4.1 Security Services and Mechanisms

Security services:

X.800 defines a security service as a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers.

X.800 divides these services into five categories and fourteen specific services

1. Authentication (who created or sent the data)
2. Access control / Availability (prevent misuse of resources)
3. Confidentiality (privacy)
4. Integrity (has not been altered)
5. Non-repudiation (the order is final)

- **Authentication** - assurance that the communicating entity is the one that it claims to be.
  - The process of proving one's identity.
  - **Peer Entity Authentication**
    - Used in association with a logical connection to provide confidence in the identity of the entities connected.
  - **Data Origin Authentication**
    - In a connectionless transfer, provides assurance that the source of received data is as claimed.

- **Access Control/Availability** - prevention of the unauthorized use of a resource

- **Data Confidentiality** –protection of data from unauthorized disclosure.
  - *Privacy* - Ensuring that no one can read the message except the intended receiver.
  - **Connection Confidentiality**
    - The protection of all user data on a connection.
  - **Connectionless Confidentiality**
    - The protection of all user data in a single data block
  - **Selective-Field Confidentiality**
    - The confidentiality of selected fields within the user data on a connection or in a single data block.
  - **Traffic Flow Confidentiality**
    - The protection of the information that might be derived from observation of traffic flows.

- **Data Integrity** - The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
  - Assuring the receiver that the received message has not been altered in any way from the original.
  - **Connection Integrity with Recovery**
    - Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.
  - **Connection Integrity without Recovery**
    - As above, but provides only detection without recovery.
  - **Selective-Field Connection Integrity**

- Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

❖ **Connectionless Integrity**

- Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

❖ **Selective-Field Connectionless Integrity**

- Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

➢ **Non-Repudiation -** protection against denial by one of the parties in a communication. A mechanism to prove that the sender really sent this message.

❖ **Non-repudiation, Origin**

- Proof that the message was sent by the specified party.

❖ **Non-repudiation, Destination**

- Proof that the message was received by the specified party.

Security Mechanism

➢ A security mechanism is a means to provide a service

❖ **E.g.** encryption, cryptographic protocols

➢ **Specific Security Mechanisms**

✓ May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

❖ **Encipherment**

✓ The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

❖ **Digital Signature**

✓ Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

❖ **Access Control**

✓ A variety of mechanisms that enforce access rights to resources.

❖ **Data Integrity**

✓ A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

❖ **Authentication Exchange**

✓ A mechanism intended to ensure the identity of an entity by means of information exchange.

❖ **Traffic Padding**

✓ The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

❖ **Routing Control**

✓ Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

❖ **Notarization**

✓ The use of a trusted third party to assure certain properties of a data exchange.

➢ **Pervasive Security Mechanisms**

  - ✓ Mechanisms that is not specific to any particular OSI security service or protocol layer.
- ❖ **Trusted Functionality**
  - ✓ That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
- ❖ **Security Label**
  - ✓ The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
- ❖ **Event Detection**
  - ✓ Detection of security-relevant events.
- ❖ **Security Audit Trail**
  - ✓ Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
- ❖ **Security Recovery**
  - ✓ Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Classical crypto systems

Cryptography - the art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form

Plain text - the original intelligible message

Cipher text- the transformed message

Cipher - an algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods

Key - some critical information used by the cipher, known only to the sender & receiver

Encipher (encode) - the process of converting plain text to cipher text using a cipher and a key

Decipher (decode) - the process of converting cipher text back into plain text using a cipher and a key

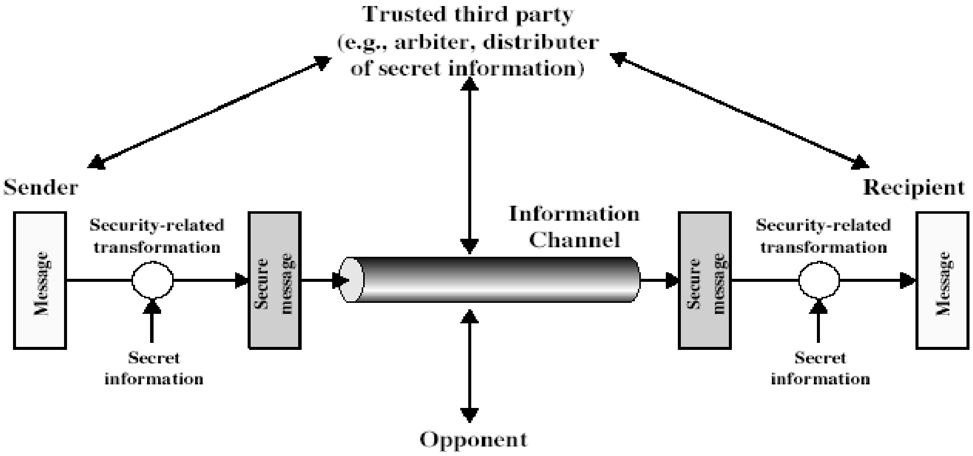


Fig 6: Model for Network Security

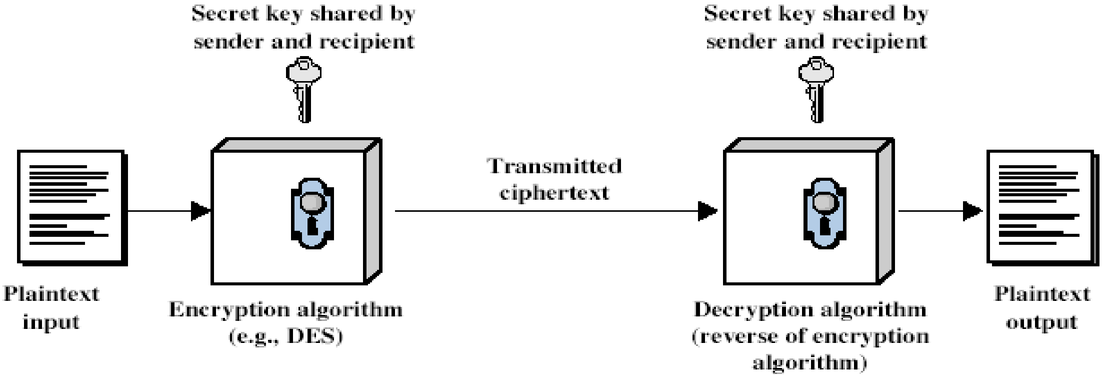

Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Fig 7: Classical crypto systems

Cryptanalysis - the study of principles and methods of transforming an unintelligible message back into an intelligible message *without* knowledge of the key. Also called **code breaking**
Cryptology - both cryptography and cryptanalysis
Cryptanalysis

- The process of attempting to discover plain text or key or both is known as cryptanalysis.
- There are 2 general approaches to attacking a conventional encryption scheme.

1. **Cryptanalytic Attacks**

   Cipher text only
   - only have access to some enciphered messages
   - use statistical attacks only

   Known plain text
   - know (or strongly suspect) some plaintext-cipher text pairs
   - use this knowledge in attacking cipher

   Chosen plain text
   - can select plaintext and obtain corresponding cipher text
   - use knowledge of algorithm structure in attack

   Chosen plain text-cipher text
   - can select plain text and obtain corresponding cipher text, or select cipher text and obtain plain text
   - allows further knowledge of algorithm structure to be used

2. **Brute Force Attack**
   - It involves trying every possible key until an intelligible translation of the cipher text into plain text is obtained.

Encryption Scheme

- Unconditionally Secure:
  - If the cipher text generated by the scheme does not contain enough information to determine the corresponding plaintext.
- Computationally Secure:
  - 2 criteria
  - The cost of breaking the cipher exceeds the value of the encrypted information.
  - The time required to break the cipher exceeds the useful lifetime of the information.

Different types of ciphers

- have two basic components of classical ciphers: **substitution** and **transposition**
- in substitution ciphers letters are replaced by other letters

- in transposition ciphers the letters are arranged in a different order

Substitution Techniques

- Caesar Cipher
- Monoalphabetic Cipher
- Playfair Cipher
- Hill Cipher
- Polyalphabetic Cipher
- Vernam Cipher

Caesar Cipher

- Proposed by Julius Caesar.
- Each alphabet in a plaintext message is replaced by an alphabet three places down the alphabet.
- Note that the alphabet is wrapped around, so that the letter following Z is A.

Plain	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
Cipher	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

- The caesar algorithm can be expressed as follows
- Encryption
  - C=E(p)=(p+3) mod 26
- Decryption
  - p=D(C)=(C-3) mod 26
- A shift may be of any amount, so that the general Caesar algorithm is
  - $C = \mathrm{E}(k, p) = (p + k) \bmod 26$
  - where k takes on a value in the range 1 to 25.
- The decryption algorithm is simply
  - $p = \mathrm{D}(k, C) = (C - k) \bmod 26$

Eg:

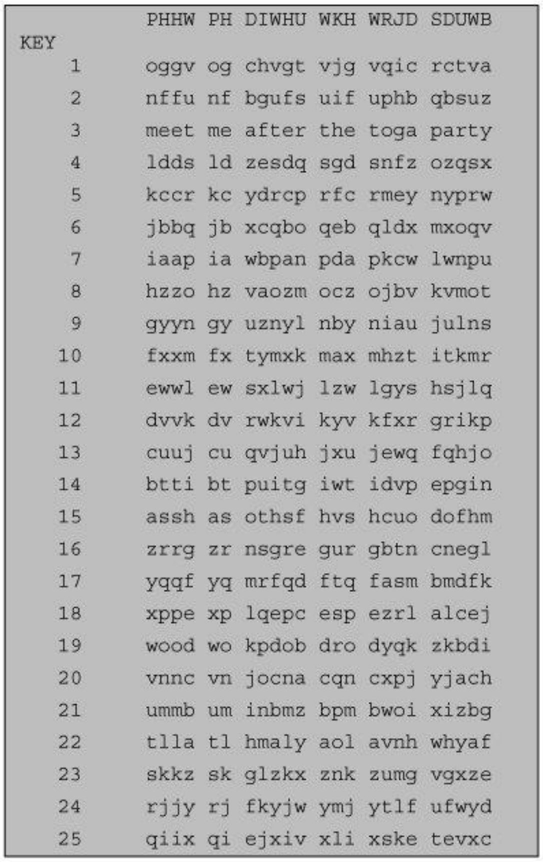
Plain text : hello
Cipher text : KHOOR

Plain text : meet me after the toga party
Cipher text : PHHW PH DIWHU WKH WRJD SDUWB

<u>convert cipher text into plaintext</u>

Cipher text: **phhw ph diwhu wkh sduwb**
Cipher text: **ehvw ri oxfn**
Cipher text: **L ORYH BRX**

- Advantages:
  - Easy to perform
  - Simple
- Disadvantages:
  1. To break a cipher text message using the Brute Force attack.
  2. There are only 25 possibilities to try out.
  3. The language of the plaintext was English



KEY	PHHW PH DIWHU WKH WRJD SDUWB
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

Fig 8 : Brute-Force Cryptanalysis of Caesar Cipher

Monoalphabetic Cipher

- ➢ Rather than using a uniform scheme for all the alphabets in a given text message, apply random substitution
- ➢ This means that in a given plaintext message, each 'A' can be replaced by any other alphabet (B through Z), each 'B' can also replaced by any other random alphabet (A or C through Z) and so on.
- ➢ There is no relation between replacements of one alphabet with any other alphabet. There is any permutation or combination of the 26 alphabets, which means (26 X 25 X … X 2) or 4 X 10^{26} possibilities.

- ➢ Advantages:
  - ❖ Extremely hard to crack the cipher text even with the most modern computers.
- ➢ Disadvantages:
  - ❖ Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet. A counter measure is to provide multiple substitutes known as homophones.
  - ❖ Relative frequency of alphabet in the cipher text can be determined and compared to standard frequency distribution for English by the cryptanalyst to break cipher text.

Character Frequencies

- ➢ in most languages letters are not equally common
- ➢ in English **e** is by far the most common letter

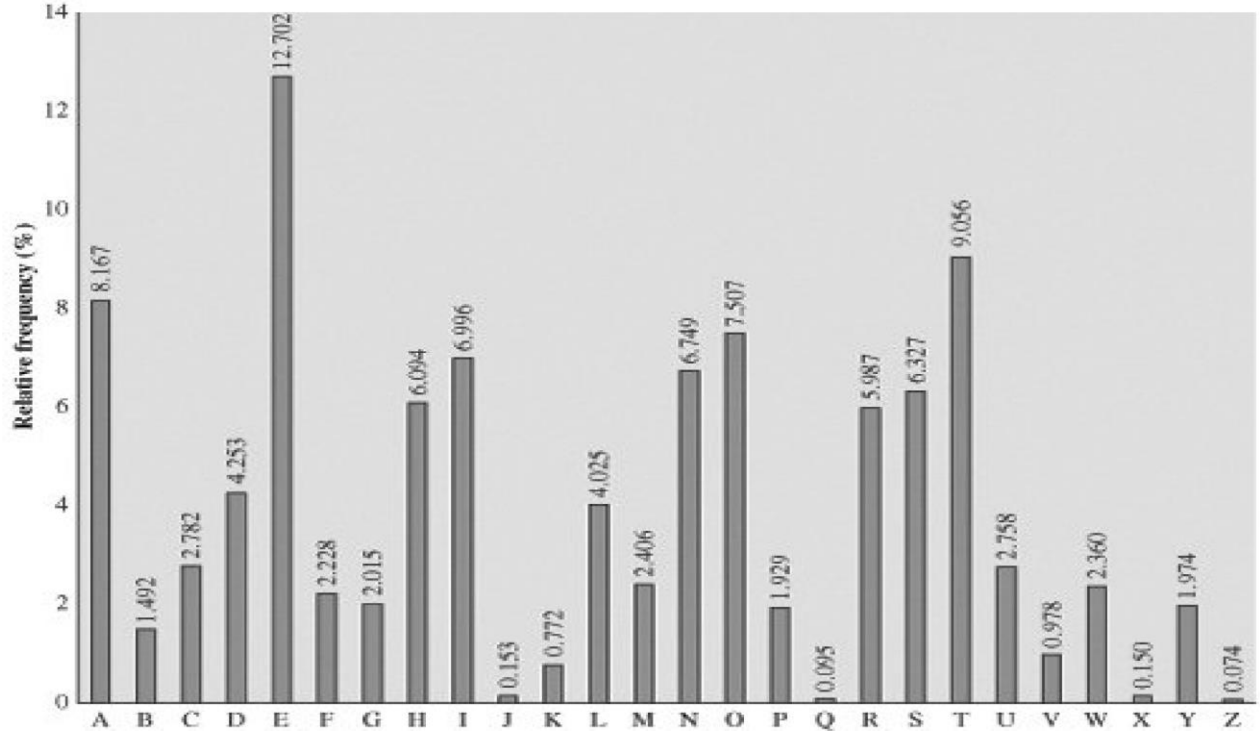


Fig 8: English character frequencies

Playfair cipher

The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plain text as single units and translates these units into cipher text digrams

- Algorithm:
  - This algorithm is based on the use of a 5 X 5 matrix of letters constructed using a keyword.
  - The matrix is constructed by filling in the letters of the keyword (minus duplications) from left to right and from top to bottom.
  - And then filling in the remainder of the matrix with the remaining letters in alphabetic order. The letters I and J count as one letter.

    For example: keyword is 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**

- Plaintext is encrypted two letters at a time, according to the following rules.

1. Repeating plaintext letters that would fall in the same pair are separated with filler letter, such as **x**.
   - For eg: **balloon** would be treated as **ba lx lo on.**

2. Plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.
    - For eg: **pq** and **ar** are encrypted as **QS** and **RM**.
3. Plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the row circularly following the last.
    - For eg: **dr** and **mu** are encrypted as **KD** and **CM**.
4. Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.
    - For eg: **hs** becomes **BP** and **ea** becomes **IM or JM**

p.t: meet me at hammersmith bridge tonight
key:charles
C.T:GDDOGDRQARKYGDHDNKPRDAMSOGUPGKICQY

Find the plain texts:
key : MONARCHY
C.T : **TOFGGAMS**
p.t : ?

1. Plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.
   For our eg: **FG** is decrypted as **EF**.
2. each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.
   For our eg: **TO** decrypts **PR** , **GA** becomes **IN** and **MS** to **AL**

C.T:	TO	FG	GA	MS
p.t:	**pr**	**ef**	**in**	**al**

C.T:HQVSITKQESAX
KEY:INFOTECH
p.t:?

C.T:CLKLCLOILKDZCFSODZBW
KEY:MONARCHY
p.t:?

C.T:EPVSZRLOISMV
KEY:ZINTA
p.t:?

K:TEENAGE
c.t: KMIZAWUZ
p.t:?

K:LAST
c.t: WLMPLWBI
p.t:?

Advantages:

- There are only 26 letters in the alphabet. Therefore 26 X 26 = 676 digrams, So that identification of individual digrams is more difficult.
- The relative frequencies of individual letters exhibit a much greater range than that of digrams, making frequency analysis much more difficult.

Disadvantages:

- Playfair cipher is breakable only if few hundreds of cipher text are known

Hill Cipher

- Multiletter cipher
- Proposed by Lester Hill
- The encryption algorithm takes ‘m’ successive plain text letters and substitutes for them ‘m’ cipher text letters
- For *Hill ciphers*, assign numerical values to each plain text and cipher text letter so that A=0, B=1, C=2 and so on.

Encryption

- For m=3, the system can be described as follows.

C1 = (K11p1+K12p2+K13p3) mod 26
C2 = (K21p1+K22p2+K23p3) mod 26
C3 = (K31p1+K32p2+K33p3) mod 26

- This can be expressed in term of column vectors and matrices.

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \text{mod } 26$$

(Or)

C=Kp mod 26, where C & p are column vectors of length 3 and k is a 3 X 3 matrix.

Example:

p=paymoremoney

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

First take 3 letters in plain text

p= p a y (15 0 24)

C=Kp mod 26=?

$$\mathbf{K}\begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} = \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} = \text{LNS.}$$

- The cipher text for the entire plain text is LNSHDLEWMTRW.

Decryption

- Using the inverse of the matrix K. The inverse K^{-1} of a matrix K is defined by K K^{-1}= K^{-1}K=I, where I is the unit matrix.
- The inverse of matrix does not always exist, but when it does, it satisfies the preceding equation, in this case the inverse is

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

- It is easily seen that if the matrix K^{-1} is applied to the cipher text, then the plaintext is recovered.

  p= Dk(C) = K^{-1} C mod 26

  Eg: p = K^{-1} (11 13 18)= (431 494 570) mod 26=(15 0 24)=pay

- Advantages:

  This scheme completely hides single letter frequencies. It is strong against cipher text only attack.

- Disadvantages:

  It is easily broken with a known plain text attack.

Polyalphabetic Cipher

- Its are the improvements made on monoalphabetic technique.
- Substitute several random patterns

Vigenère Cipher

- The Vigenère cipher is a method of encryption that uses a series of different Caesar ciphers based on the letters of a keyword.
- In this scheme, use a matrix known as the Vigenère tableau
- Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left.
- A normal alphabet for the plaintext runs across the top.

Encryption:

- The process of encryption is simple.

  Eg: k=x, p=y then C=V

- To encrypt a message, a key is needed that is as long as the message. Usually the key is a repeating keyword.

  Eg:

  Key = DECEPTIVE; Plaintext: we are discovered save yourself

Plain	w	e	a	r	E	d	i	s	c	o	v	e	r	e	d	s	a	v	e	y	o	u	r	s	e	l	f
Key	D	E	C	E	P	T	I	V	E	D	E	C	E	P	T	I	V	E	D	E	C	E	P	T	I	V	E
Cipher	Z	I	C	**V**	**T**	**W**	Q	N	G	R	Z	G	**V**	**T**	**W**	A	V	Z	H	C	Q	Y	G	L	M	G	J

Decryption:

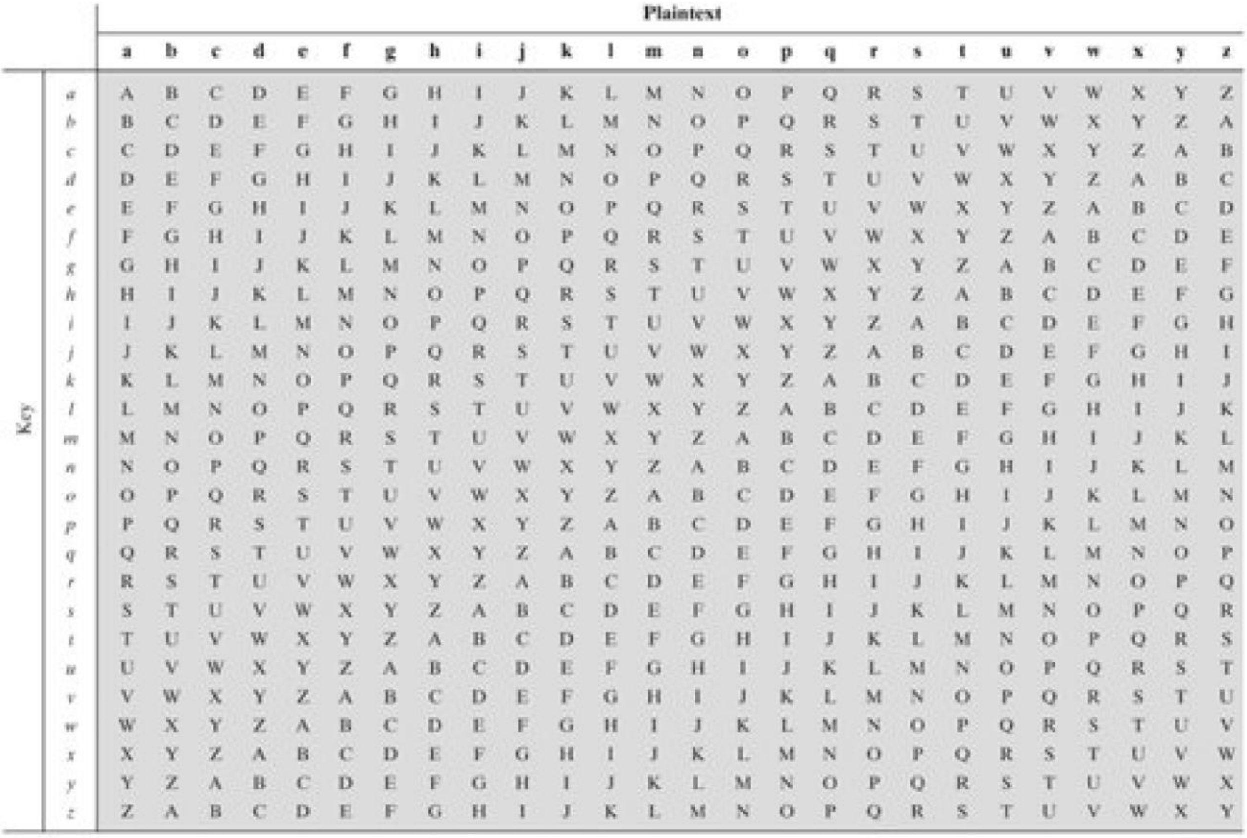
- The key letter again identifies the row.
- The position of the cipher text letter in that row determines the column and the plain text letter is at the top of that column.

Eg:

K=INDIA

C=WCHZABVRVSCPFMSA

p=?



		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
Key	a	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
	b	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	A
	c	C	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
	d	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
	e	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	D
	f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	z	Z	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

Fig 9 : The Modern Vigenère Tableau - I

➢ Advantages:

❖ The strength of this cipher is that there are multiple cipher text letters for each plain text letter. Thus the letter frequency information is obscured.

➢ Disadvantages:

1. Using statistical information.
   - the statistical properties of the cipher text should be the same as that of the plain text.
2. Determining the length of the keyword. **VTW** repeated.

➢ To overcome these

- Keyword can be eliminated by using a non repeating keyword that is as long as the message itself.
- So introducing auto key system. In which a keyword is concatenated with plain text itself to providing a running key.
- Eg:
  Key = DECEPTIVE; Plaintext: we are discovered save yourself

Plain	w	e	a	r	e	d	i	s	c	o	v	e	r	e	d	s
Key	D	E	C	E	P	T	I	V	E	W	E	A	R	E	D	I
Cipher	Z	I	C	**V**	**T**	**W**	Q	N	G	K	Z	E	**I**	**T**	**G**	A

Plain	a	v	e	y	o	u	r	s	e	l	f
Key	S	C	O	V	E	R	E	D	S	A	V

Cipher	S	X	S	T	S	L	U	V	W	L	A

- Even this scheme is vulnerable to cryptanalysis, because the key and the plain text share the same frequency distribution of letters, a statistical technique can be applied.

Vernam Cipher

- Proposed by Gilbert Vernam.
- His system works on binary data rather than letters.
- The system can be expressed as
  Encryption
  $$Ci = pi \oplus Ki$$
  Decryption
  $$pi = Ci \oplus Ki$$

Disadvantages:

1. Use repeated key
2. It can be broken with sufficient cipher text, the use of known or probable plain text sequences or both.

One-Time Pad

- Joseph Mauborgne, proposed an improvement to the vernam cipher that yields the ultimate in security.
- The one-time pad (OTP), also called the perfect cipher, is a crypto algorithm where plaintext is combined with a random key that was truly as long as the message with no repetitions.
- It produces random output that bears no information whatsoever about the plaintext, there is simply no way to break the code.
- In OTP, four important rules are followed. If these rules are applied correctly, the one-time pad can be proven to be unbreakable. However, if only one of these rules is disregarded, the cipher is no longer unbreakable.
  1. The key is as long as the plaintext.
  2. The key is truly random
  3. There should only be two copies of the key: one for the sender and one for the receiver (some exceptions exist for multiple receivers)
  4. The keys are used only once, and both sender and receiver must destroy their key after use

  Using a Vigenere table with 27 characters in which the 27th character is the space character, but with a one time key is as long as the message

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

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

Fig 10: The Modern Vigenère Tableau - II

Eg1:

Cipher	A	N	K	Y	O	D	K	Y	U	R	E	P	F	J	B	Y	O	J	D	S
Key	P	X	L	M	V	M	S	Y	D	O	F	U	Y	R	V	Z	W	C		T
Plain	m	R		M	u	s	t	a	r	d		w	i	t	h		t	h	e	

Cipher	P	L	R	E	Y	I	U	N	O	F	D	O	I	U	E	R	F	P	L	U	Y	T	S
Key	N	L	E	B	N	E	C	V	G	D	U	P	A	H	F	Z	Z	L	M	N	Y	I	H
Plain	c	a	n	D	l	e	s	t	i	c	k		i	n		t	h	e		h	a	L	l

Plain text: mr mustard with the candlestick in the hall

Eg2:

Cipher	A	N	K	Y	O	D	K	Y	U	R	E	P	F	J	B	Y	O	J	D	S	P	L
Key	M	F	U	G	P	M	I	Y	D	G	A	X	G	O	U	F	H	K	L	L	L	M
plain	m	I	S	S		s	c	a	R	l	e	t		w	i	t	h		t	h	e	

Cipher	R	E	Y	I	U	N	O	F	D	O	I	U	E	R	F	P	L	U	Y	T	S
Key	H	S	Q	D	Q	O	G	T	E	W	B	Q	F	G	Y	O	V	U	H	W	T
Plain	k	n	I	f	e		i	n		t	h	e		l	i	b	r	a	r	Y	

Plain text: miss scarlet with the knife in the library

- **Is one-time pad unbreakable?**
- If all rules of one-time pad are followed? Yes! Since the key is truly random, one cannot determine which key is used. If someone had infinite computational power he could go through all possible keys (a brute force attack). He would find out that applying the key XVHEU on cipher text QJKES would produce the (correct) word TODAY. Unfortunately, he would also find out that the key FJRAB would produce the word LATER, and even worse, DFPAB would produce the word NEVER. He has no idea which key is the right one. In fact, you can produce any desired word or phrase from any OTP-encrypted message, as long as you use the 'right' wrong key. There is no way to verify if a solution is the right one. Therefore, the one-time pad system is proven completely secure.

The enciphered word:

Plain text	:	T O D A Y
OTP-Key	:	X V H E U
Cipher text	:	Q J K E S

The deciphered word, with one correct and two wrong OTP keys:

Cipher text	:	Q J K E S	Q J K E S	Q J K E S
OTP-Key	:	X V H E U	F J R A B	D F P A B
		---------	---------	---------
Plain text	:	T O D A Y	L A T E R	N E V E R

- The one-time pad encryption scheme itself is mathematically unbreakable.

Advantages:

1. It produces random output that bears no information whatsoever about the plaintext, there is simply no way to break the code.
2. Exhaustive search of all possible keys lead to many legible plain texts.

Disadvantages:

1. Supplying Random characters in volume is a significant task
2. Every message to be sent, a key of equal length is needed by the sender and the receiver, so key distribution problem exists.

TRANSPOSITION TECHNIQUES

- Performing some sort of permutation on the plain text letters.ie, transposition or permutation ciphers hide the message contents by rearranging the order of the letters

Reverse cipher

- write the message backwards
  Plain: I CAME I SAW I CONQUERED
  Cipher: DEREU QNOCI WASIE MACI

Rail Fence cipher

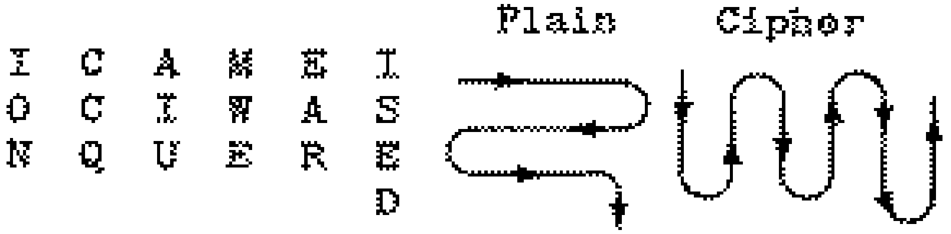
- write message as a sequence of diagonals
- read off cipher row by row
- depth 2

p: I A E S W C N U R D
C M I A I O Q E E

- Cipher: IAESW CNURD CMIAI OQEE

Geometric Figure

- write message following one pattern and read out with another



I	C	A	M	E	I
O	C	I	W	A	S
N	Q	U	E	R	E
					D

Cipher: IONQC CAIUE WMEAR DESI

Row Transposition ciphers

- in general write message row by row in a number of columns and then use some rule to read off from these columns
- key could be a series of number being the order to; read off the cipher; or write in the plaintext
  p: come home tomorrow

Col 1	Col2	Col 3	Col 4	Col 5	Col 6
c	o	m	e	h	o
m	e	t	o	m	o
r	r	o	w	y	z

Key: 461253

Cipher: eowoozcmroerhmymto

Block (Columnar) Transposition ciphers

- Introduce more complexity than Row Transposition ciphers.

Algorithm:

1. Write the plain text message row by row in a rectangle of a pre defined size.
2. Read the message column- by – column in any random order
3. The message thus obtained is the cipher text of round 1
4. Repeat steps 1 to 3 as many times as desired

Adv: more complex to crack cipher text.

Eg:

Plain text: come home tomorrow

1. Consider rectangle with 6 columns. Write the plain text.

Col 1	Col2	Col 3	Col 4	Col 5	Col 6
c	o	m	e	h	o
m	e	t	o	m	o
r	r	o	w	y	z

2. Order of column (key): 4,6,1,2,5,3

3. Cipher text: eowoozcmroerhmymto, now this is the input to round 2.

4. Write the round 1 output in rectangle format

Col 1	Col2	Col 3	Col 4	Col 5	Col 6
e	o	w	o	o	z
c	m	r	o	e	r
h	m	y	m	t	o

5. Key: 4,6,1,2,5,3

6. Cipher text = oomzroechommoetwry