## 6.11 Investigates the security aspects of communication and protection of devices connected to the Internet

**Encryption and digital signature – basic idea**

**Encryption**

Encryption is a technique used in cryptography which provides confidentiality of transmitting data.

There are two types of encryption:

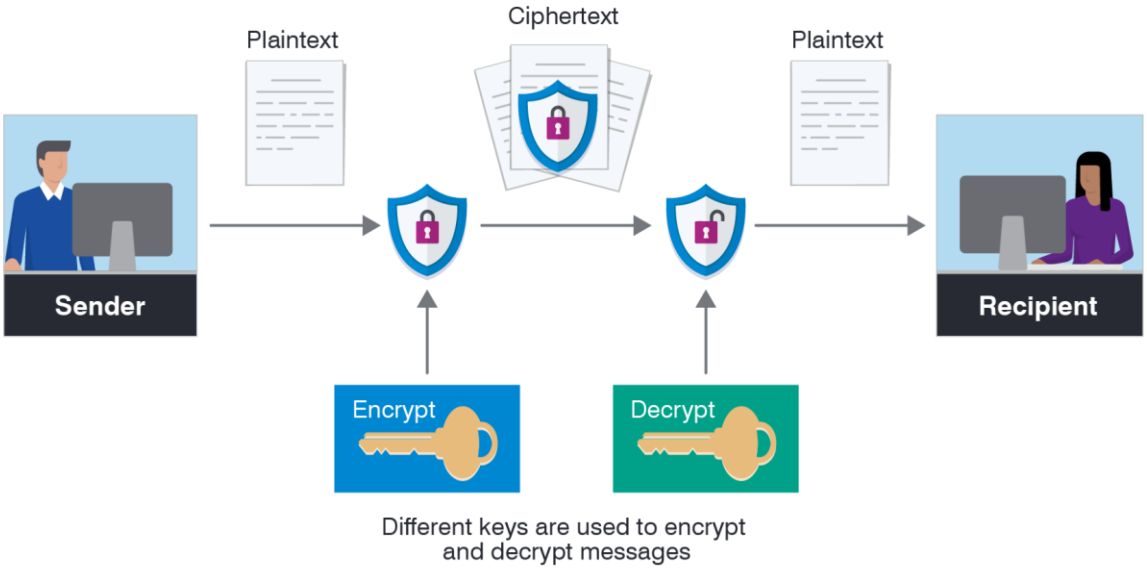
1. Symmetric Key Encryption - The encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption. When using symmetric key encryption users must share a common key prior to exchange of information.

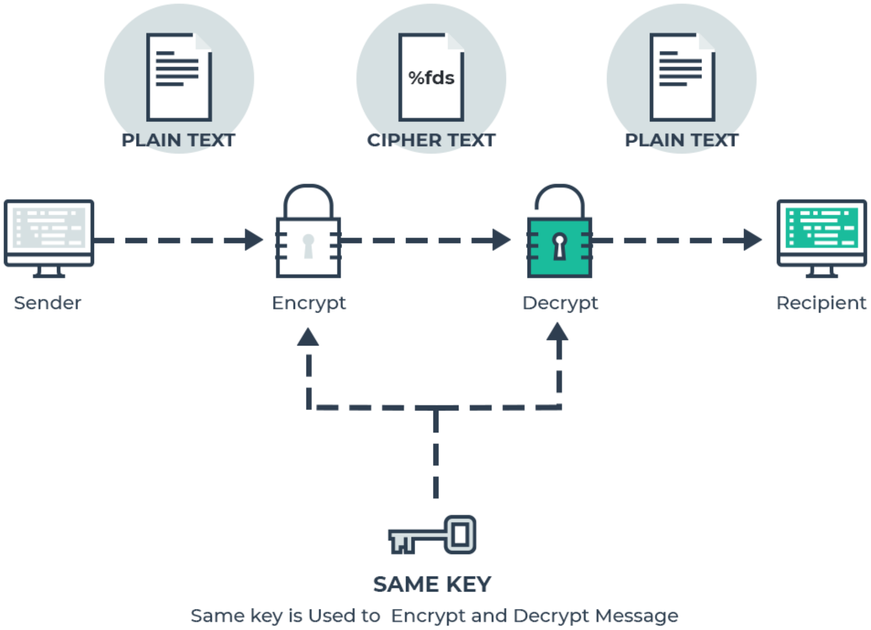
2. Asymmetric Key Encryption - The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption. Every user in this system needs to have a pair of dissimilar keys, private key and public key. These keys are mathematically related − when one key is used for encryption, the other can decrypt the cipher text back to the original plaintext.

Consider it through an example that a person **A** wants to send some message to person **B**. but he fears that what if a third person **C** read that message. So **A** wish to find safe way by which he can send message to **B** and **C** can't read it. So he uses some techniques.

Now A made this plain text to cipher text by using some function and send that cipher text to **B**. now **B** uses the inverse of that function to get the plain text back. In this way A can securely communicate with **B**.

Encoding some information in a way that you and some trusted person have an access to get that information is called encryption and for the third party it's just like trash until they get the decryption function.

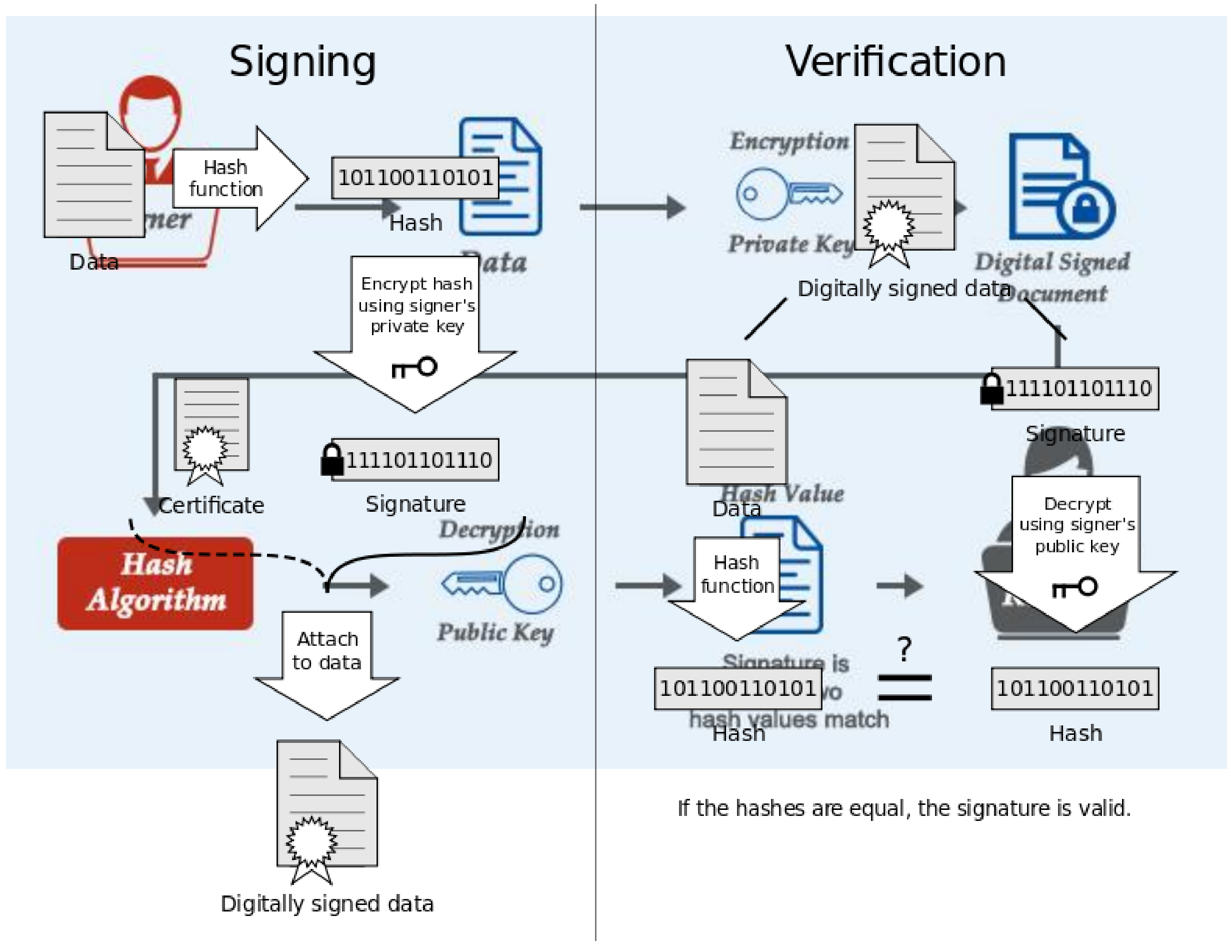




## Digital signature

- In the real world you use your signature to make sure that it was you who have signed.
- Suppose you ordered a device from an e-commerce site. When you are going to receive it the delivery boy ask you to sign on the paper or in some device to ensure your identity.
- So just like real world, in the virtual world you need the digital signature to verify the authenticity of document.
- A digital signature guarantees the authenticity of an electronic document or message.
- How it works- In this process we proceed some data through a hash function. Then it can be encrypted by signer’s private key. So now that electronic document contains the data, encrypted hashed data and name of the hash function that has been used.
- Verifier has the signer's public key and with the help of that verifier decrypt it to get hashed data. Verifier also know which hash has been used. So it passes the data through the hash and get some hashed data. Then it match that hashed data to the decrypted data.

- If it matched then it verified.



Digital signatures help to authenticate the sources of messages. Digital signatures allow us to verify the author, date and time of signatures, authenticate the message contents.

**The most common network security threats**

1. **Malware -** Malware, or malicious software, is any program or file that is harmful to a computer user. Types of malware can include computer viruses, worms, Trojan horses and spyware.

2. **Computer virus** - Computer viruses are pieces of software that are designed to be spread from one computer to another. They're often sent as email attachments or downloaded from specific websites with the intent to infect your computer and other computers on your contact list by using systems on your network.

3. **Trojan horse** - A "Trojan horse" refers to tricking someone into inviting an attacker into a securely protected area. In computing, it holds a very similar meaning — a Trojan horse, or "Trojan," is a malicious bit of attacking code or software that tricks users into running it willingly, by hiding behind a genuine program.

   They spread often by email; it may appear as an email from someone you know, and when you click on the email and its included attachment, you've immediately downloaded malware to your computer. Trojans also spread when you click on a false advertisement.

   Once inside your computer, a Trojan horse can record your passwords by logging keystrokes, hijacking your webcam, and stealing any sensitive data you may have on your computer.

4. **Phishing** - Phishing is a method of a social engineering with the goal of obtaining sensitive data such as passwords, usernames, and credit card numbers.

   The attacks often come in the form of instant messages or phishing emails designed to appear legitimate. The recipient of the email is then tricked into opening a malicious link, which leads to the installation of malware on the recipient's computer. It can also obtain personal information by sending an email that appears to be sent from a bank, asking to verify your identity by giving away your private information.

5. **Rogue security software** - Rogue security software is malicious software that mislead users to believe there is a computer virus installed on their computer or that their security measures are not up to date. Then they offer to install or update users' security settings. They'll either ask you to download their program to remove the alleged viruses, or to pay for a tool. Both cases lead to actual malware being installed on your computer.

6. **Adware and spyware** - By "adware" we consider any software that is designed to track data of your browsing habits and, based on that, show you advertisements and pop-ups. Adware collects data with your permission.

   When adware is downloaded without consent, it is considered malicious.

   Spyware works similarly to adware, but is installed on your computer without your knowledge. It can contain key loggers that record personal information including email addresses, passwords, even credit card numbers, making it dangerous because of the high risk of identity theft.

7. **Computer worm** - Computer worms are pieces of malware programs that replicate quickly and spread from one computer to another. A worm spreads from an infected computer by sending itself to all of the computer's contacts, then immediately to the contacts of the other computers. Interestingly, they are not always designed to cause harm; there are worms that are made just to spread. Transmission of worms is also often done by exploiting software vulnerabilities.

8. **DOS and DDOS attack** - A DoS attack is performed by one machine and its internet connection, by flooding a website with packets and making it impossible for legitimate users to access the content of flooded website. Fortunately, you can't really overload a server with a single other server or a PC anymore. In the past years it hasn't been that common if anything, then by flaws in the protocol.

A DDoS attack, or distributed denial-of-service attack, is similar to DoS, but is more forceful. It's harder to overcome a DDoS attack. It's launched from several computers, and the number of computers involved can range from just a couple of them to thousands or even more.

Since it's likely that not all of those machines belong to the attacker, they are compromised and added to the attacker's network by malware. These computers can be distributed around the entire globe, and that network of compromised computers is called botnet.

Since the attack comes from so many different IP addresses simultaneously, a DDoS attack is much more difficult for the victim to locate and defend against.

9. **Rootkit** - Rootkit is a collection of software tools that enables remote control and administration-level access over a computer or computer networks. Once remote access is obtained, the rootkit can perform a number of malicious actions; they come equipped with key loggers, password stealers and antivirus disablers.

   Rootkits are installed by hiding in legitimate software: when you give permission to that software to make changes to your OS, the rootkit installs itself in your computer and waits for the hacker to activate it. Other ways of rootkit distribution include phishing emails, malicious links, files, and downloading software from suspicious websites.

10. **SQL Injection attack** - SQL injection attacks are designed to target data-driven applications by exploiting security vulnerabilities in the application's software. They use malicious code to obtain private data, change and even destroy that data, and can go as far as to void transactions on websites. It has quickly become one of the most dangerous privacy issues for data confidentiality.

11. **Man-in-the-middle attacks** - Man-in-the-middle attacks are cybersecurity attacks that allow the attacker to listening on communication between two targets. It can listen to a communication which should, in normal settings, be private.

Here are just some of the types of MITM attacks:

- DNS spoofing
- HTTPS spoofing
- IP spoofing
- ARP spoofing
- SSL hijacking
- Wi-Fi hacking

**Protection against unauthorized malicious accesses**

- **Firewalls**: are systems that act against unauthorized accesses to protected data.

- **Antivirus software**: are software that detect and quarantine the malicious software that tries to harm a computer.

- **Computer users must be properly educated** to protect the network devices against malicious attacks and unauthorized accesses. Passwords must be chosen with utmost care and antivirus software must be periodically updated to protect the system from attacks.

**Read for more derails about End to End Encryption - [https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE](https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE)**

**Reference**

Teachers Guide 2017
https://www.quora.com/What-is-the-difference-between-encryption-and-digital-signature
https://securitytrails.com/blog/top-10-common-network-security-threats-explained