Introduction and Classical Ciphers

Unit-1 [7 Hours]

Terminology

- Security
- Computer Security
- Information Security
- Network Security
- Cryptography
- Cryptosystem
- Cryptology
- Cryptoanalysis

Security

- Security, in information technology (IT), is the defense of digital information and IT assets against internal and external, malicious and accidental threats.
- This defense includes detection, prevention and response to threats through the use of security policies, software tools and IT services.

Computer Security

- It is a process and the collection of measures and controls that ensures the Confidentiality, Integrity and Availability (CIA) of the assets in computer systems.
- Computer Security protects you from both software and hardware part of a computer systems from getting compromised and be exploited.

Information Security

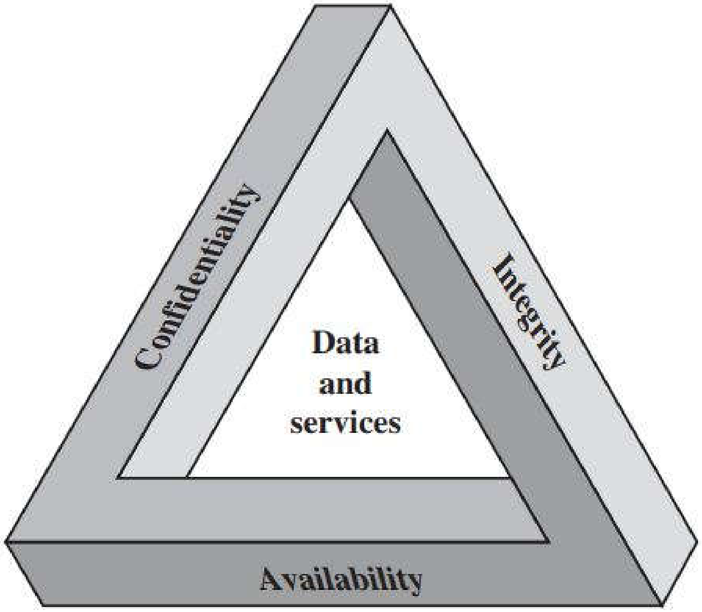
- Information security is primarily concerned with making sure that data in any form is kept secure in terms of preserving its confidentiality, integrity and availability.
- Information is a significant asset that can be stored in different ways such as digitally stored, printed, written on papers or in human memory. It can be communicated through different channels such as spoken languages, gestures or using digital channel such as email, SMS, social media, video, audio etc.
- Information security differs from cybersecurity such that information security aims to keep data in any form secure, whereas cybersecurity protects only digital data. Cybersecurity is the subset of information security.

Network Security

- It is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies.
- An effective network security manages access to the network. It targets a variety of threats and stop them from entering or spreading on your network.
- Network security, a subset of cybersecurity, aims to protect any data that is being sent through devices in your network to ensure that the information is not changed or intercepted.

CIA Triad

- Confidentiality, Integrity, and Availability is called **CIA Triad**.
- It is a model designed to guide policies for information security within an organization.



Confidentiality

- Confidentiality is the concealment of information of resources.
- This term covers two related concepts:

- **Data confidentiality**: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
- **Privacy**: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

Integrity

- Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change.
- This term covers two related concepts:
  - **Data integrity:** Assures that information and programs are changed only in a specified and authorized manner.
  - **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Availability

- Availability refers to the ability to use the information or resource desired.
- Assures that systems work promptly and service is not denied to authorized users.

In addition to CIA Triad

- Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present complete picture. Two of the most commonly mentioned are:
  - Authenticity
  - Accountability

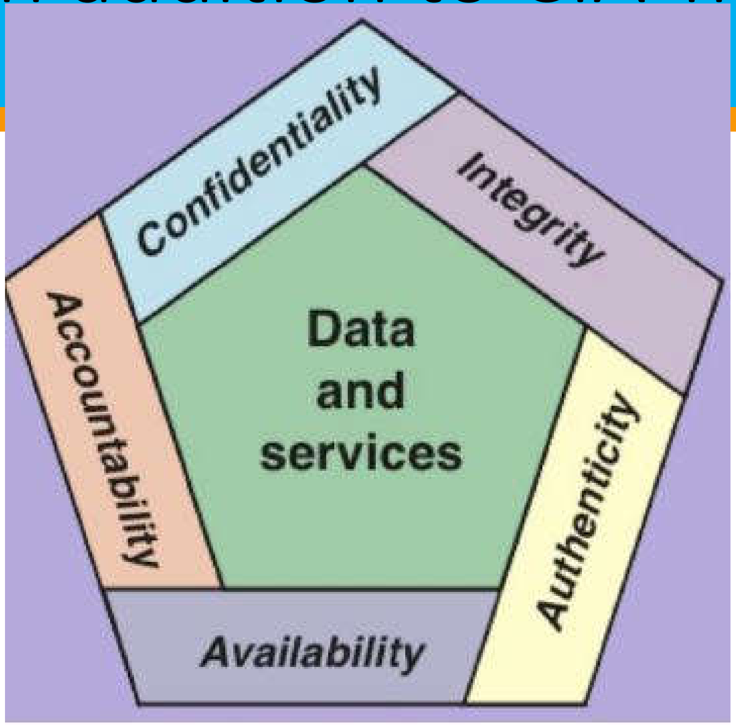


Figure: Essential Network and Computer Security Requirements

Authenticity

- The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
- Authenticity is assurance that a message, transaction, or other exchange is from source it claims to be from, i.e. proof of identity

Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely that entity.
- It means that every individual who works with an information system should have specific responsibilities for information assurance.
- Security must keep records of the activities to permit later forensic analysis to trace security breaches or to aid in transactins disputes.

Security

- A fundamental goal for a cryptosystem is for it to be "**secure**".
- **But what does it means to be secure and how can we gain confidence that something is indeed secure?**
- Security in cryptography involves consideration of three different aspects: an *attack model*, an *adversarial goal*, and a *security level*.
- The attack model specifies the information that is available to the adversary. (protocol, public key)
- The adversarial goal specifies exactly what is means to "break" the cryptosystem.
- The security level attempts to quantify the effort required to break the cryptosystem.

Security

- A statement of security for a cryptographic scheme will assert that a particular adversarial goal cannot be achieved in a specified attack model, given specified computational resources.

Cryptography

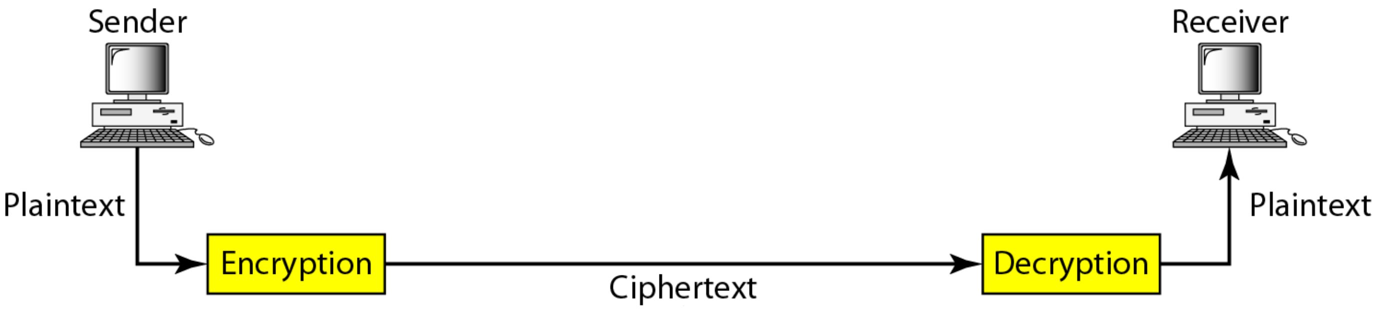
- Cryptography, a word with Greek origins, means “secret writing.” and is the art and science of concealing meaning.
- The Concise Oxford English Dictionary (9th ed.) defines cryptography as “*the art of writing or solving codes*." This is historically accurate, but does not capture the current breadth of the field or its modern scientific foundations. The definition focuses solely on the codes that have been used for centuries to enable secret communication.
- But cryptography nowadays encompasses much more than this: it deals with mechanisms for ensuring integrity, techniques for exchanging secret keys, protocols for authenticating users, electronic voting, cryptocurrency, and more.
- Modern cryptography involves *the study of mathematical techniques for securing digital information, systems, and distributed computations against adversarial attacks.*
- It involves three distinct mechanisms: symmetric-key encipherment, asymmetric-key encipherment, and hashing.
- In short, *the art and science of keeping message secure* is **cryptography**, and it is practiced cy **cryptographers**.

Cryptography

- Cryptography is the techniques of converting ordinary plain text into unintelligible text and vice-versa.
- Cryptography is the practice and study of techniques for secure communication in the presence of third parties.
- Techniques used for deciphering message without any knowledge of the enciphering details fall into the area of **cryptanalysis**. Cryptanalysis is what the layperson calls "*breaking the code*". Cryptanalysts are practitioners of cryptanalysis (the art and science of breaking ciphertext)
- The branch of mathematics encompassing both cryptography and cryptanalysis together are called **cryptology** and its practitioners are **cryptologists**.

Terminology

- Suppose a **sender** wants to send a message to a **receiver**. Moreover, this sender wants to send the message securely: She wants to make sure an eavesdropper cannot read the message.
- A message is **plaintext** (sometimes called cleartext). The process of disguising a message in such a way as to hide its substance with the help of ***key*** is **encryption**. An encrypted message is **ciphertext**. The process of turning ciphertext back into original plaintext is **decryption**; it also uses a ***key***.
- Encryption and decryption algorithms are referred as ***ciphers***


Sender
Receiver
Plaintext
Encryption
Ciphertext
Decryption
Plaintext

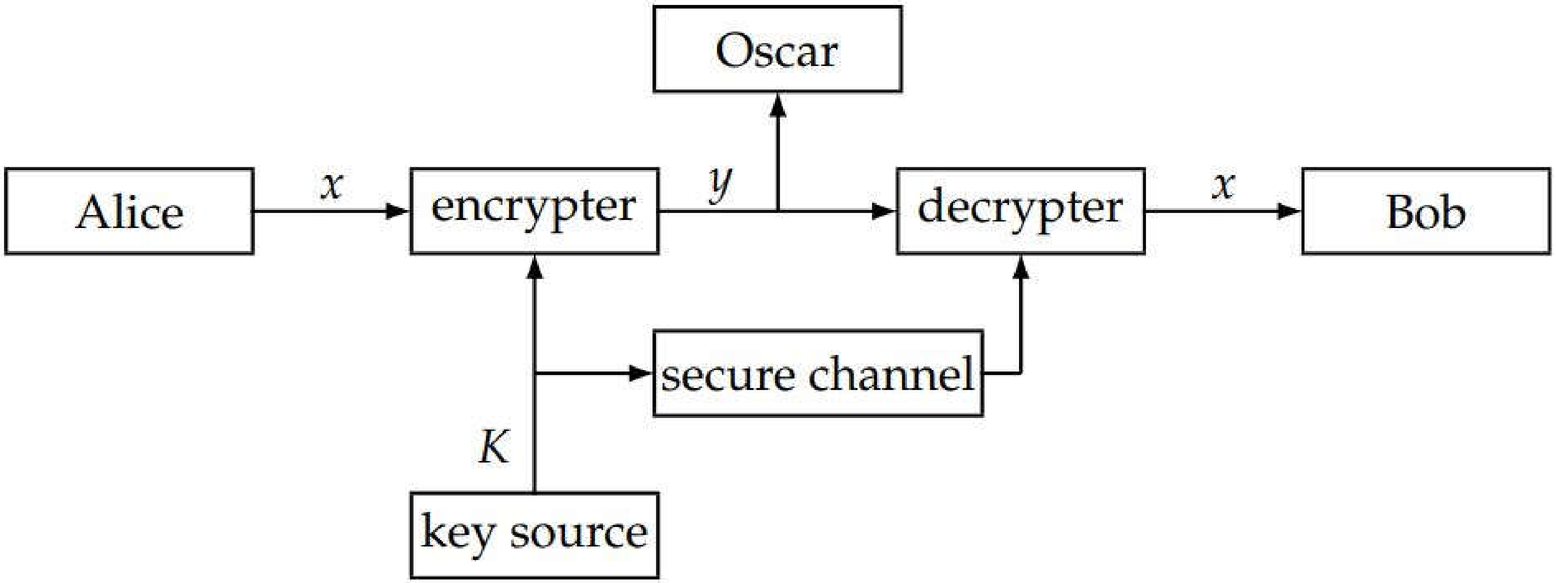
Terms

- **Plain text**: Original message fed to encryption algorithm; readable.
- **Encryption algorithm**: changes plain text to coded ciphertext by various substitution and transformation methods. The process of converting plaintext to ciphertext is called *enciphering* or *encryption*.
- **key**: input to the encryption algorithm. Known to sender and receiver only.
- **Ciphertext**: coded/scrambled output message by the algorithm. Different secret key applied on plain text produces different ciphertext.
- **Decryption Algorithm**: the encryption algorithm that run in reverse i.e. takes ciphertext and key to produce the original transmitted plain text. The process is known as *deciphering* or *decryption*.

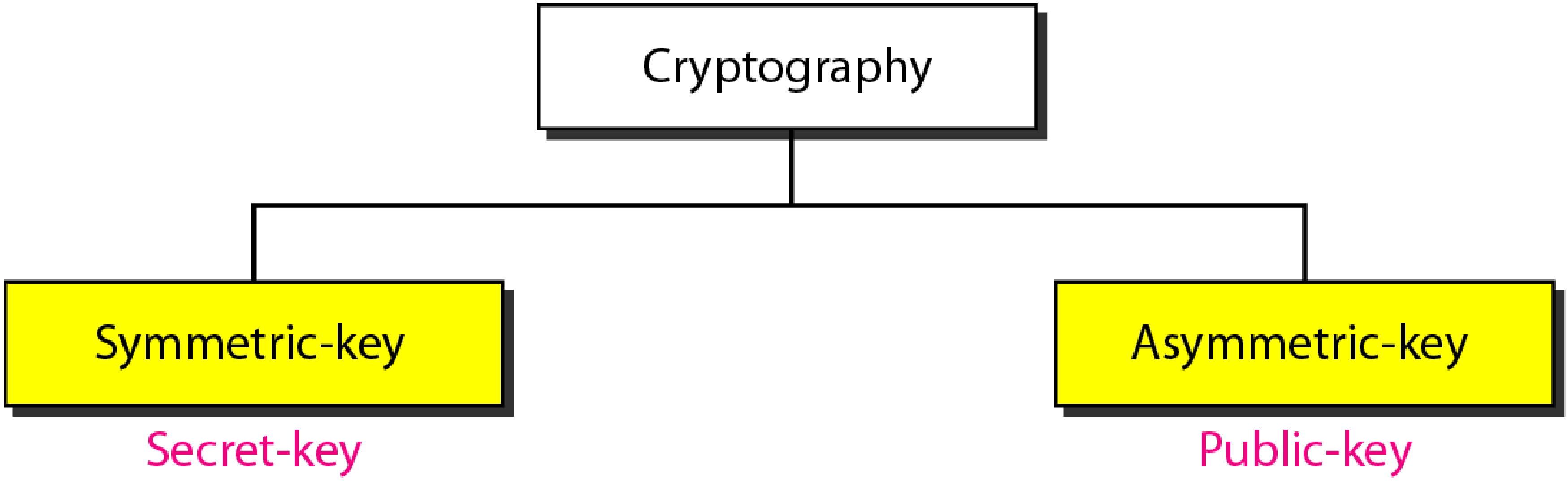
Cryptosystem: Definition

- A ***cryptosystem*** is a five tuple ($\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}$) where the following conditions are satisfied:
- $\mathcal{P}$ is a finite set of possible *plaintexts*;
- $\mathcal{C}$ is a finite set of possible *ciphertexts*;
- $\mathcal{K}$, the *keyspace*, is a finite set of possible *keys*;
- For each K ε $\mathcal{K}$, there is a encryption rule e_K ε $\mathcal{E}$, and a corresponding decryption rule d_K ε $\mathcal{D}$. Each eK : $\mathcal{P} \rightarrow \mathcal{C}$ and d_K : $\mathcal{C} \rightarrow \mathcal{P}$ are functions such that $d_K(e_K(x)) = x$ for every plaintext element x ε $\mathcal{P}$.

The Communication Channel



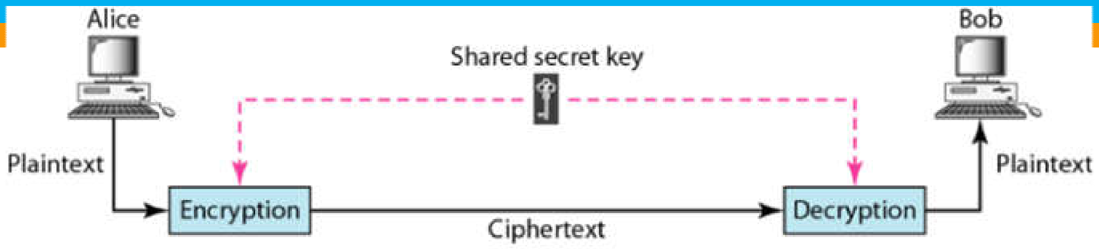
Cryptography Category



Symmetric Key Cryptography

- Symmetric encryption (also called *classical cryptosystems*), also referred to as *conventional encryption*, *secret-key*, or single-key encryption, was the only type of encryption in use prior to the development of public-key encryption in the late 1970s.
- Same key is shared by sender (for encryption) and receiver (for decryption).
- Ciphertext is generated either by *substitution* or *transformation* method by encryption algorithm.
- A symmetric encryption has five ingredients:
    - Plaintext
    - Encryption algorithm
    - Secret key
    - Ciphertext
    - Decryption algorithm

Symmetric Key Cryptography



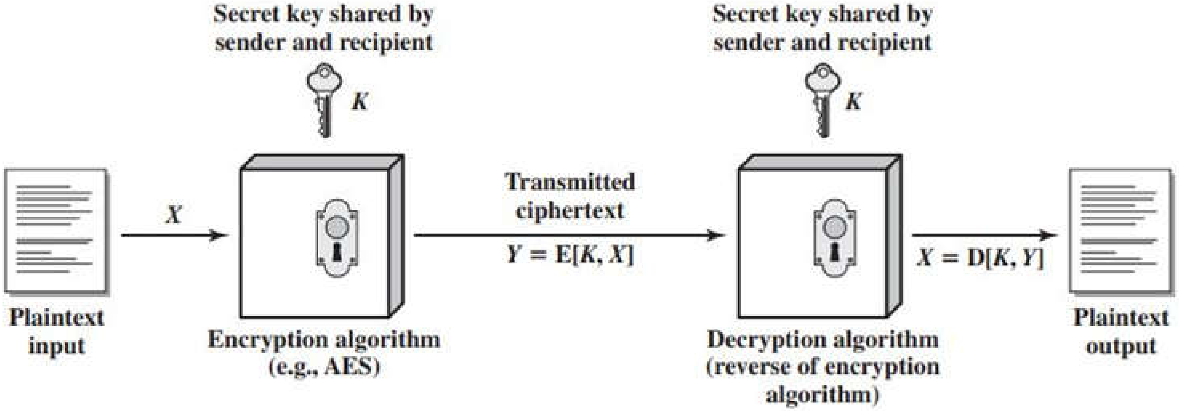

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E[K, X]
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure: Simplified Model of Symmetric Encryption

Symmetric Key Cryptography

- There are two requirements for secure use of symmetric encryption:

1. We need a strong algorithm.
   - At minimum, an operator who knows the algorithm and has access to one or more ciphertext would be unable to decipher the ciphertext.
2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

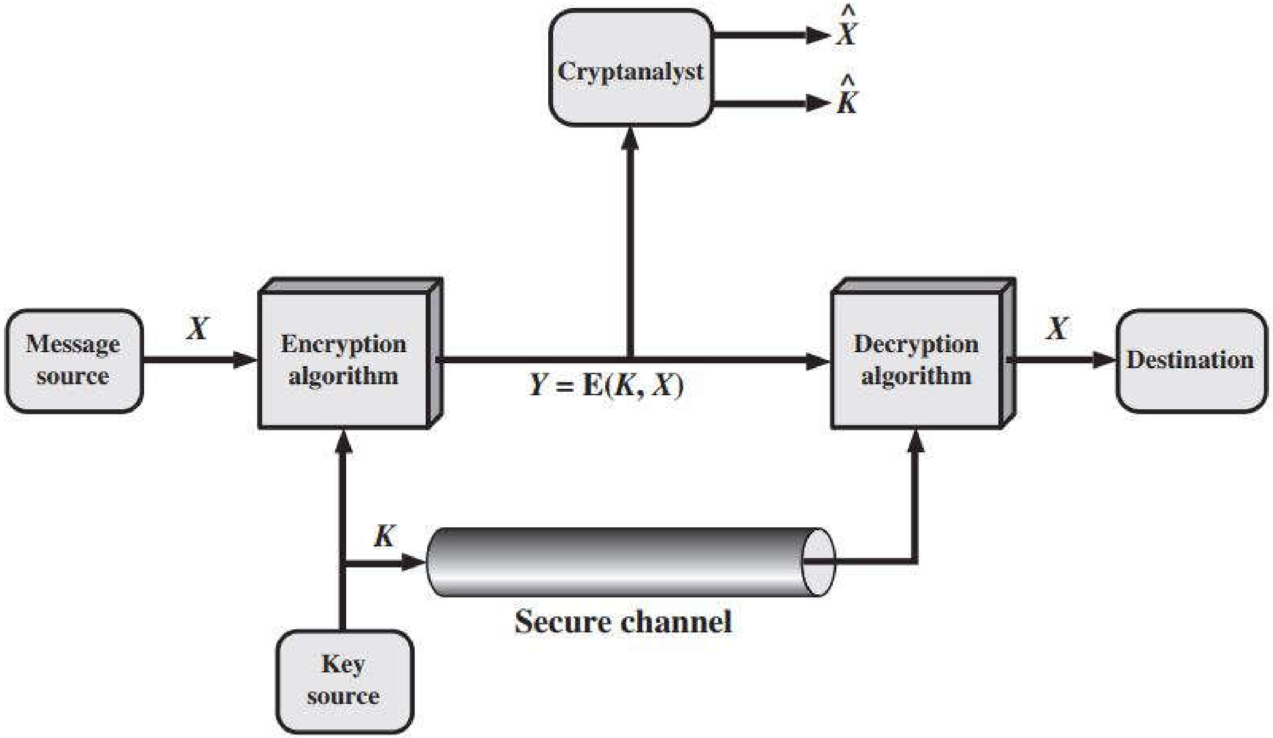


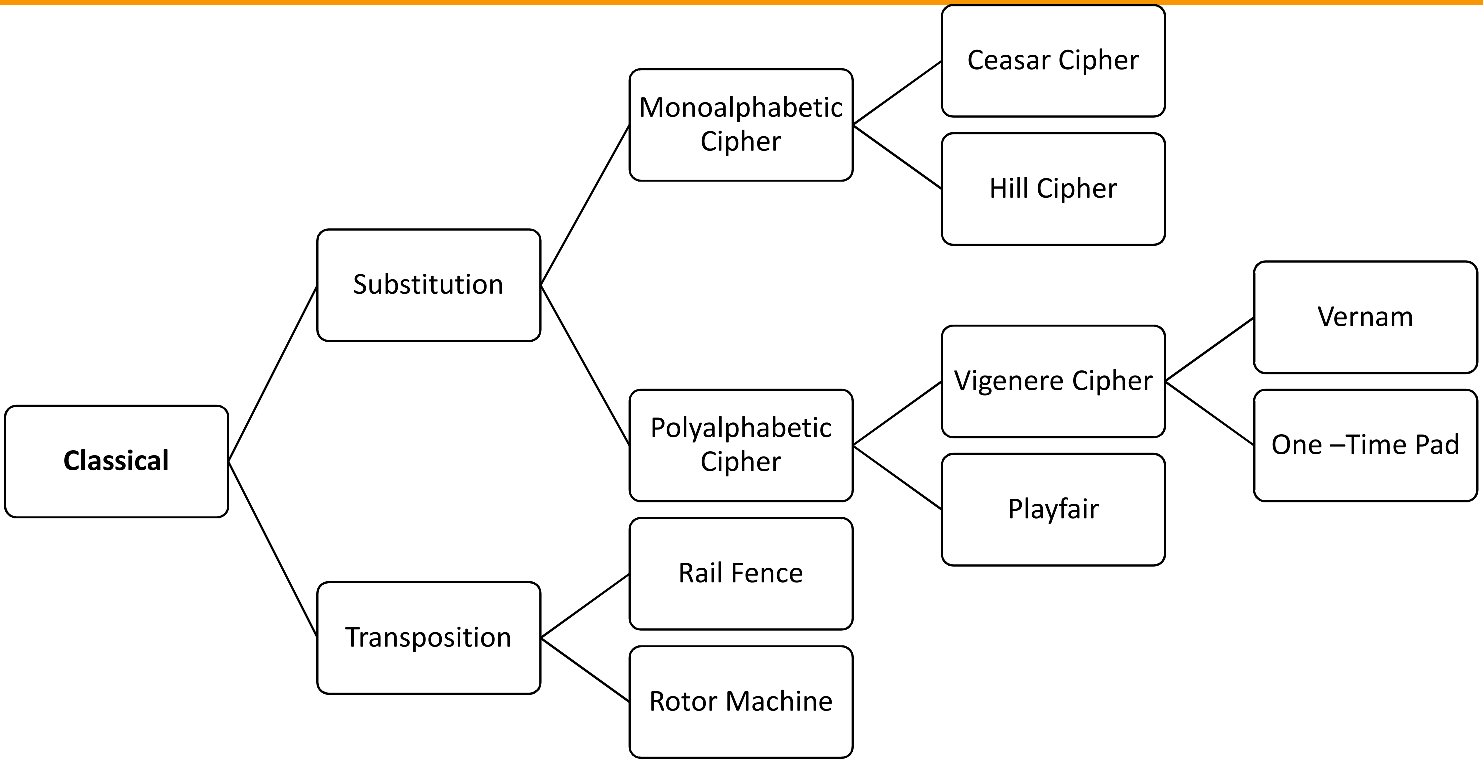
Figure: Model of Symmetric Cryptosystem

Cryptographic System Characteristics

The type of operations used for transforming plaintext to ciphertext.

1. **All encryption algorithms are based on two general principles**: *substitution*, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and *transposition*, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (i.e., that all operations are reversible). Most systems, referred to as product systems, involve multiple stages of substitutions and transpositions.
2. **The number of keys used**. If both sender and receiver use the same key, the system is referred to as *symmetric, single-key, secret-key, or conventional encryption*. If the sender and receiver use different keys, the system is referred to as *asymmetric, two-key, or public-key encryption*.
3. **The way in which the plaintext is processed**. A *block cipher* processes the input one block of elements at a time, producing an output block for each input block. A *stream cipher* processes the input elements continuously, producing output one element at a time, as it goes along.

Symmetric/Classical/Single-Key Cryptosystem



Substitution Cipher

- A substitution technique is one in which **the letters of plaintext are replaced by other letters or by numbers or symbols**.
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.
- For example: Caesar cipher, Vigenere Cipher, One-time pad are example of substitution cipher.

Caesar Cipher

- earliest known Substitution cipher
- by Julius Caesar
- Shift cipher: involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.
- Earliest known and simplest substitution scheme developed by Julis Ceasar.

  plain: meet me after the toga party

  cipher: PHHW PH DIWHU WKH WRJD SDUWB
- A Caesar cipher is susceptible to a statistical ciphertext-only attack

Cesear Cipher

- can define transformation as:

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
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

- mathematically give each letter a number

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- then have Caesar cipher as:

$$c = \mathrm{E}(p) = (p + k) \bmod (26)$$

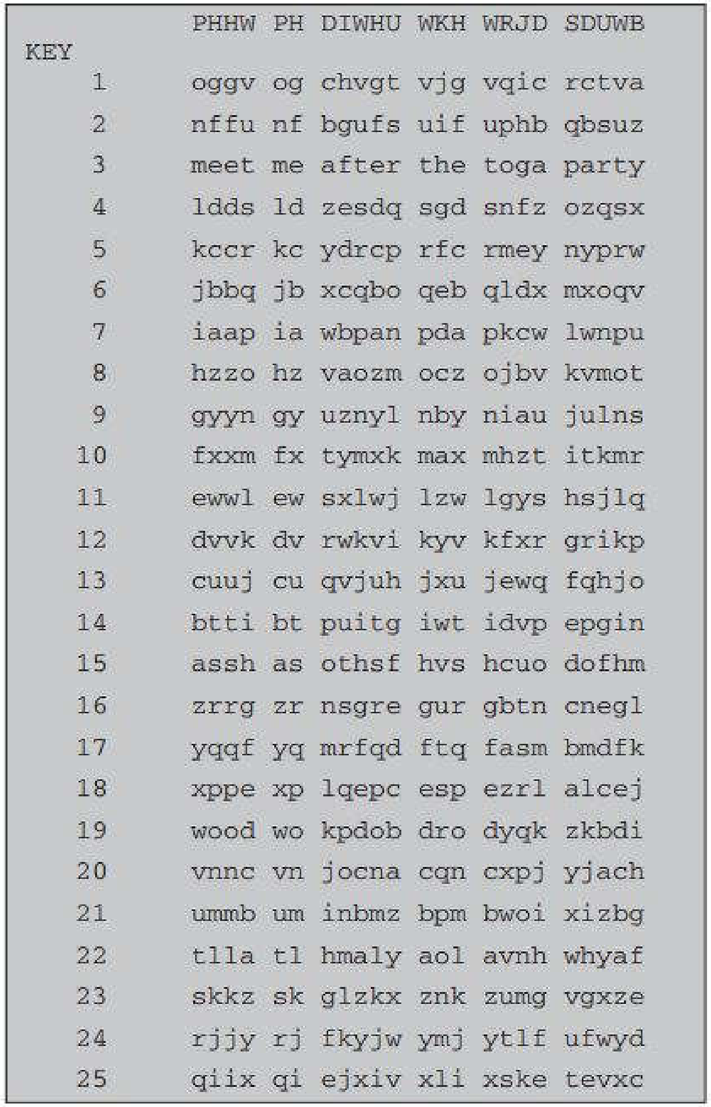
$$p = \mathrm{D}(\mathrm{c}) = (\mathrm{c} - k) \bmod (26)$$

Cryptanalysis of Caesar Cipher

- only have 26 possible ciphers
  - A maps to A,B,..Z
- could simply try each in turn
- a **brute force search**
- given ciphertext, just try all shifts of letters
- do need to recognize when have plaintext
- eg. break ciphertext "GCUA VQ DTGCM"

Problem with Ceasar Cipher

- Three important characteristics of this problem enabled us to use a bruteforce cryptanalysis:
  1. The encryption and decryption algorithms are known.
  2. There are only 25 keys to try.
  3. The language of the plaintext is known and easily recognizable.



```
            PHHW PH DIWHU WKH WRJD SDUWB
KEY
    1       oggv og chvgt vjg vqic rctva
    2       nffu nf bgufs uif uphb qbsuz
    3       meet me after the toga party
    4       ldds ld zesdq sgd snfz ozqsx
    5       kccr kc ydrcp rfc rmey nyprw
    6       jbbq jb xcqbo qeb qldx mxoqv
    7       iaap ia wbpan pda pkcw lwnpu
    8       hzzo hz vaozm ocz ojbv kvmot
    9       gyyn gy uznyl nby niau julns
   10       fxxm fx tymxk max mhzt itkmr
   11       ewwl ew sxlwj lzw lgys hsjlq
   12       dvvk dv rwkvi kyv kfxr grikp
   13       cuuj cu qvjuh jxu jewq fqhjo
   14       btti bt puitg iwt idvp epgin
   15       assh as othsf hvs hcuo dofhm
   16       zrrg zr nsgre gur gbtn cnegl
   17       yqqf yq mrfqd ftq fasm bmdfk
   18       xppe xp lqepc esp ezrl alcej
   19       wood wo kpdob dro dyqk zkbdi
   20       vnnc vn jocna cqn cxpj yjach
   21       ummb um inbmz bpm bwoi xizbg
   22       tlla tl hmaly aol avnh whyaf
   23       skkz sk glzkx znk zumg vgxze
   24       rjjy rj fkyjw ymj ytlf ufwyd
   25       qiix qi ejxiv xli xske tevxc
```

Figure: Brute Force Cyrptanalysis of Caesar Cipher

Monoalphabetic Ciphers

- rather than just shifting the alphabet could shuffle (jumble) the letters arbitrarily
- each plaintext letter maps to a different random ciphertext letter.
- Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if ‘A’ is encrypted as ‘D’, for any number of occurrences in that plaintext, ‘A’ will always get encrypted to ‘D’ .

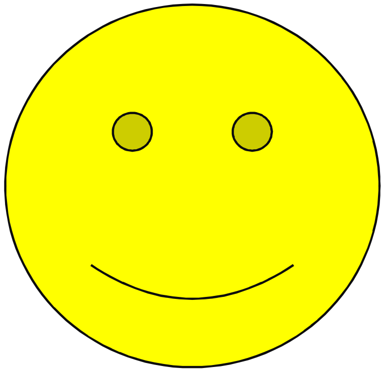
```
Plain:  abcdefghijklmnopqrstuvwxyz
Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext:  ifwewishtoreplaceletters
Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA
```

Monoalphabetic Cipher Security

- now have a total of 26! = 4 x 10^{26} possible keys

with so many keys, might think is **secure**



problem is language characteristics

Cryptanalysis on Monoalphabetic Cipher

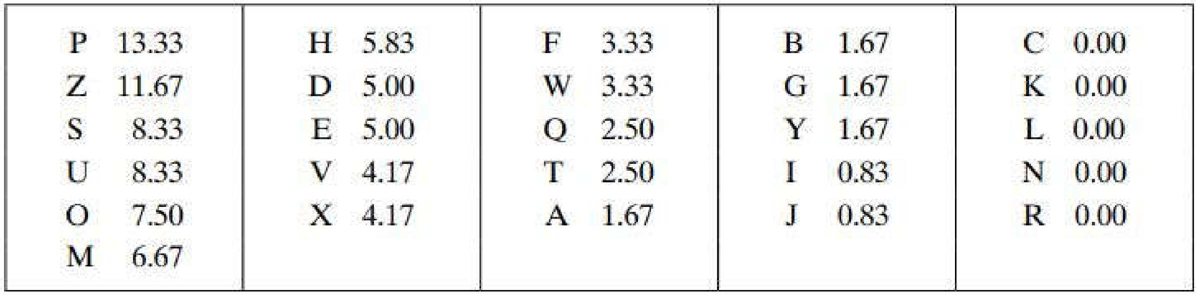
- If the cryptanalyst knows the nature of the plaintext (e.g., on compressed English text), then the analyst can exploit the regularities of the language.
- calculate letter frequencies for ciphertext
- compare counts/plots against known values
- if caesar cipher look for common peaks/troughs
  - peaks at: A-E-I triple, NO pair, RST triple
  - troughs at: JK, X-Z
- for monoalphabetic must identify each letter
  - tables of common double/triple letters help

Example: Cryptanalysis

- given ciphertext:

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

- count relative letter frequencies



P	13.33	H	5.83	F	3.33	B	1.67	C	0.00
Z	11.67	D	5.00	W	3.33	G	1.67	K	0.00
S	8.33	E	5.00	Q	2.50	Y	1.67	L	0.00
U	8.33	V	4.17	T	2.50	I	0.83	N	0.00
O	7.50	X	4.17	A	1.67	J	0.83	R	0.00
M	6.67								

Example: Cryptanalysis

- given ciphertext:

  UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
  VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
  EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
- count relative letter frequencies
- guess P & Z are e and t
- guess ZW is th and hence ZWP is the
- proceeding with trial and error finally get:

  it was disclosed yesterday that several informal but
  direct contacts have been made with political
  representatives of the viet cong in moscow

Playfair Cipher

- *not even the large number of keys in a monoalphabetic cipher provides security*
- one approach to improving security was to encrypt multiple letters
- the **Playfair Cipher** is an example
- invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair

Playfair Key Matrix

- a 5X5 matrix of letters is constructed based on a keyword
- fill in letters of keyword
- fill rest of matrix with other letters
- eg. using the keyword MONARCHY

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

Encrypting and Decrypting

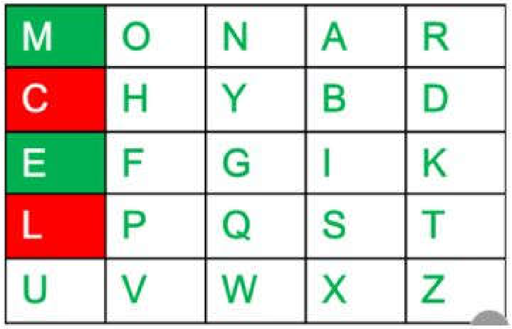
- plaintext is encrypted two letters at a time
  1. if a pair is a repeated letter, insert filler like 'X’, so that balloon would be treated as ba lx lo on.
  2. if both letters fall in the same row, replace each with letter to right.
     For example, ar is encrypted with RM.
  3. if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom) For example, mu is encrypted with CM.
  4. otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

Example: Playfair Cipher

- plaintext: instruments
- after split: 'in' 'st' 'ru' me' 'nt' 'sz'

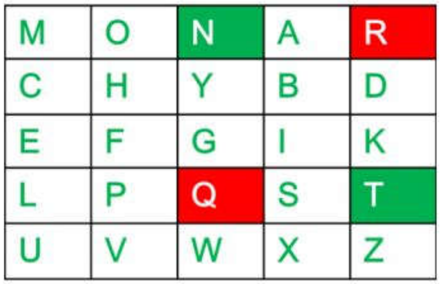
- 'ME' → 'CL'
- 'ST' → 'TL'
- 'NT' → 'RQ'

- ciphertext: 'GATLMZCLRQTX



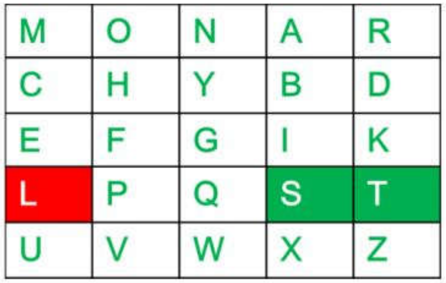
M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

'ME' → 'CL'



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

'NT' → 'RQ'



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

'ST' → 'TL'

Polyalphabetic Ciphers

- **polyalphabetic substitution ciphers**
- improve security using multiple cipher alphabets
- make cryptanalysis harder with more alphabets to guess and flatter frequency distribution
- use a key to select which alphabet is used for each letter of the message
- use each alphabet in turn
- repeat from start after end of key is reached
- example: Vigenere Cipher, One-Time-Pad

Vigenere Cipher

- simplest polyalphabetic substitution cipher
- effectively multiple caesar ciphers
- key is multiple letters long $K = k_1 \ k_2 \ ... \ k_d$
- i^{th} letter specifies i^{th} alphabet to use
- use each alphabet in turn
- repeat from start after d letters in message
- decryption simply works in reverse

Example of Vigenere Cipher

- write the plaintext out
- write the keyword repeated above it
- use each key letter as a caesar cipher key
- encrypt the corresponding plaintext letter
- eg using keyword *deceptive*

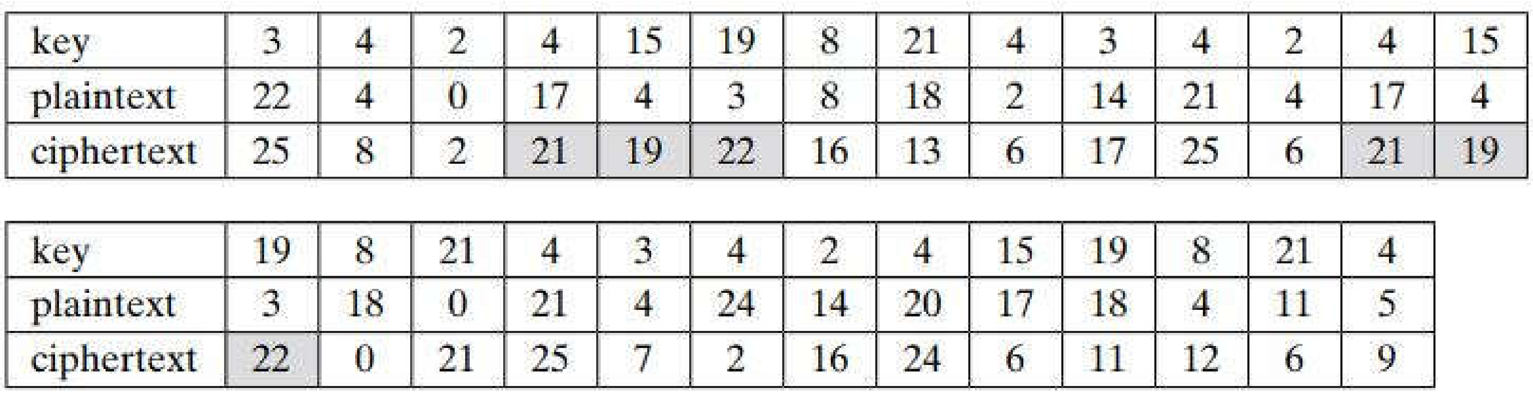
```
key:       deceptivedeceptivedeceptive
plaintext: wearediscoveredsaveyourself
ciphertext:ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

Example of Vigenere Cipher

eg using keyword *deceptive*

```
key:       deceptivedeceptivedeceptive
plaintext: wearediscoveredsaveyourself
ciphertext:ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

Expressed numerically, we have the following result.



key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
plaintext	22	4	0	17	4	3	8	18	2	14	21	4	17	4
ciphertext	25	8	2	21	19	22	16	13	6	17	25	6	21	19

key	19	8	21	4	3	4	2	4	15	19	8	21	4
plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5
ciphertext	22	0	21	25	7	2	16	24	6	11	12	6	9

Vigenere Cipher Algorithm

- We can express the Vigenère cipher in the following manner. Assume a sequence of plaintext letters $P = p_0, p_1, p_2, c, p_{n-1}$ and a key consisting of the sequence of letters $K = k_0, k_1, k_2, \ldots\ldots K_{m-2}, k_{m-1}$, where typically $\boldsymbol{m < n}$.
- The sequence of ciphertext letters $C = C_0, C_1, C_2, c, C_{n-1}$ is calculated as follows:
  $C = C_0, C_1, C_2, c, C_{n-1} = \mathrm{E}(K, P) = \mathrm{E}[(k_0, k_1, k_2, c, k_{m-1}), (p_0, p_1, p_2, c, p_{n-1})]$
  $= (p_0 + k_0) \bmod 26, (p_1 + k_1) \bmod 26, c, (p_{m-1} + k_{m-1}) \bmod 26,$
  $(p_m + k_0) \bmod 26, (p_{m+1} + k_1) \bmod 26, c, (p_{2m-1} + k_{m-1}) \bmod 26$

Cryptanalysis of Vegenere Cipher

- There are multiple ciphertext letters for each plaintext letter, one for reach unique letter of the keyword.
- an improvement is achieved over the Playfair cipher, but considerable frequency information remains, so susceptible to statistical technique as in other case of polyalphabetic ciphers.

Autokey Cipher

- ideally want a key as long as the message
- Vigenère proposed the **autokey** cipher with keyword is prefixed to message as key
- knowing keyword can recover the first few letters
- use these in turn on the rest of the message
- but still have frequency characteristics to attack
- eg. given key *deceptive*

```
key:        deceptivewearediscoveredsav
plaintext:  wearediscoveredsaveyourself
ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA
```

One-Time Pad

- if a truly random key as long as the message is used, the cipher will be secure
- called a One-Time pad
- is unbreakable since ciphertext bears no statistical relationship to the plaintext
- since for **any plaintext** & **any ciphertext** there exists a key mapping one to other
- can only use the key **once** though
- problems in generation & safe distribution of key

Example: One Time Pad

- Suppose that we are using a Vigenère scheme with 27 characters in which the twenty-seventh character is the space character, but with a one-time key that is as long as the message. Consider the ciphertext:
- ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

We now show two different decryptions using two different keys:

ciphertext:	ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:	*pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih*
plaintext:	MR MUSTARD WITH THE CANDLESTICK IN THE HALL
ciphertext:	ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
key:	*pftgpmiydgaxgoufhklllmhsqdqogtewbqfgyovuhwt*
plaintext:	miss scarlet with the knife in the library

Which is the correct key?

No Answer

Is One-Time Pad breakable

- one-time is entirely due to randomness of the key.
- Two fundamental difficulties:
  - making large quantities of random keys
  - problem of key distribution an protection

Hill Cipher

- Hill cipher is a multi-lettered substitution cipher based on linear algebra.
- Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, ..., Z = 25 is used, but this is not an essential feature of the cipher.
- To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26.
- To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.
- The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26).

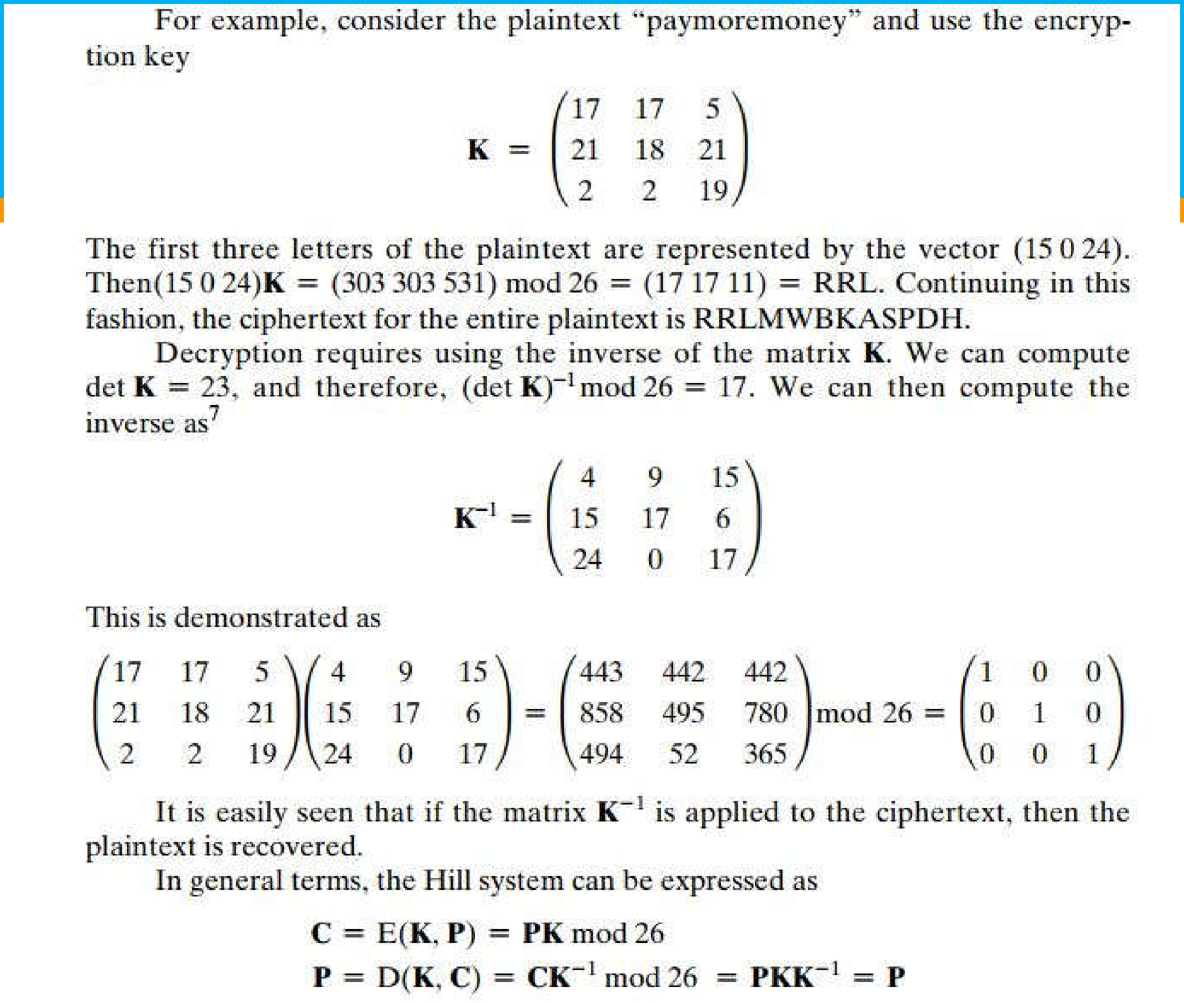
Algorithm: Hill Cipher

- Let m = 3 and plaintext x = (p_1, p_2, p_3), then ciphertext c = (c_1, c_2, c_3) can be calculated as:

- $(c_1, c_2, c_3) = (p_1, p_2, p_3)\begin{bmatrix} k11 & k12 & k13 \\ k21 & k22 & k23 \\ k31 & k32 & k33 \end{bmatrix} \text{mod } 26$

- $c_1 = (k11*p_1 + k21 * p_2 + k31 * p_3)$ mod 26
- $c_2 = (k12*p_1 + k22 * p_2 + k32 * p_3)$ mod 26
- $c3 = (k13*p_1 + k23 * p_2 + k33 * p_3)$ mod 26

Example: Hill Cipher



For example, consider the plaintext "paymoremoney" and use the encryption key

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

The first three letters of the plaintext are represented by the vector (15 0 24). Then$(15\ 0\ 24)\mathbf{K} = (303\ 303\ 531) \bmod 26 = (17\ 17\ 11) =$ RRL. Continuing in this fashion, the ciphertext for the entire plaintext is RRLMWBKASPDH.

Decryption requires using the inverse of the matrix **K**. We can compute det **K** = 23, and therefore, $(\det \mathbf{K})^{-1} \bmod 26 = 17$. We can then compute the inverse as[7]

$$\mathbf{K}^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

This is demonstrated as

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

It is easily seen that if the matrix $\mathbf{K}^{-1}$ is applied to the ciphertext, then the plaintext is recovered.

In general terms, the Hill system can be expressed as

$$\mathbf{C} = \mathrm{E}(\mathbf{K}, \mathbf{P}) = \mathbf{PK} \bmod 26$$
$$\mathbf{P} = \mathrm{D}(\mathbf{K}, \mathbf{C}) = \mathbf{CK}^{-1} \bmod 26 = \mathbf{PKK}^{-1} = \mathbf{P}$$

Transposition/Permutation Ciphers

- now consider classical **transposition** or **permutation** ciphers
- these hide the message by rearranging the letter order without altering the actual letters used.
- can recognise these since have the same frequency distribution as the original text

Rail Fence Cipher

- In Rail Fence, the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
- For example: to encipher the message "meet me after the toga party" with rail fence of depth 2, we write the following:

```
m e m a t r h t g p r y
 e t e f e t e o a a t
```

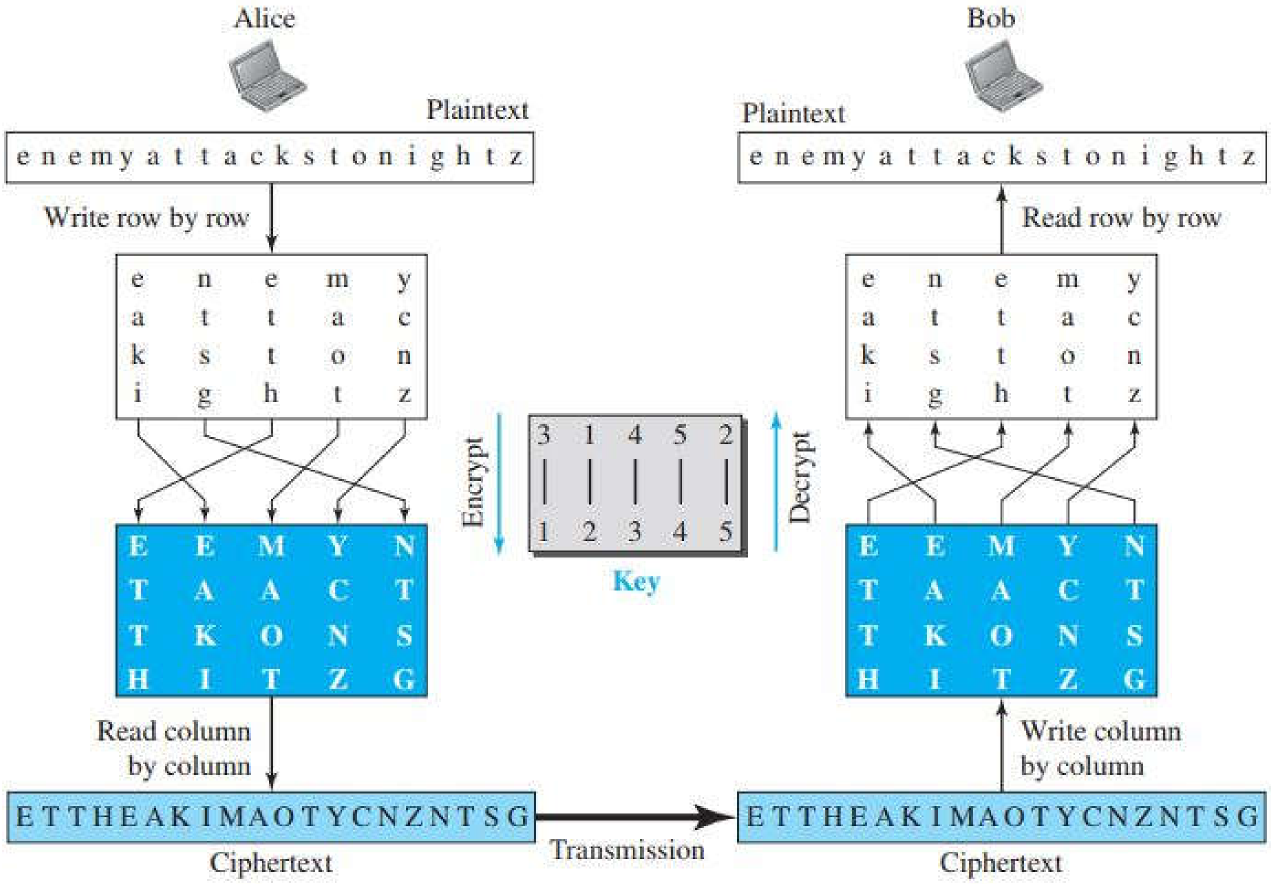
- giving ciphertext

```
MEMATRHTGPRYETEFETEOAAT
```

Rectangular Scheme

- Write the **message in a rectangle**, row by row, and read the message off, column by column, but **permute the order of the columns**. The order of the columns then becomes the key to the algorithm.
- For example:
- Suppose Alice wants to secretly send the message “Enemy attacks tonight” to Bob. The encryption and decryption is shown in Figure. Note that we added an extra character (z) to the end of the message to make the number of characters a multiple of 5.

Rectangular Scheme



enemyattackstonightz

e	n	e	m	y
a	t	t	a	c
k	s	t	o	n
i	g	h	t	z

3	1	4	5	2
1	2	3	4	5

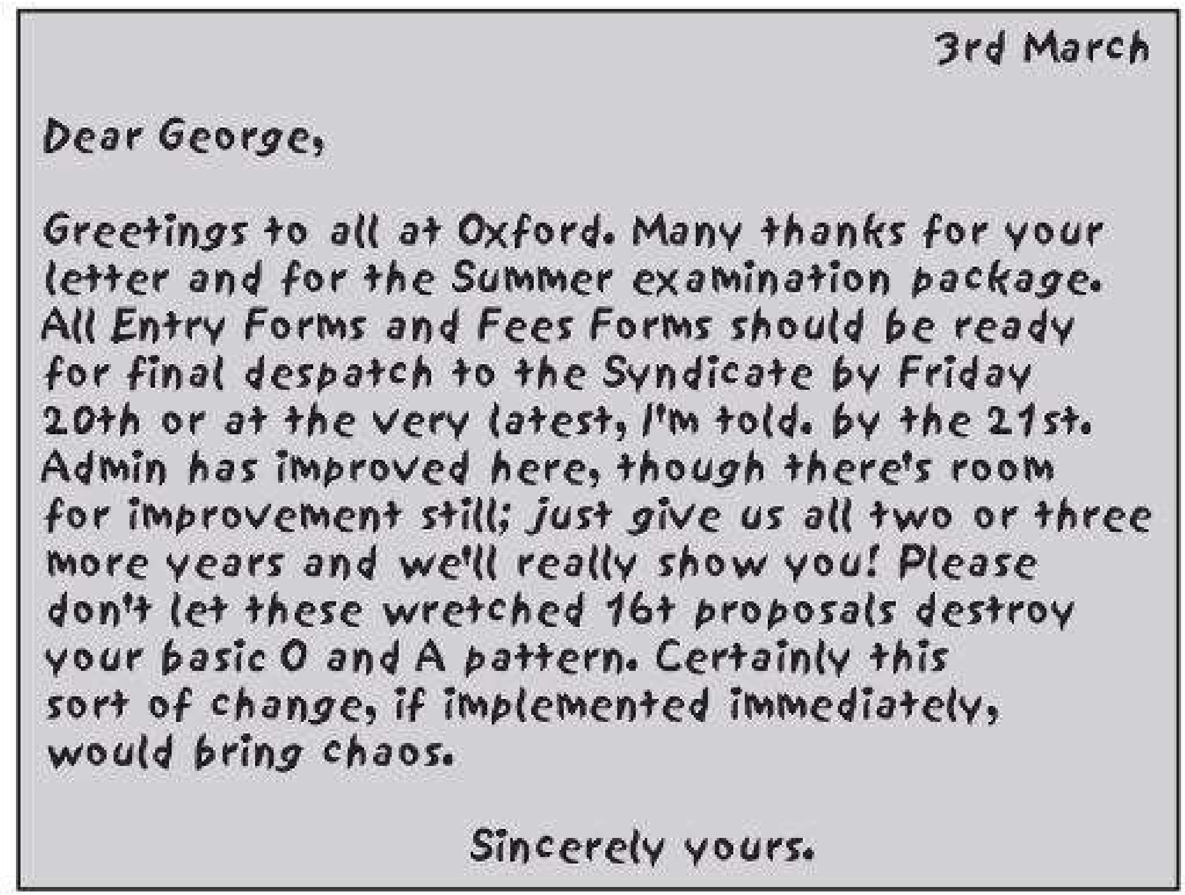
E	E	M	Y	N
T	A	A	C	T
T	K	O	N	S
H	I	T	Z	G

ETTHEAKIMAOTYCNZNTSG

Steganography

- an alternative to encryption
- hides existence of message
  - using only a subset of letters/words in a longer message marked in some way
    - character marking
    - using invisible ink
    - pin punctures
    - typewriter correction ribbon
  - hiding in LSB in graphic image or sound file
- has drawbacks
  - high overhead to hide relatively few info bits
  - once the system is discovered, it becomes virtually worthless
  - can be used in conjunction with encryption

Steganography



3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told. by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours.

Figure: A Puzzle for Inspector Morse

Your package ready Friday 21st room three. Please destroy this message.

Rectangular Scheme

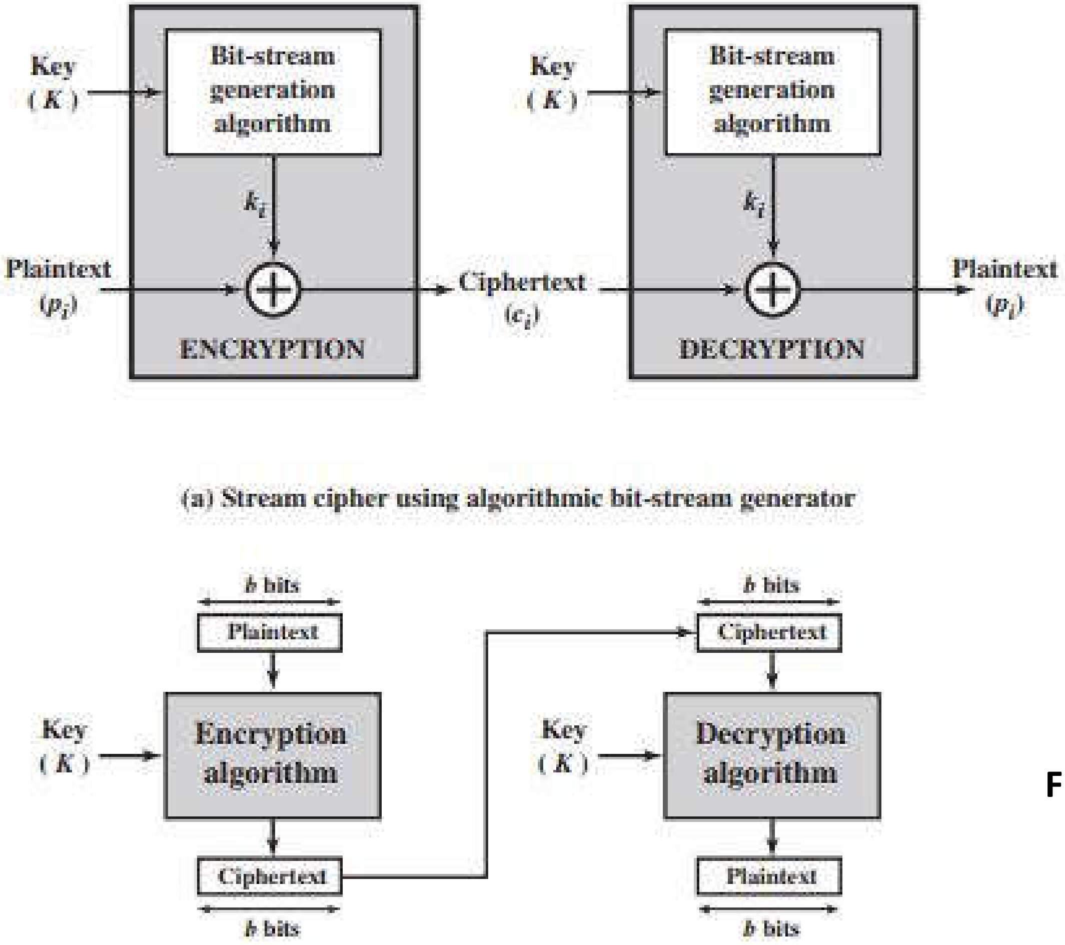
- A pure transposition is easily recognized because it has the same letter frequencies, as the original plaintext.
- cryptanalysis is fairly straightforward and involves laying out the cipher in a matrix and playing around with column positions.

Modern Ciphers

- Block Ciphers
- Stream Ciphers
- Symmetric Ciphers
- Asymmetric Ciphers

Modern Ciphers

- In Modern ciphers, digital data is represented in strings of binary digits (bits), unlike alphabets.
- These binary bits are processed to convert into another binary strings as ciphertext.
- Based on how these binary strings are processed, a symmetric encryption scheme can be classified as:
  1. stream cipher
  2. block cipher



(a) Stream cipher using algorithmic bit-stream generator

(b) Block cipher

Figure: Stream and Block Cipher

Stream Cipher

- A stream cipher is a type of cryptographic algorithm used for encrypting data. Unlike block ciphers, which operate on fixed-size blocks of data, **stream ciphers encrypt data one bit or byte at a time, producing a continuous stream of encrypted output**. This makes stream ciphers particularly useful for applications where data is transmitted in a continuous flow, such as real-time communication or data streaming.
- The core idea behind a stream cipher is the generation of a pseudorandom stream of bits, called the keystream, which is then combined with the plaintext using a *bitwise XOR operation* to produce the ciphertext. The keystream is generated using a cryptographic key and an initialization vector (IV) in some cases.
- One of the well-known stream ciphers is the "RC4" (Rivest Cipher 4), which was widely used in various applications like wireless communication protocols and web security. However, due to security vulnerabilities, its usage has been greatly reduced in recent years in favor of more secure alternatives.

Stream Cipher

Here's a simplified overview of how a stream cipher works:

1. **Key Generation**: The encryption process begins with generating a secret key that both the sender and the receiver possess.
2. **Initialization**: If an IV is used, it is combined with the key to initialize the internal state of the cipher algorithm.
3. **Keystream Generation**: The stream cipher generates a keystream by repeatedly applying a cryptographic function (usually a shift register or a feedback shift register) to the key and IV (if applicable). The resulting keystream is a sequence of pseudorandom bits that appear unpredictable without knowledge of the key.
4. **Encryption**: The plaintext data is bitwise XORed with the keystream, resulting in the ciphertext. Each bit of the plaintext is encrypted independently using the corresponding bit from the keystream.
5. **Decryption**: To decrypt the ciphertext, the same keystream generation process is applied to the key (and IV, if used) to recreate the original keystream. The keystream is then XORed with the ciphertext to obtain the original plaintext.

Block cipher

- A block cipher is a type of cryptographic algorithm used for encrypting data in fixed-size blocks. Unlike stream ciphers, which encrypt data bit by bit or byte by byte, block ciphers operate on larger blocks of data, typically consisting of a fixed number of bits (e.g., 64, 128, or 256 bits). The input block is transformed into an encrypted output block of the same size using a secret encryption key.
- The basic operation of a block cipher *involves a substitution-permutation network (SPN) structure*. This structure consists of several rounds of operations, each involving substitution (usually represented by a substitution box or S-box) and permutation (bit shuffling) operations, often followed by a key mixing step.

Block Cipher

- It's important to note that the security of a block cipher depends on the strength of the algorithm itself, the secrecy of the key, and the number of rounds used in the encryption process. A higher number of rounds generally makes the cipher more secure, but it can also increase computational overhead.
- One of the most well-known block ciphers is the Advanced Encryption Standard (AES). AES supports key lengths of 128, 192, or 256 bits and is widely used for secure data encryption in various applications, including secure communication, data storage, and more.
- Block ciphers provide a strong foundation for modern cryptographic systems, but it's essential to choose algorithms that have undergone extensive analysis and scrutiny to ensure their security against various types of attacks.

Block cipher

Here's a simplified overview of how a block cipher works:

1. **Key Generation:** The encryption process begins with generating a secret key that both the sender and the receiver possess.
2. **Subkey Generation**: The key is expanded into a set of subkeys, one for each round of the block cipher. These subkeys are derived from the original key through various mathematical operations.
3. **Encryption**: The plaintext data is divided into fixed-size blocks. Each block is then subjected to a series of rounds. In each round, the block is subjected to a combination of substitution, permutation, and mixing operations, using the corresponding round subkey. The exact operations performed in each round are determined by the specific block cipher algorithm being used.
4. **Decryption**: To decrypt the ciphertext, the same process is reversed. Each ciphertext block undergoes the inverse of the encryption operations for each round, using the corresponding round subkeys. After all rounds are reversed, the original plaintext block is obtained.

Asymmetric Cryptography

- Asymmetric cryptography, also known as **public-key cryptography**, is a cryptographic approach that uses a pair of mathematically related keys for encryption and decryption.
- This is in contrast to symmetric cryptography, where the same key is used for both encryption and decryption.
- The key pair in asymmetric cryptography consists of a public key and a private key.

Asymmetric Cryptography

- Here's how asymmetric cryptography works:

1. **Key Pair Generation**:
   - Public Key: This key is intended to be shared openly with anyone. It's used for encryption and verifying digital signatures.
   - Private Key: This key is kept secret and known only to the owner. It's used for decryption and creating digital signatures.
2. **Encryption**:
   - If someone wants to send a confidential message to a recipient, they obtain the recipient's public key and use it to encrypt the message.
   - Only the recipient, who possesses the corresponding private key, can decrypt and read the message.

Asymmetric Cryptography

3. **Digital Signatures:**
   - A digital signature is used to verify the authenticity and integrity of a message or document.
   - The sender uses their private key to create a digital signature for the message.
   - The signature is a unique value that is derived from the message's content and ensures that the message hasn't been tampered with.
   - The recipient can use the sender's public key to verify the digital signature. If the signature is valid, it confirms that the message originated from the claimed sender and that it hasn't been altered.
4. **Key Exchange**:
   - Asymmetric cryptography can also be used for secure key exchange. For instance, the *Diffie-Hellman key exchange protocol* allows two parties to establish a shared secret key over an insecure channel without actually transmitting the key itself.

Uses:Asymmetric Cryptography

- Common applications of asymmetric cryptography include secure communication protocols (like HTTPS), digital signatures for document authentication, and public key infrastructure (**PKI**) systems that manage the distribution and verification of public keys.

- Notable asymmetric cryptographic algorithms include **RSA** (*Rivest-Shamir-Adleman*) for encryption and digital signatures, and ***Elliptic Curve Cryptography (ECC)***, which offers strong security with shorter key lengths compared to RSA.

Pros an Cons: Asymmetric Cryptography

- Asymmetric cryptography offers several advantages, such as enhanced security for key exchange and digital signatures. However, it is generally slower and requires more computational resources compared to symmetric cryptography, which is often faster and more efficient for encrypting large amounts of data.