Fundamentals of Information Security (S22)

> Prof. Shinnazar Seytnazarov
>
> Summarized by Igor Mpore

Lecture 1: Introduction to Computer Security

1.1 Computer Security

Defined as measures and controls that ensure **confidentiality**, **integrity**, and **availability** of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.

1.2. Three key objectives (the CIA triad)

- Confidentiality: no disclosure to unauthorized parties
- Integrity: no modification of information by unauthorized parties
- Availability: System or resource shall be available for its intended use.

1.3. Levels of security breach impact

- Low: the loss will have a limited impact, e.g., a degradation in mission or minor damage.
- Moderate: the loss has a serious effect, e.g., significance degradation on mission or significant harm to individuals but no loss of life or threatening injuries
- High: the loss has severe or catastrophic adverse effect on operations, organizational assets or on individuals (e.g., loss of life)

1.4. Examples of security requirements confidentiality

- Student grade information: high confidentiality and only available when approved
- Student enrollment: moderate confidentiality
- Directory information: low confidentiality
- Patient's allergy information: high confidentiality since it's integrity should be high enough
- A system that provides authentication: High confidentiality

1.5. Computer Security Challenges

- Not simple
- Unexpected attacks
- Procedures used are often counter-intuitive
- Must decide where to deploy mechanics
- Involves algorithms and secret information
- Many battles between Admin and attackers
- Requires constant monitoring

- Regarded as hindrance to using system

1.6. Model for Computer Security

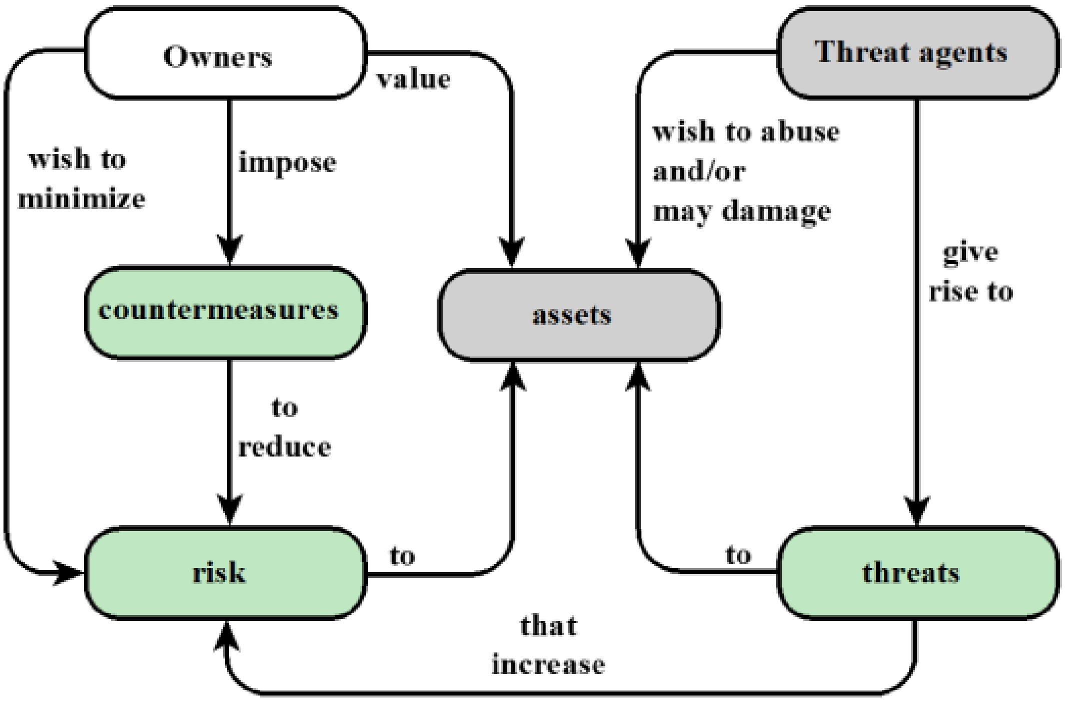


Figure 1.2 Security Concepts and Relationships

1.7 Components of Computer Security

- System Resources (Assets of Computer Security):
  - Hardware
  - Software
  - Data
  - Communication facilities and Networks
- Our Vulnerabilities concern
- Treats that exploit vulnerabilities
- Attack is a threat that already occured out
  - **Active attack**: attacker tries to modify content of the message
  - **Passive attack**: the attacker reads and copies content of a message and can use it for malicious purposes
  - **Internal attacks a.k.a Insider:** An internal attack occurs when an individual or a group within an organization seeks to disrupt operations or exploit organizational assets Ex: selling companies data after being fired for money
  - **External attacks a.k.a Outsider:** An external threat relates to outsider attacks on the part of individuals attempting to gain unauthorized access to the network of the targeted organization.
- Countermeasures: actions taken to prevent, detect, recover and minimize risks

1.8 Vulnerabilities, Threats and Attacks

- Categories of vulnerabilities
  - Corrupted: loss of intergrity
  - Leaky: loss of confidentiality
  - Unavailable or very slow: loss of availability
- Treats
  - Capable of exploiting vulnerabilities
  - Represent potential security harm to an asset
- Attacks (threats carried out)
  - Types explained above 👆

1.9 Fundamentals of Security Design Principles

1. Economy of mechanism: security mechanism should be as simple as possible
2. Fail-safe defaults: unless a subject is given explicit access to an object, it should be denied access to that object
3. Complete mediation: all accesses to objects should be checked to ensure they are allowed
4. Open design: the security of a mechanism should not depend on the secrecy of its design or implementation
5. Separation of privilege: system should not grant permission based upon a single condition
6. Least privilege: a user is given the minimum levels of access – or permissions – needed to perform his/her job functions.
7. Least common mechanism: that mechanisms used to access resources should not be shared
8. Psychological acceptability: security mechanisms should not make the resource more difficult to access than if the security mechanisms were not present
9. Isolation: least privilege and privilege separation
10. Encapsulation: is a form of isolation which is designed on the principle of object-oriented principles. Here the processes of the protected system can only access the data object of the system and these processes can only be invoked from a domain entry point.
11. Modularity: network security should be multilayered, with many different techniques used to protect the network. No security mechanism can be guaranteed to withstand every attack. Therefore, each mechanism should have a backup mechanism
12. Layering: approach that deploys multiple security controls to protect the most vulnerable areas of your technology environment where a breach or cyberattack could occur.
13. Least astonishment: It proposes that a component of a system should behave in a way that most users will expect it to behave.

Lecture 2: Cryptographic tools

2.1 Symmetric Encryption

Also known as single key Encryption. It has two requirements for secure use which are:\

- Needs a strong encryption Algorithm
- Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure

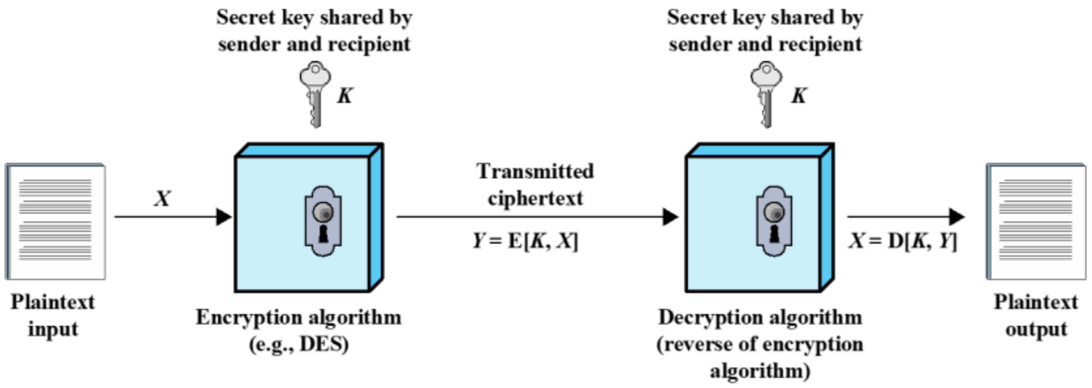
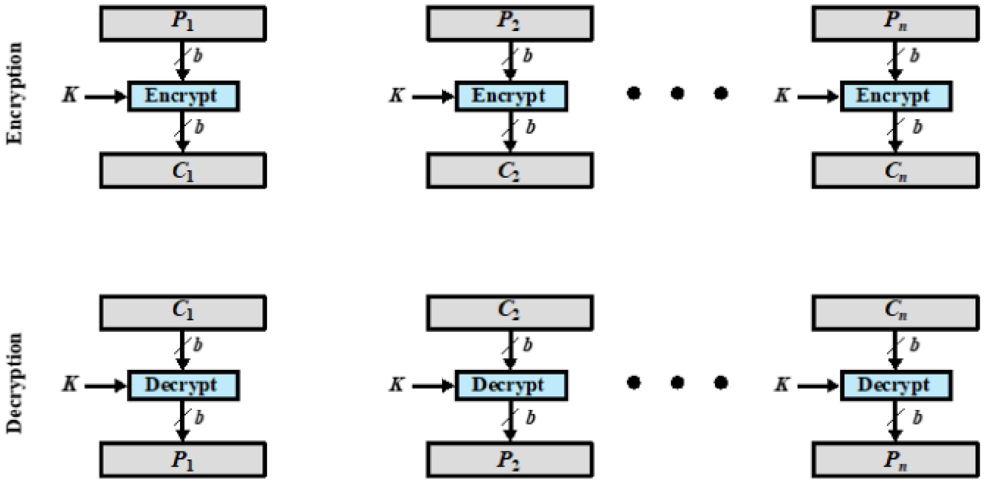

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E[K, X]
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

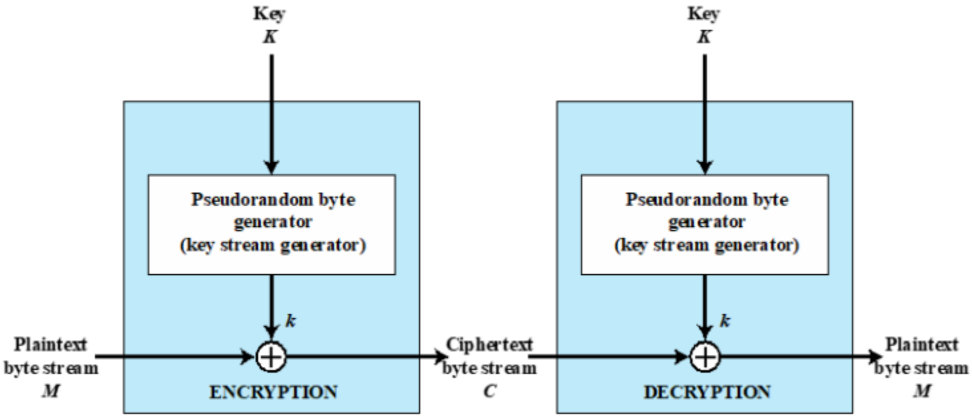
Figure 2.1 Simplified Model of Symmetric Encryption

2.1.1 Types of Symmetric Encryption

1. Block Cipher:
   - This is the most common type of Symmetric encryption which processes the input one block of elements at a time and produces the output block for each input block.
   - In addition to that, it can reuse keys



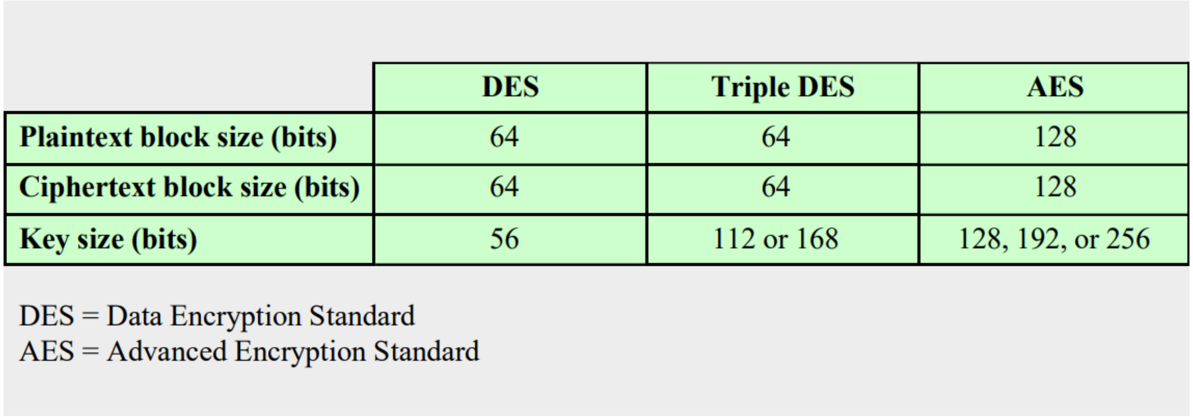
2. Stream Cipher:
   - It processes input elements continuously (one byte at a time) and produces output of one element at a time.
   - It's almost always faster and has far less code


Key
K
Pseudorandom byte generator (key stream generator)
k
Plaintext byte stream M
ENCRYPTION
Ciphertext byte stream C
Key
K
Pseudorandom byte generator (key stream generator)
k
DECRYPTION
Plaintext byte stream M

2.1.2 Three popular symmetric Encryption

1. DES (Data Encryption Standard): uses 64 bit plaintext block and 56 bit key to produce a 64 bit ciphertext block
2. Triple DES: repeats basic DES algorithm three times using either two or three unique keys
3. AES (Advanced Encryption Standard): Uses symmetric block cipher with 128 bit data & 128/192/256 bit keys. it's now widely available commercially.

Their comparison

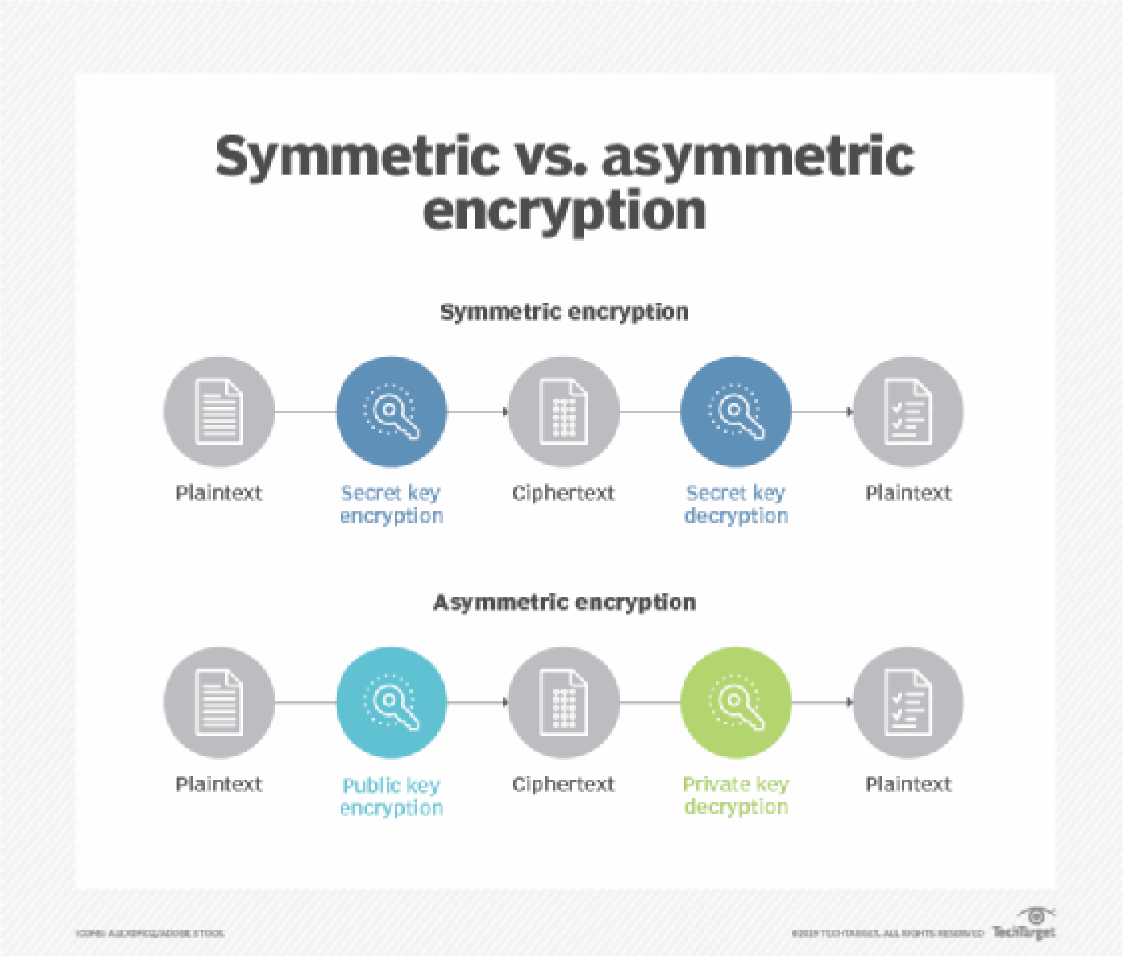


	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard
AES = Advanced Encryption Standard

2.2 Asymmetric Encryption

a.k.a Public-key Crytography. It uses pairs of keys that consists of a **public key and a private key**. The generation of such key pairs depends on cryptographic algorithms which are based on mathematical problems termed one-way functions.



2.3 Cryptographic systems

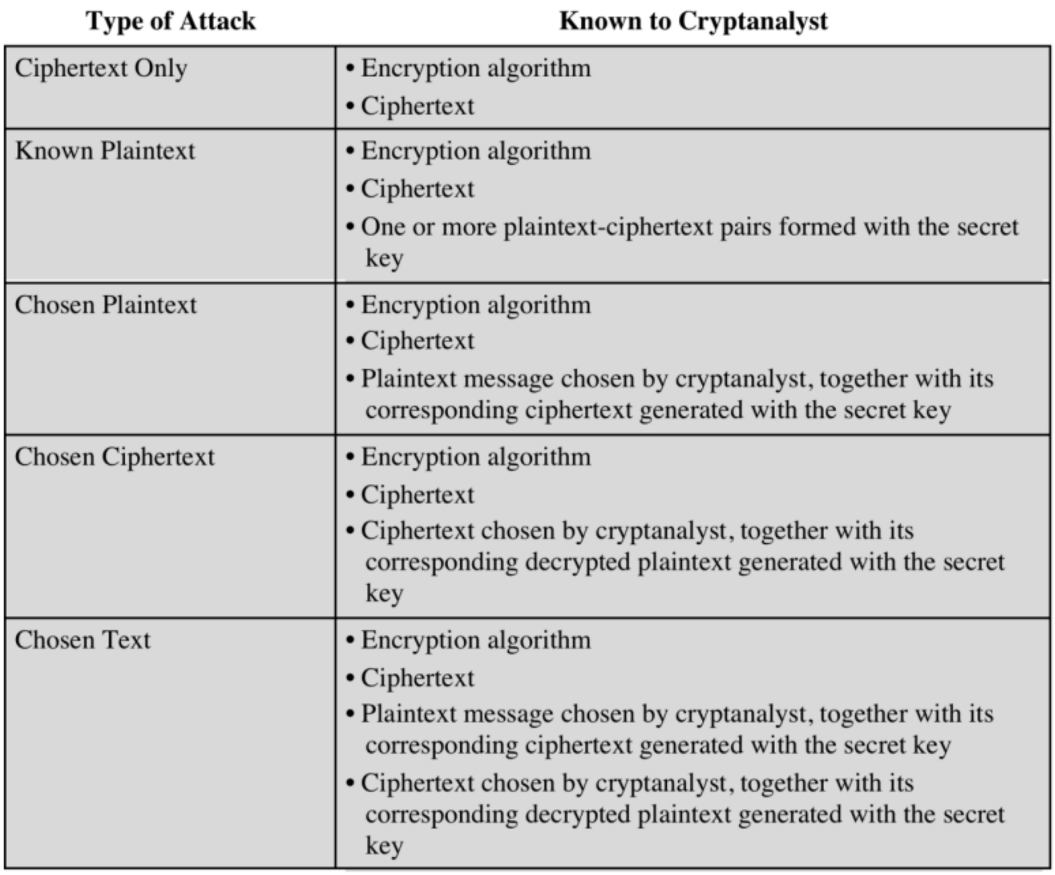
They are 3 independent dimensions:

- Type of Operations used
  - Substitution
  - Transposition
  - Rotor machine
  - XOR cipher
- Number of keys
  - Symmetric, single key,secret key, conventional encryption
  - Asymmetric, two key, a.k.a public-key encryption
- The way the plaintext is processed
  - block cipher
  - stream cipher

2.4 Attacking symmetric encryption

1. Cryptanalysis:
   - Involves relying on the nature of the algorithm, plaintext characteristics and sometimes samples of plaintext-ciphertext pairs.

   Types of cryptanalysis attacks



Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

2. Brute-force attack:
    - Involves trying all possible keys on some ciphertext intil you get an intelligible translation into plaintext.

2.5 Simple Ciphers (link)

1. Substitution ciphers

   Involves replacing every group of plaintext letters with another predefined group.

   Ex: Caesar Cipher

2. Transposition ciphers

   transposition ciphers rearrange the original message letters.

   Ex: Rail Fence Cipher

1. Rotor machines

   Electric rotor machines were mechanical devices that allowed to use encryption algorithms that were much more complex than ciphers, which were used manually.

   Ex: Enigma, Bomber

2. Simple XOR

   This algorithm adds subsequent plaintext bytes to secret key bytes using XOR operation. After using the last secret key byte, one should return to the first byte.

   Ex: M XOR K = C , C XOR K = M

2.6 Steganography

Steganography works **by hiding information in a way that doesn't arouse suspicion**. One of the most popular techniques is 'least significant bit (LSB) steganography. In this type of steganography, the information hider embeds the secret information in the least significant bits of a media file such as photo, video or even audio.

1. Image Steganography (link)
2. Audi Steganography (link)
3. Video Steganography (link)
4. Covert channels: Tunnelshell (ICMP link)

Lecture 3: Cryptographic tools

3.1 Message Authentication

Message encryption is good against passive attack and then message authentication protects against message authentication. To achieve authentication, sender and receiver can share a common key. Depending on the environment, the security system decides if both message encryption and authentication is neccessary or one is enough.8