disk or in a database can be encrypted to prevent disclosure of sensitive data should the physical media be lost or stolen. In addition, it can also provide integrity protection of data at rest to detect malicious tampering.

OSI security architecture

The OSI security architecture helps the managers responsible for the security of an organization in defining the requirements for security. The OSI security architecture was introduced as an 'international standard' which let the computer and communication vendor develop the products that have security features based on this architecture. The OSI security architecture has a structure definition of services and mechanism for providing security to the organization's information.

OSI Security Architecture Defines:

1. Security Attacks
2. Security Mechanism
3. Security Services

SECURITY ATTACKS

Security attacks can be defined as an action that risks the security of information owned by the company.

1.Passive Attack

In a passive attack, the attacker monitors or eavesdrops the transmission between and sender and receiver and the attacker try to retrieve the information being transmitted. In passive attack neither the sender nor the receiver is aware of the attack as the attacker only retrieve the message, he doesn't perform any alteration to the captured message. The message is sent and received in the normal fashion.Therefore, is more difficult to identify the passive attack. Though identification of passive attack is tedious, you can definitely implement encryption in order to prevent the success of this attack which means even if the attack happens the attacker is unable to extract the information.

The passive attack is further classified into two types.

Release of message content

- The release of the message content is a kind of attack where the attacker listens to the telephone conversation, tracks electronic mail or the transferred file to retrieve the confidential message being transmitted. The opponent is quite interested in the content of the released message.

Traffic analysis

- To protect the released message content the organization may apply a mask over the content of the message so that even if the attacker captures the message, he would not be able to understand the message. This technique of masking the released message is termed as encryption.
- In traffic analysis passive attack, the attacker monitors the pattern, length and frequency of the released message to guess the original message.

2.Active Attack

We have seen that in the passive attack the attacker does not alter the message, but in the active attack the attacker alters, modify the transmitted message by creating a false data stream.It is quite difficult to prevent the active attack instead the goal is to identify the source of active attack and apply a recovery measure.

The active attack is further classified into four types

- Masquerade

In masquerade active attack, the attacker pretends to be the sender.

- Replay

In the replay, the message is captured in a passive way and is retransmitted to produce an unauthorized effect.

- Modification of message

Modification of message means some data stream of the message is altered or modified to create an unauthorized effect.

- Denial of services

The attacker suppresses all the messages directed to a particular receiver by overloading the network to degrade the network performance

SECURITY SERVICES

The security mechanism is an entire process that is specifically designed to identify the attack and develops a strategy to recover or prevent the attack.

- Authentication: It assures that the entity involves in the communication is the one it is claiming for.
- Access Control: This service assures that only the authorized entities are accessing the resources and prevents unauthorized access.
- Data Confidentiality: This service manages to maintain the confidentiality of data by preventing the exposure of the message content to the attacker.
- Data Integrity: This service makes it sure that the data received at the receiver end is from an authorized entity.
- Nonrepudiation: This service restricts the sending and receiving entity from denying the transmitted message.

In all the OSI security architecture the things that need to be concentrated are security attack, service and mechanism to prevent the risk to the security of information of an organization.

SECURITY MECHANISMS

One of the most specific security mechanisms in use is cryptographic techniques. Encryption or encryption-like transformations of information are the most common means of providing security. Some of the mechanisms are:

Encipherment

Digital Signature

Access Control

Phishing

Phishing is a type of cybersecurity attack during which malicious actors send messages pretending to be a trusted person or entity. Phishing messages manipulate a user, causing them to perform actions like installing a malicious file, clicking a malicious link, or divulging sensitive information such as access credentials. Phishing is the most common type of social engineering, which is a general term describing attempts to manipulate or trick computer users. Social engineering is an increasingly common threat vector used in almost all security incidents. Social engineering attacks, like phishing, are often combined with other threats, such as malware, code injection, and network attacks.

The basic element of a phishing attack is a message, sent by email, social media, or other electronic communication means.

A phisher may use public resources, especially social networks, to collect background information about the personal and work experience of their victim. These sources are used to gather information such as the potential victim's name, job title, and email address, as well as interests and activities. The phisher can then use this information to create a reliable fake message.

Typically, the emails the victim receives appear to come from a known contact or organization. Attacks are carried out through malicious attachments or links to malicious websites. Attackers often set up fake websites, which appear to be owned by a trusted entity like the victim's bank, workplace, or university. Via these websites, attackers attempt to collect private information like usernames and passwords, or payment information.

Some phishing emails can be identified due to poor copywriting and improper use of fonts, logos, and layouts. However, many cybercriminals are becoming more sophisticated at creating authentic-looking messages, and are using professional marketing techniques to test and improve the effectiveness of their emails.

5 Types of Phishing Attacks

Email Phishing

Most phishing attacks are sent via email. Attackers typically register fake domain names that mimic real organizations and send thousands of common requests to victims.

For fake domains, attackers may add or replace characters (e.g. my-bank.com instead of mybank.com), use subdomains (e.g. mybank.host.com) or use the trusted organization's name as the email username (e.g. mybank@host.com).

Many phishing emails use a sense of urgency, or a threat, to cause a user to comply quickly without checking the source or authenticity of the email.

Email phishing messages have one of the following goals:

- Causing the user to click a link to a malicious website, in order to install malware on their device.
- Causing the user to download an infected file and using it to deploy malware
- Causing the user to click a link to a fake website and submit personal data.
- Causing the user to reply and provide personal data.

Spear Phishing

Spear phishing includes malicious emails sent to specific people. The attacker typically already has some or all of the following information about the victim: Name, Place of employmen, job title, Email address, Specific information about their job role, Trusted colleagues, family members, or other contacts, and samples of their writing

This information helps increase the effectiveness of phishing emails and manipulate victims into performing tasks and activities, such as transferring money.

Whaling

Whaling attacks target senior management and other highly privileged roles. The ultimate goal of whaling is the same as other types of phishing attacks, but the technique is often very subtle. Senior employees commonly have a lot of information

in the public domain, and attackers can use this information to craft highly effective attacks.

Typically, these attacks do not use tricks like malicious URLs and fake links. Instead, they leverage highly personalized messages using information they discover in their research about the victim. For example, whaling attackers commonly use bogus tax returns to discover sensitive data about the victim, and use it to craft their attack.

Smishing and Vishing

This is a phishing attack that uses a phone instead of written communication. Smishing involves sending fraudulent SMS messages, while vishing involves phone conversations.

In a typical voice phishing scam, an attacker pretends to be a scam investigator for a credit card company or bank, informing victims that their account has been breached. Criminals then ask the victim to provide payment card information, supposedly to verify their identity or transfer money to a secure account (which is really the attacker's).

Vishing scams may also involve automated phone calls pretending to be from a trusted entity, asking the victim to type personal details using their phone keypad.

Angler Phishing

These attacks use fake social media accounts belonging to well known organizations. The attacker uses an account handle that mimics a legitimate organization (e.g. "@pizzahutcustomercare") and uses the same profile picture as the real company account.

Attackers take advantage of consumers' tendency to make complaints and request assistance from brands using social media channels. However, instead of contacting the real brand, the consumer contacts the attacker's fake social account.

When attackers receive such a request, they might ask the customer to provide personal information so that they can identify the problem and respond appropriately. In other cases, the attacker provides a link to a fake customer support page, which is actually a malicious website.

Ransomware

is a type of malicious software (malware) that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker. In many cases, the ransom demand comes with a deadline. If the victim doesn't pay in time, the data is gone forever or the ransom increases.

Ransomware is malware that employs encryption to hold a victim's information at ransom. A user or organization's critical data is encrypted so that they cannot access files, databases, or applications. A ransom is then demanded to provide access. Ransomware is often designed to spread across a network and target database and file servers, and can thus quickly paralyze an entire organization. It is a growing threat, generating billions of dollars in payments to cybercriminals and inflicting significant damage and expenses for businesses and governmental organizations.

Ransomware is a malicious software which infects many computers and displays messages demanding you pay a fee to get your system working again. The malware class is a criminal moneymaking scheme that is set up by an email message, instant messages or misleading links on the website. It locks a computer screen or encrypts predefined files with a password.

Types of Ransomware

There are 3 types of Ransomware, which are given below

1.Scareware

Scareware is not as scary. It includes security software and technical support scams. In Scareware, we receive a pop-up message claiming that the malware was discovered, and the only way to get rid of the virus is to pay online. If you do nothing, you continuously receive pop-ups, but the files are almost safe.

If you do not have the company's software on your computer, it will not monitor you for ransomware infection.

2.Screen locker

Upgrade the Terror Alert Orange for these people. When lock-screen Ransomware is found on our computer, it means that you are out of your PC. If they suspect you of

theft, child pornography or other cybercrimes, they will go through the appropriate legal channels.

3.Encrypt Ransomware

It is dangerous stuff. These are the people who are snatching our files and encrypt them, demanding payment for decryption and redistribution. This type of Ransomware is so terrible because once cybercriminals pile up our files; no security software or system can restore or return it until you pay the ransom. And if you pay, there is no guarantee that cybercriminals will give those files back to you.

DoS attack

A denial-of-service (DoS) attack, also known as a brute-force attack, is used to prevent online services from functioning properly. It's usually triggered by an intruder flooding a website with a large amount of traffic or requests in an effort to overwhelm the site's infrastructure and bring it down.

A distributed denial-of-service (DDoS) attack is a more sophisticated DoS attack in which an attacker takes control of multiple computers to overwhelm its target.

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. Popular flood attacks include:

- Buffer overflow attacks – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to

handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks

- ICMP flood – leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.
- SYN flood – sends a request to connect to a server, but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

Other DoS attacks simply exploit vulnerabilities that cause the target system or service to crash. In these attacks, input is sent that takes advantage of bugs in the target that subsequently crash or severely destabilize the system, so that it can't be accessed or used.

An additional type of DoS attack is the Distributed Denial of Service (DDoS) attack. A DDoS attack occurs when multiple systems orchestrate a synchronized DoS attack to a single target. The essential difference is that instead of being attacked from one location, the target is attacked from many locations at once. The distribution of hosts that defines a DDoS provide the attacker multiple advantages:

- He can leverage the greater volume of machine to execute a seriously disruptive attack
- The location of the attack is difficult to detect due to the random distribution of attacking systems (often worldwide)
- It is more difficult to shut down multiple machines than one
- The true attacking party is very difficult to identify, as they are disguised behind many (mostly compromised) systems

Modern security technologies have developed mechanisms to defend against most forms of DoS attacks, but due to the unique characteristics of DDoS, it is still regarded as an elevated threat and is of higher concern to organizations that fear being targeted by such an attack.

Network security model

A Network Security Model exhibits how the security service has been designed over the network to prevent the opponent from causing a threat to the confidentiality or authenticity of the information that is being transmitted through the network.

For a message to be sent or receive there must be a sender and a receiver. Both the sender and receiver must also be mutually agreeing to the sharing of the message. Now, the transmission of a message from sender to receiver needs a medium i.e. Information channel which is an Internet service.

A logical route is defined through the network (Internet), from sender to the receiver and using the communication protocols both the sender and the receiver established communication.

Well, we are concerned about the security of the message over the network when the message has some confidential or authentic information which has a threat from an opponent present at the information channel. Any security service would have the three components discussed below:

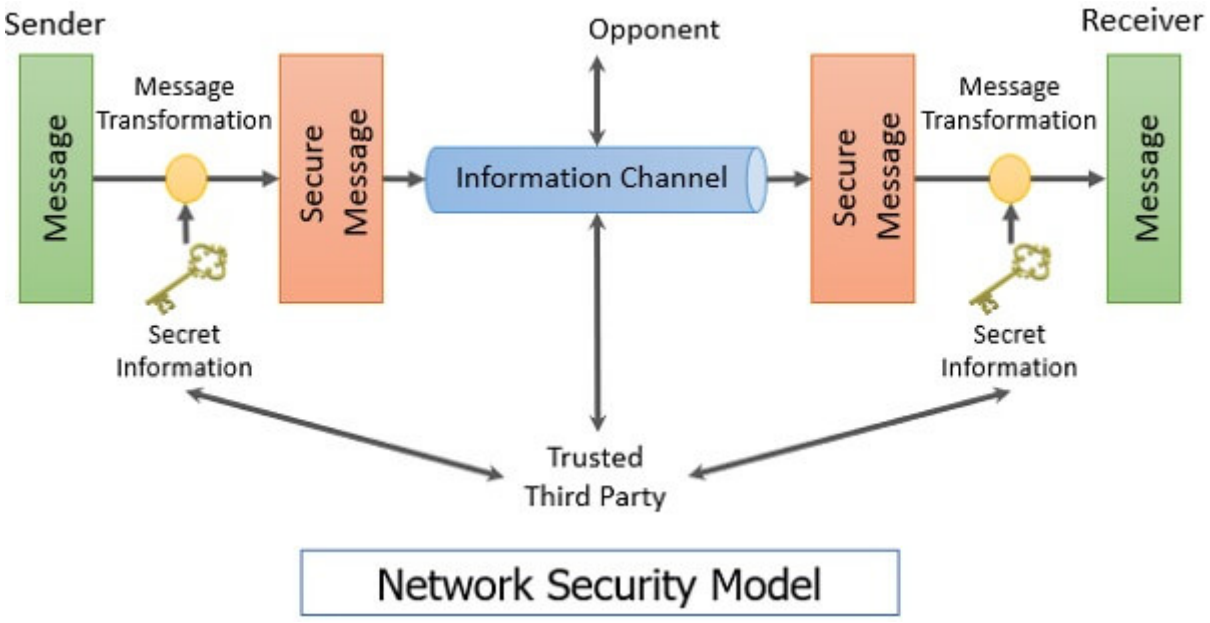
1. Transformation of the information which has to be sent to the receiver. So, that any opponent present at the information channel is unable to read the message. This indicates the encryption of the message.

It also includes the addition of code during the transformation of the information which will be used in verifying the identity of the authentic receiver.

2. Sharing of the secret information between sender and receiver of which the opponent must not any clue. Yes, we are talking of the encryption key which is used during the encryption of the message at the sender's end and also during the decryption of message at receiver's end.

3. There must be a trusted third party which should take the responsibility of distributing the secret information (key) to both the communicating parties and also prevent it from any opponent.

Now we will study a general network security model with the help of the figure given below:



Network Security Model

The network security model presents the two communicating parties sender and receiver who mutually agrees to exchange the information. The sender has information to share with the receiver.

But sender cannot send the message on the information cannel in the readable form as it will have a threat of being attacked by the opponent. So, before sending the message through the information channel, it should be transformed into an unreadable format.

Secret information is used while transforming the message which will also be required when the message will be retransformed at the recipient side. That's why a trusted third party is required which would take the responsibility of distributing this secret information to both the parties involved in communication.

So, considering this general model of network security, one must consider the following four tasks while designing the security model.

1. To transform a readable message at the sender side into an unreadable format, an appropriate algorithm should be designed such that it should be difficult for an opponent to crack that security algorithm.

2. Next, the network security model designer is concerned about the generation of the secret information which is known as a key.

This secret information is used in conjunction with the security algorithm in order to transform the message.

3. Now, the secret information is required at both the ends, sender's end and receiver's end. At sender's end, it is used to encrypt or transform the message into unreadable form and at the receiver's end, it is used to decrypt or retransform the message into readable form.

So, there must be a trusted third party which will distribute the secret information to both sender and receiver. While designing the network security model designer must also concentrate on developing the methods to distribute the key to the sender and receiver.

An appropriate methodology must be used to deliver the secret information to the communicating parties without the interference of the opponent.

It is also taken care that the communication protocols that are used by the communicating parties should be supporting the security algorithm and the secret key in order to achieve the security service.

Till now we have discussed the security of the information or message over the network. Now, we will discuss the network access security model which is designed to secure the information system which can be accessed by the attacker through the network.

You are well aware of the attackers who attack your system that is accessible through the internet. These attackers fall into two categories:

1. Hacker: The one who is only interested in penetrating into your system. They do not cause any harm to your system they only get satisfied by getting access to your system.

2. Intruders: These attackers intend to do damage to your system or try to obtain the information from the system which can be used to attain financial gain.

The attacker can place a logical program on your system through the network which can affect the software on your system. This leads to two kinds of risks:

a. Information threat: This kind of threats modifies data on the user's behalf to which actually user should not access. Like enabling some crucial permission in the system.

b. Service threat: This kind of threat disables the user from accessing data on the system.

Well, these kinds of threats can be introduced by launching worms and viruses and may more like this on your system. Attack with worms and viruses are the software

attack that can be introduced to your system through the internet.