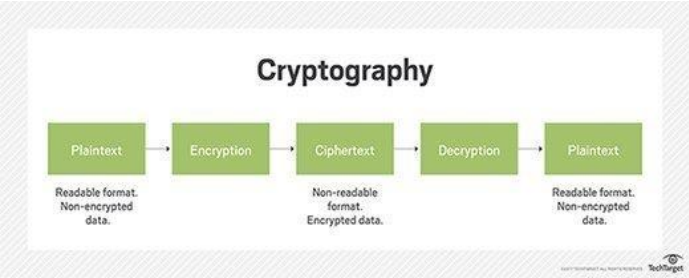
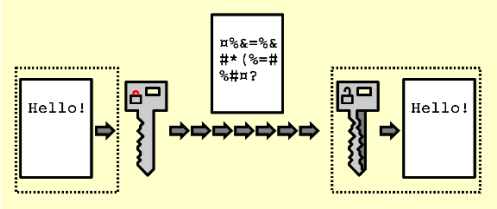
The Difference Between Encryption and Cryptography

- **Cryptography** is the science of "secret writing".
- It includes steganography, which is the science of hiding a secret message inside another, seemingly legitimate message that acts as the carrier so the hidden, unseen message will not appear during transit.
- Simply, "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."



Encryption

- Encryption is considered a component of cryptography, and it is concerned with concealing secret messages by obscuring them.
- In other terms, encryption converts plaintext data into another obscured form called ciphertext using a specific cryptographic algorithm. This ciphertext can't be decrypted to its original state without owning or having access to the associated decryption key.



Cryptographic Functions

- Cryptography is an essential information security tool.
- It provides the four most basic services for information security.
  1. **Authentication**
  2. **Nonrepudiation**
  3. **Confidentiality**

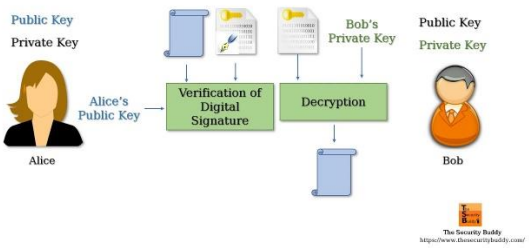
4. **Integrity**

1. **Authentication**

- For example, when a user requests access to remote resources stored on a server, he or she needs to supply their credentials, for instance, a username and password.
- If the user credentials match, the system will grant the user access, or authorize, the access to the data or computing resources matching the associated access control tables otherwise, access will be denied.

2. Non-repudiation:

- The concept of nonrepudiation is important in the e commerce world. To repudiate means to deny, and this concept is simple when a user performs an action, he or she cannot later deny it.
- For example, when a bank client sends a money transfer from his or her account to another account using an electronic transfer.
- Later, this client may deny sending any transfer from his or her account and demand the money be returned.
- Here, there should be a technical mechanism in the bank to confirm that this client has legally authorized the transaction.



3. **Confidentiality:**

- Confidentiality ensures that data is not made available or disclosed to unauthorized parties.
- When the data is confidential, no one should be allowed access to it except the authorized people who possess the decryption key.
- Confidentiality can be achieved by using a strong encryption algorithm combined with a strong and complex passphrase.

4. **Integrity:**

- Integrity means that data is not viewed or manipulated by an unauthorized, or even an authorized, user during storage or transit.
- Technically, users can assure data integrity in transit by using hashing, which provides a mechanism to ensure that data has not been tempered with or changed during transmission.
- While the data is at rest, integrity can be achieved by physically controlling access to server/network device rooms, restricting access to data.

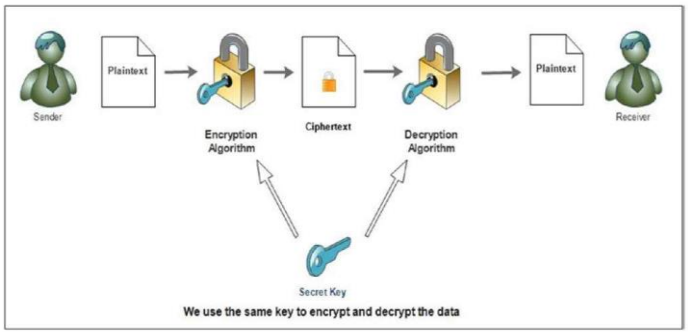
Cryptographic Types

- There are different classifications of cryptographic algorithms. The most common one is classifying them according to the number of security keys used in the encryption/decryption process.
- A cryptographic algorithm works in combination with a key (a number, word, or phrase) to encrypt and decrypt data. This key is composed of a string of bits. The larger the key (contains more bits), the greater the number of patterns that can be created, thus making it harder to break.

1. **Symmetric Cryptography**

- Also known as secret key cryptography (SKC).
- In this type of encryption, both the sender and the receiver use the same key to encrypt and decrypt the data.
- The main disadvantage of this scheme is that the entire operation is dependent on the secrecy of the key.
- If the key is compromised by an unauthorized party, the whole system is breached.

- Symmetric encryption algorithms are split into stream ciphers and block ciphers Stream ciphers encrypt plaintext bits individually, whereas block ciphers encrypt an entire block of plaintext bits at a time as a single unit.
- Some of the popular symmetric encryption algorithms are AES/ Rijndael Blowfish, CAST 5 DES, IDEA, RC 2 RC 4 RC 6 Serpent, Triple DES, and Twofish.



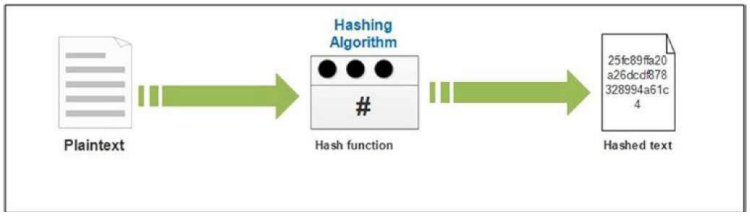
2. **Asymmetric Cryptography**

- Also known as public key cryptography (PKC).
- This cryptographic schema uses two different keys for encryption and decryption The two keys are mathematically linked.
- However, no one can derive the decryption key (private key) from the encryption key (public key).
- In asymmetrical cryptography, the public key can be distributed freely however, the private key should be kept secret to avoid collapsing the whole system.
- The public key is used to encrypt the secret message or to verify the digital signature of the sender, while the private key is used to decrypt the scrambled message or to create a digital signature.
- Popular asymmetric encryption algorithms are the RSA encryption algorithm, Diffie Hellman, Digital Signature Algorithm, ElGamal ECDSA, and XTR.

Cryptographic Hash

- A cryptographic hash function (also called a digest) converts a digital file (and returns a fixed size value, which is called the hash value.
- To ensure the integrity of a file (or any piece of data), a hash of a file can be sent to accompany the file.

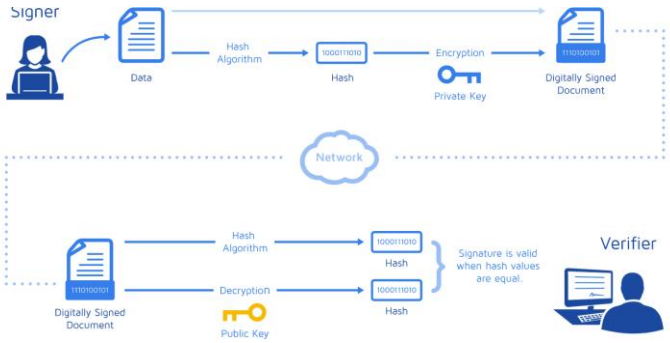
- The receiver may then compute a hash of the data received and compare it with the hash received. If the two outputs match, then you can assert that a message has not been tampered with.
- There are different hash functions, the most popular of which are MD 5 SHA 1 and SHA 256. The best secure hash algorithm is the one that has the best speed and is collision resistant.



Digital Signature

- A digital signature is a way to assure that an e mail or digital file is authentic.
- A digital signature is considered the digital equivalent of a handwritten signature or a rubber stamp.
- A digital signature is based on asymmetric cryptography (public key).
- For example, to have your e mail signed, you need first to generate two keys (private and public keys).
- The signing software (such as an e mail client like Thunderbird) creates a hash (also called a message digest) of the data that you are going to sign. The private key is used then to encrypt the hash.
- The result is the digital signature. Finally, the e mail client appends the digital signature to the e mail. Now all the data that was hashed has been signed

How Digital Signature Works?



The Difference Between Digital Signatures and Electronic Signatures

Digital Signature	Electronic Signature
Secure a document.	Verify a document.
Authorized and regulated by CA.	Not authorized.
Comprised of more security features.	Comprised of less security features.
Common types of digital signature are based on Adobe and Microsoft.	Main types of electronic signature include verbal, hand signature, checkbox and others.
Can be verified.	Cannot be verified.
Preferred more than electronic signature due to high levels of authenticity	Easy to use but less authentic
Particularly concerned about securing the document	Shows intent to sign the contract

Cryptographic Systems Trust Models

- Cryptographic systems are designed to form the basis of information security.
- In a cryptographic schema, there are a number of methods to assure that the person you are communicating with is really the authorized party.
- The following are the most popular trust models:
- The Web of Trust concept is used in Pretty Good Privacy (PGP) and other Open PGP compatible systems.
- Kerberos is a distributed authentication service designed to provide strong authentication for client server applications by using secret key cryptography.
-
- A certification authority (CA) is a third party entity that issues a digital certificate to authenticate a user's ownership of a public key.

Web of Trust

- The Web of Trust is used in Pretty Good Privacy and other compatible systems to establish a trust relationship between a public key and its owner.
- It is a decentralized security model in which participants authenticate the identities of other users.
- The Web of Trust is similar to social networking web sites.

- A user can add unknown people to his or her list of friends if they already have friends in common.
- Examples are Facebook and LinkedIn.
- For example, if Susan trusts Nihad, then Susan could also trust the public key of Rita, who does not know if this key has been authenticated by Nihad.

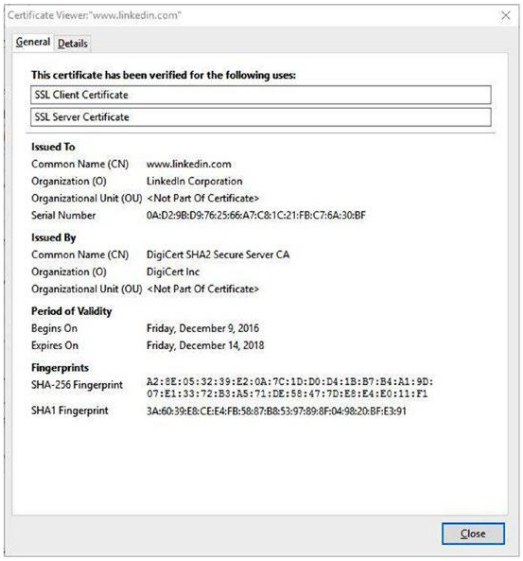
Kerberos

- Kerberos is a network authentication protocol developed by MIT It works through a client server architecture by using secret key cryptography.
- Kerberos provides secure authentication between the user and server rather than a host to host approach.
- The main component of a Kerberos schema is a central server (or a trusted third party server) used for authenticating requests.
- In a Kerberos network, each connected host has its own secret key, and one of these hosts is the central Kerberos server, also known as a key distribution center (KDC).
- All host secret keys will be stored on the KDC server.
- Kerberos provides secure communication by checking each connected host's secret key with the one stored on it (the host can do the same with the Kerberos server).
- After a client and server have used Kerberos to assure their identities, they can begin to exchange encrypted data across an unsecured network such as the Internet.

Certificates and Certificate Authorities

- Certificate authorities (CAs) issue digital certificates for web sites, online services, IoT devices, and individuals.
- These certificates contain their identity credential in order to be recognized and trusted online (trusted because CA has already verified the identity of each digital certificate holder).
- CAs play a critical role in today's digital age.
- They build trust relationships between different business partners online, encrypt business transactions, and secure the communications between different parties conducting e-commerce transactions.

- A digital certificate is like your passport You can use it within your country to verify your identity.
- If you are in the United States and your passport is issued from New York, you can safely use it in Washington.
- The local authorities in Washington will recognize and trust your personal information because your passport is issued by a government agency they trust (New York authorities).
- If you moved outside the United States, foreign countries that accept U S passports will also verify and trust your details, because they trust in the government papers issued by U S authorities.



Sample Digital Certificate Linkedin.com

Disk Encryption Using Open Source Tools

- The main advantage of open source solutions is that they don't have backdoors (although an audit should be performed before using any program).
- This does not mean all proprietary solutions have one, but the open source solutions can be reviewed by the public for possible backdoors or for any feature that might facilitate an attack against their cryptographic algorithm.
- Open source encryption software also has being more stable and interoperable.

- Closed software is usually linked to one vendor, which can impose restrictions on its usage and the other system that can integrate with it.
- Disk Encryption
- Disk encryption is a technology which protects information by converting it into code that cannot be deciphered easily by unauthorized people or processes.
- It is used to prevent unauthorized access to data storage.

Encryption Using VeraCrypt

- VeraCrypt can encrypt the Windows partition, fixed drive data partitions, and removable media, and it can create encrypted containers to store sensitive information.
- VeraCrypt also supports plausible deniability through the following:
  1. It supports hidden volumes and hidden operating system.
  2. Encrypted VeraCrypt devices and volumes look as if they are full of random data; they contain no signature for being a VeraCrypt container.

Multitask Encryption Tools

- 7 Zip: 7 Zip (www 7 zip org) is open source archiver software that works on all Windows versions (beginning from NT).
- It allows you to compress and encrypt data using the AES 256 encryption algorithm.
- Using it is simple;
- just right click the file or folder you want to compress and select Z Zip ➤ Add to archive.

Encryption Using VeraCrypt

1. AES Crypt:

- AES (Advanced Encryption Standard) Crypt (https://www.aescrypt.com) is a free, open source program.
- Integrates with the Windows right click context menu.
- It uses AES 256 encryption to do its job.

- To encrypt a file, right click the file and select AES Encrypt Then enter the password to lock the file another file with the same name but with AES extension will appear in the same directory.
- To decrypt it, right click the encrypted result and select AES Decrypt. Then enter its password The encrypted file should appear unencrypted in the same directory with its original extension.

2. **Protect Microsoft Office Files:**

- All Microsoft Office documents beginning with Microsoft Office 2007 can be protected with a password to prevent others from opening or modifying your documents.
- This feature uses AES 128 by default.

Steps involved are :

1. In Microsoft Office 2007, click the Microsoft Office button and select Prepare ➤ Encrypt Document.
2. Type your password and confirm it.
3. Then click OK.
4. Finally, save the changes to your file.

3. Protect PDF Files:

PDF documents are used widely for both personal and business use.

1. To protect a PDF file with a password, open the file you want to protect, select File ➤ Properties, and go to the Security tab.
2. From the Security Method drop down menu, select Password Security.
3. Another window will pop up where you should select the option “Require a password to open the document” and type the password in the corresponding field.
4. Click the OK button, and another pop up window will appear asking you to confirm your password. Type it again and click OK.