Terminologies

- **Plaintext:** Message or data which are in their normal, readable (not crypted) form.
- **Encryption:** Encoding the contents of the message in such a way that hides its contents from outsiders.
- **Ciphertext**: The encrypted message

Terminologies

- **Decryption:** The process of retrieving the plaintext back from the ciphertext.

- **Key:** Encryption and decryption usually make use of a key, and the coding method is such that decryption can be performed only by knowing the proper key.

Terminologies

- **Cryptography** is the art or science of keeping messages secret. It deals with all aspects of secure messaging, authentication, digital signatures, electronic money, and other applications.

- **Cryptosystems:** A cryptographic system (cryptosystem) consists of a pair of data transformations, namely encryption and decryption.

Terminologies

- **Cryptanalysis:** The art of **breaking** ciphers, i.e. retrieving the plaintext without knowing the proper key.

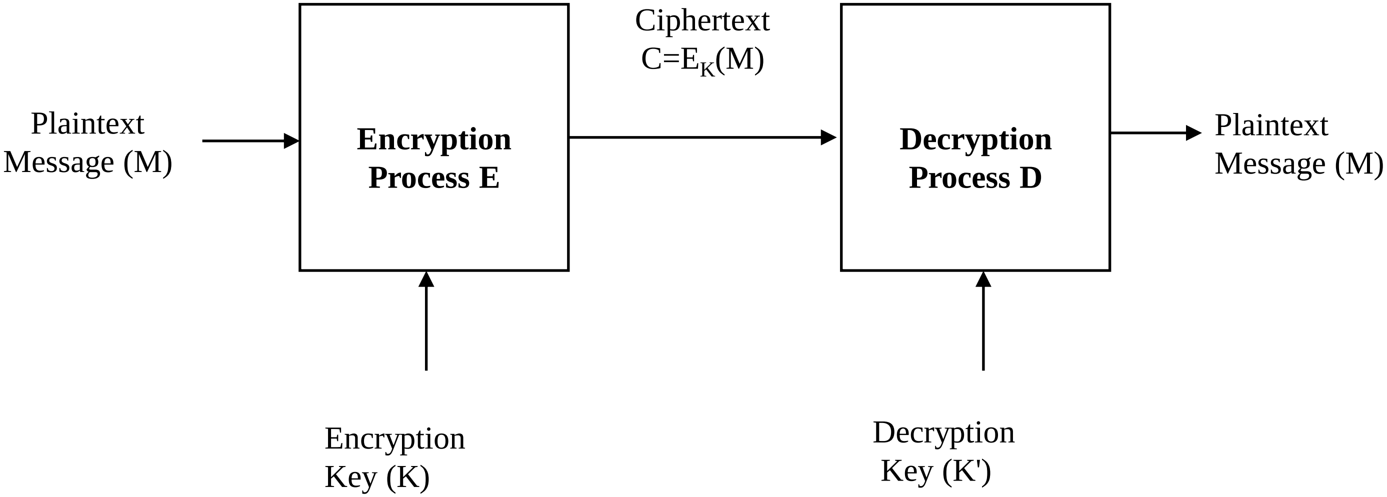
- **Cryptographers:** People who do cryptography

- **Cryptanalysts:** practitioners of cryptanalysis

Conventional Cryptosystem Principles

- **An cryptosystem has the following five ingredients:**
  - Plaintext
  - Encryption algorithm
  - Secret Key
  - Ciphertext
  - Decryption algorithm
- **Security depends on the secrecy of the key, not the secrecy of the algorithm**

Conventional Cryptosystem Principles

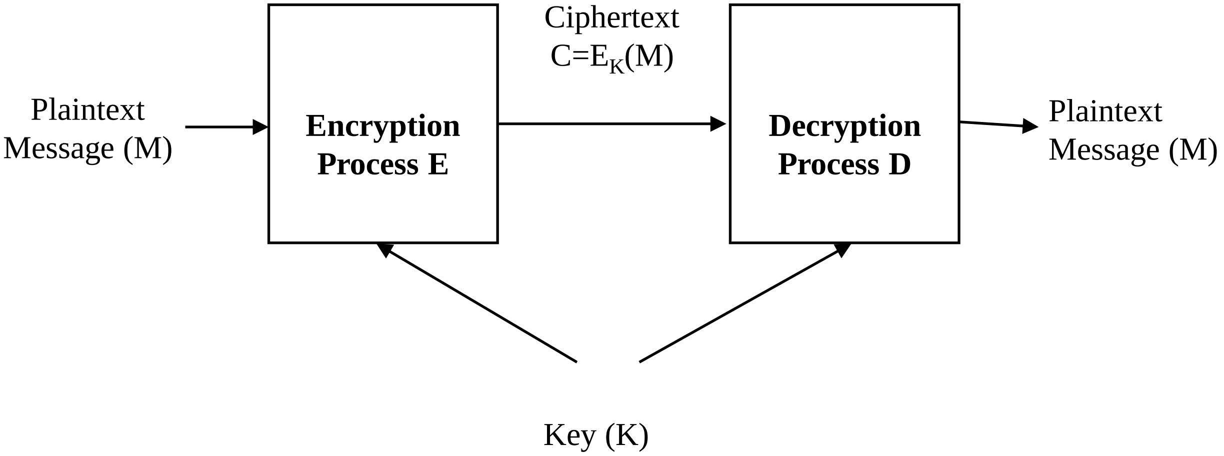


Classifications

- **Classification of cryptosystems**
  - Symmetric cryptosystems
  - Asymmetric cryptosystems

Symmetric Cryptosystem

- The same key is used for both encryption and decryption purposes



Symmetric Cryptosystem

- Examples of symmetric cryptosystem are Data Encryption Standard (DES)

- Problem : How do we distribute the key securely?

Key Distribution

- A key could be selected by A and physically delivered to B.
- A third party could select the key and physically deliver it to A and B.
- If A and B have previously used a key, one party could transmit the new key to the other, encrypted using the old key.

Key Distribution

- If A and B each have an encrypted connection to a third party C, C could deliver a key on the encrypted links to A and B.

- **Session key:**
  - Data encrypted with a one-time session key.At the conclusion of the session the key is destroyed

Assymmetric Cryptosystem

- Different keys are used for encryption and decryption purposes.

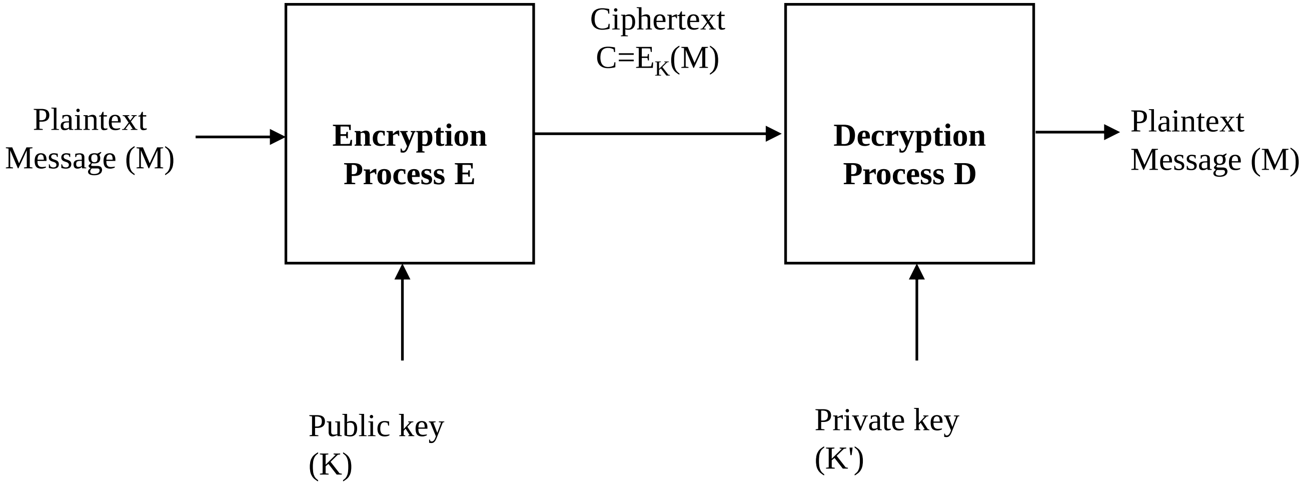
- The pair of keys are mathematically related and consist of a public key that can be published without doing harm to the system's security and a private key that is kept secret.

- Also known as public key cryptosystems

Assymmetric Cryptosystem

- The public key is used for encryption purposes and lies in the public domain.
- Anybody can use the public key to send an encrypted message.
- The private key is used for decryption purposes and remains secret.
- An example of a public cryptosystem is the RSA cryptosystem.

Assymmetric Cryptosystem



Encyption – can it be broken?

- Theoretically, it is possible to devise unbreakable cryptosystems

- However, practical cryptosystems almost always are breakable, given adequate time and computing power

- The trick is to make breaking a cryptosystem hard enough for the intruder

Types of Ciphers

- Ciphers can be broadly classified into the following two categories depending upon whether

  (i) a symbol of plaintext is immediately converted into a symbol of ciphertext (Stream Ciphers)

  (ii) or a group of plaintext symbols are converted as a block into a group of ciphertext symbols (Block Ciphers)

Stream Ciphers

- A symbol of plaintext is immediately converted into a symbol of ciphertext
- **Advantages**
  - Speed of transformation
  - Low error propagation
- **Disadvantages**
  - Low diffusion
  - Susceptible to malicious insertions and modifications

Block Ciphers

- A group of plaintext symbols are converted as a block into a group of ciphertext symbols
- **Advantages**
  - Diffusion
  - Immunity to insertions
- **Disadvantages**
  - Slowness of encryption
  - Error propagation

General Types of Ciphers

- **Substitution ciphers**
  - Letters of the plaintext messages are replaced with other letters during the encryption

- **Transposition ciphers**
  - The order of plaintext letters is rearranged during encryption

General Types of Ciphers

- **Product ciphers**
  - Combine two or more ciphers to enhance the security of the cryptosystem

Trends

- **Block size:** larger block sizes mean greater security
- **Key Size:** larger key size means greater security
- **Number of rounds:** multiple rounds offer increasing security

Monoalphabetic Substitution Ciphers

- **Caesar cipher**

  $c_i=E(p_i)=p_i+3 \; mod \; 26$

  Plaintext: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

  Ciphertext: d e f g h i j k l m n o p q r s t u v w x y z a b c

- **Example**

  Plaintext: CRYPTOGRAPHY IS GREAT FUN

  Ciphertext: fubswrjudskb lv juhdw

Polyalphabetic Substitution Ciphers

- Flatten the frequency distribution of letters by combining high and low distributions

- **Example:**

Plaintext: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Ciphertext1: a d g j m p s v y b e h k n q t w z c f i l o r u x

Ciphertext2: n s x c h m r w b g l q v a f k p u z e j o t y d i

Plaintext: VIGENERE TABLEAUX

Ciphertext: lbshnhzh fndqmniy

Transposition Ciphers

- Rearrangement of the letters or a message

Columnar transposition

Plaintext	Ciphertext
W H Y D O	welrnel
E S I T A	hswatta
L W A Y S	yiaihhn
R A I N I	dtyneed
N T H E N	oasinrs
E T H E R	
L A N D S	

Characteristics of good cipher

- **Shannon characteristics**
  - The amount of secrecy should determine the amount of labor appropriate for the encryption and decryption
  - The set of keys and encryption algorithm should be free of complexity
  - The implementation of the process should be as simple as possible

Characteristics of good cipher

- Errors in encryption should not propagate and cause corruption of further information in the message.
- Ciphertext size should not be larger than plaintext

- **Confusion**
  - The change in ciphertext triggered by an alteration in the plaintext should be unpredictable

Characteristics of good cipher

- **Diffusion**
  - Change in the plaintext should affect many parts of the ciphertext

- **Other issues**
  - Perfect secrecy vs. Effective secrecy
  - Redundancy of languages
  - Unicity distance

Methods of attack

- **Ciphertext-only attack**
  - The attacker gets a ciphertext and tries to find the corresponding plaintext.

- **Known-plaintext attack**
  - The attacker has some plaintext and its matching ciphertext. The task is to find a key corresponding to this match.

Methods of attack

- **Chosen-plaintext attack**
  - Here, the attacker selects a plaintext and ciphers it using the cryptotechinque he attacks. The plaintext may be chosen to ease the task of key finding.

Application of Cryptography

- Confidentiality
- Authentication
- Message Integrity
- Digital Signature