IT2352-CRYPTOGRAPHY AND NETWORK SECURITY

UNIT I

Background:

- Information Security requirements have changed in recent times
- Traditionally provided by physical and administrative mechanisms
- Computer needs automated tools to protect files and other stored information
- Use of networks and communications links requires measures to protect data during transmission

Computer Security

Generic name for the collection of tools designed to protect data from the hackers

Network Security

It measures to protect data during their transmission

Internet Security

It measures to protect data during their transmission over a collection of interconnected networks

OSI Security Architecture

To assess effectively the security needs of an organization and to evaluate and choose various security products and policies, the manager responsible for security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. This is difficult enough in a centralized data processing environment; with the use of local and wide area networks, the problems are compounded. ITU-T (International telecommunication union) Recommendation X.800, Security Architecture for OSI, defines such a systematic approach. The OSI security architecture is useful to managers as a way of organizing the task of providing security.

Aspects of Security:

OSI security architecture focuses on the 3 aspects of information security.

• **Security attack:** Any action that compromises the security of information owned by an organization.

• **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

• **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Difference between Attack and Threat:

Attack	Threat
Attack is an intelligent act that is deliberate to evade security and violate the security policy of a system.	Threat is a possible danger that exploits vulnerability.

1. Security Attack:

- Security attack is defined as any action that compromises the security of information owned by an organization
- often threat & attack used to mean same thing
- It have a wide range of attacks
- There are two types of attacks
    1. Passive attack
    2. active attack

Passive Attacks:

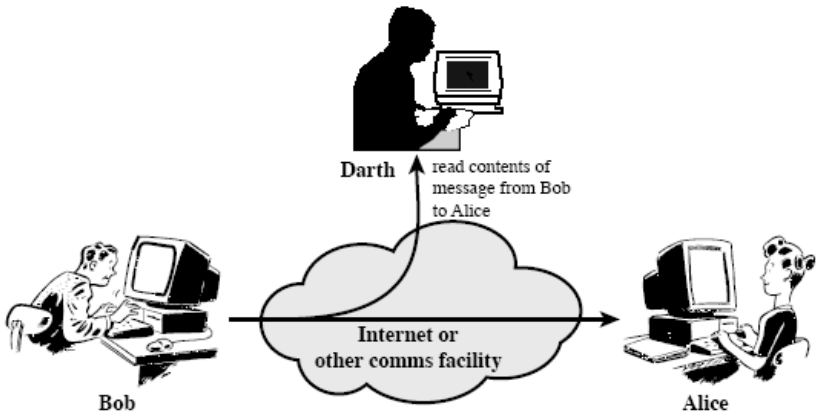
- Only involve monitoring (interception) of the information, or eavesdropping, but does not affect the system resources.
- Difficult to detect.
- It is possible to prevent the passive attack by encryption rather than detection.

There are two types of passive attacks:

1. Release of message contents
2. Traffic analysis

Release of message contents:

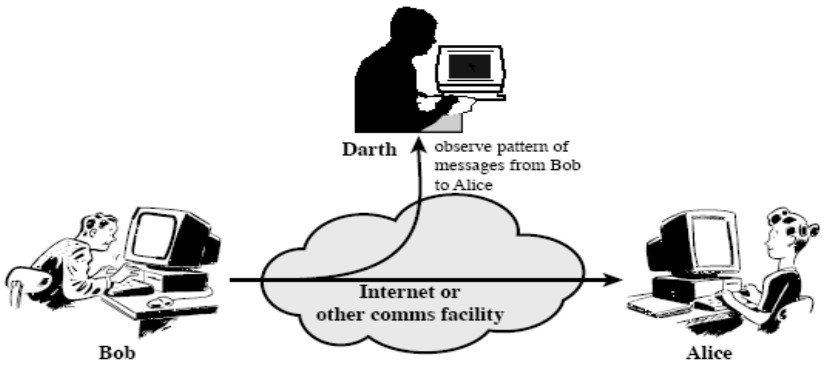
- Learn the content of transmitted messages
- The message to be transmitted should be prevented from eavesdropping.



(a) Release of message contents

Traffic Analysis:

- Monitoring the pattern of transmitted messages
  - Include the source & destination, frequency, and length of messages
- Determine the location and identity of communicating hosts



(b) Traffic analysis

Active Attacks:

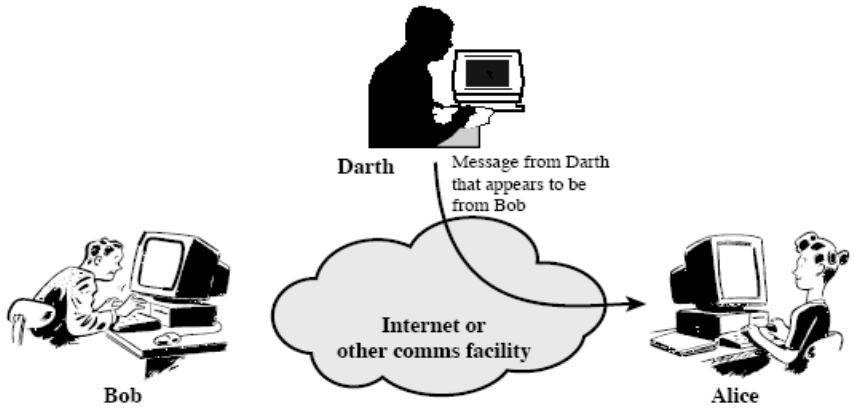
- Active attacks involve some modification of the data stream or the creation of a false stream.
- Involves alteration to the data.
- Difficult to prevent.
- Detection is possible and can be recovered from any disruption or delays caused by them.

Types of active attacks:

1. Masquerade
2. Replay
3. Modification of messages
4. Denial of service
5. Software attacks

Masquerade:

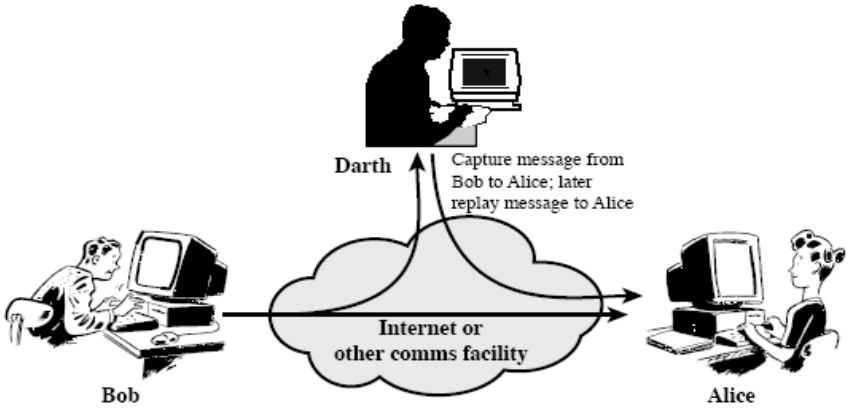
One entity pretends to be a different entity



(a) Masquerade

Replay:

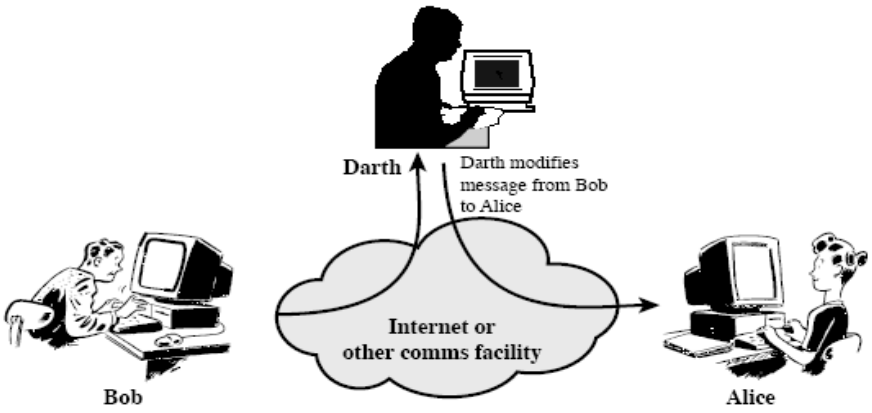
Passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect



(b) Replay

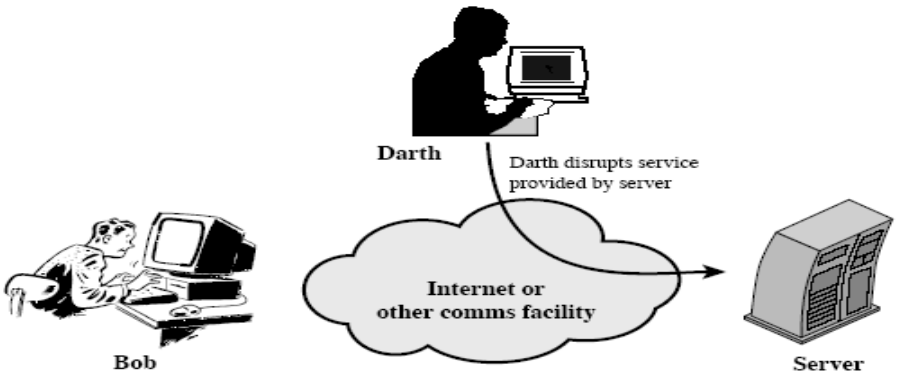
Modification of messages:

Alters some portion of a legitimate message or delay the message.



(c) Modification of messages

Denial of service:



(d) Denial of service

- It prevents or inhibits the normal use or management of communications facilities.
- It Suppress all the messages directed to a user or disable the network, degrade the performance.

Software attacks:

Software attacks are those which can be introduced into the systems or networks.

Example: - worms, viruses.

2. 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. Perhaps a clearer definition is found in RFC 2828, which provides the following definition: a processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms.

Different types of security services available:

- Authentication
- Access Control
- Data Confidentiality
- Data Integrity
- Non-Repudiation

Authentication

- It assures that the communication is authentic.
- It is the process of giving individuals access to system objects based on their identity.
- Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.
- It is usually based on a username and password

Access Control

It is the process of preventing unauthorized use of a resource

Data Confidentiality

It is the process of protecting data from unauthorized user.

Data Integrity

It assures that the data received is sent by an authorized entity and are not modified/replayed/deleted/updated.

Non-Repudiation

- protection against denial by one of the parties in a communication
- Nonrepudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.
- Nonrepudiation can be obtained through the use of:
    - digital signatures
    - confirmation services
    - timestamps

3. Security Mechanism:

- Feature designed to detect, prevent, or recover from a security attack
- no single mechanism will support all services required
- *Types*
    - Specific security mechanisms
    - Pervasive security mechanisms

Specific security mechanisms:

It may be incorporated into the appropriate protocol layer in order to provide some of the OSI security services

- Encipherment
- digital signatures
- access controls
- data integrity
- traffic padding
- Notarization
- Routing control etc,.

Encipherment:

- Use some mathematical algorithm to transform the data to some other format.

- It is used either to protect the confidentiality of data units and traffic flow information or to support or complement other security mechanisms.

Digital signatures:

- It is a data appended to the transformation that allows a receiver of the data unit to prove the source and integrity of the data is against forgery
- Digital signatures incorporate the data (or the hash of the data) that are signed.
- Different data therefore result in different signatures even if the signatory is unchanged.

Access controls:

- Prevention of the unauthorized use of a resource

Data integrity

- Assurance that data received is sent by an authorized entity

Traffic padding

- Insertion of bits into the data which is used during traffic analysis.
- It is used to protect against traffic analysis attacks.

Notarization

- It is used to assure certain properties of the data communicated between two or more entities, such as its integrity, origin, time, or destination.
- Use of Trusted third party(TTP) to assure

Routing control

- It is used to choose either dynamically or by prearrangement specific routes for data transmission

Pervasive security mechanisms:

- They are not specific to any particular OSI security services or protocol layer.
  - security labels
  - event detection

- security audit trails
- security recovery.

Security labels

- The name used for the security related resources.
- indicate sensitivity levels

Event detection

- Detection of events related to security
- detect apparent violations of security

Security audit trails

- Review of system records and activities
- detect breaches in security
- recommend any indicated changes in control, policy, and procedures.

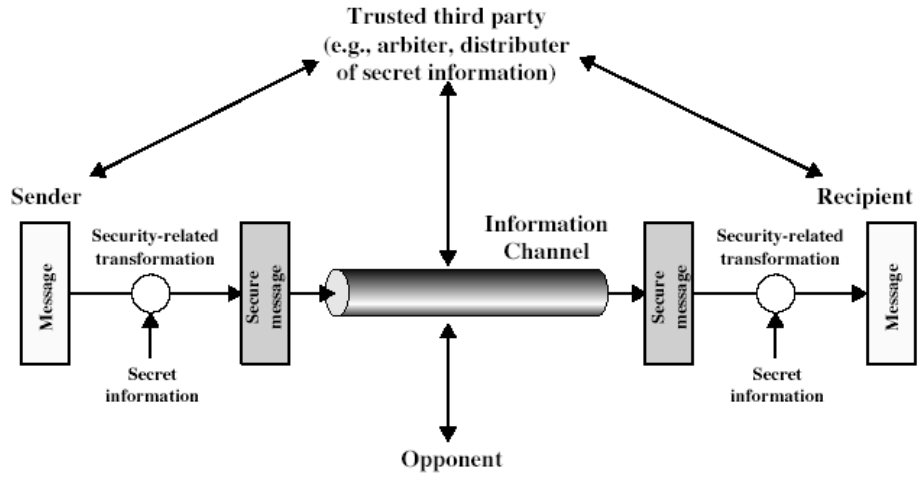
Security recovery

- deals with requests from mechanisms such as event handling and management functions
- takes recovery actions as the result of applying a set of rules.

Model for Network Security

In considering the place of encryption, it's useful to use the following two models.

The first diagram models information flowing over an insecure communications channel, in the presence of possible opponents. Hence an appropriate security transform (encryption algorithm) can be used, with suitable keys, possibly negotiated using the presence of a trusted third party.

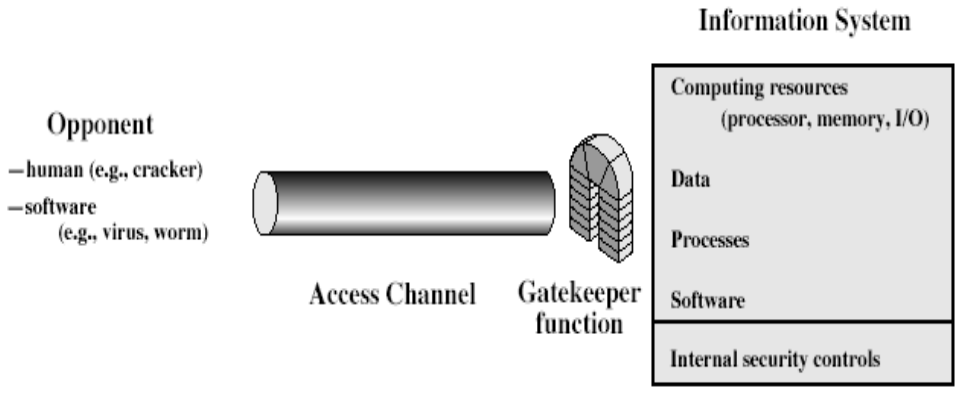


This general model shows that there are four basic tasks in designing a particular security service,

1. design a suitable **algorithm** for the security transformation
2. generate the **secret information (keys)** used by the algorithm
3. develop **methods to distribute** and share the secret information
4. specify a **protocol** enabling the users to use the transformation and secret information for a security service

Model for Network Access Security

The second, illustrated in Figure, model is concerned with controlled access to information or resources on a computer system, in the presence of possible opponents. Here appropriate controls are needed on the access and within the system, to provide suitable security. Some cryptographic techniques are useful here also.



Using this model requires us to:

1. select appropriate **gatekeeper functions** to identify users
2. implement **security controls** to ensure only authorised users access designated information or resources

CLASSICAL ENCRYPTION TECHNIQUES:

SYMMETRIC CIPHER MODEL:

- Symmetric encryption is also referred to as Conventional / private-key / single-key encryption.
- Sender and recipient share a common key
- All classical encryption algorithms are private-key
- It was only type prior to invention of public-key in 1970's

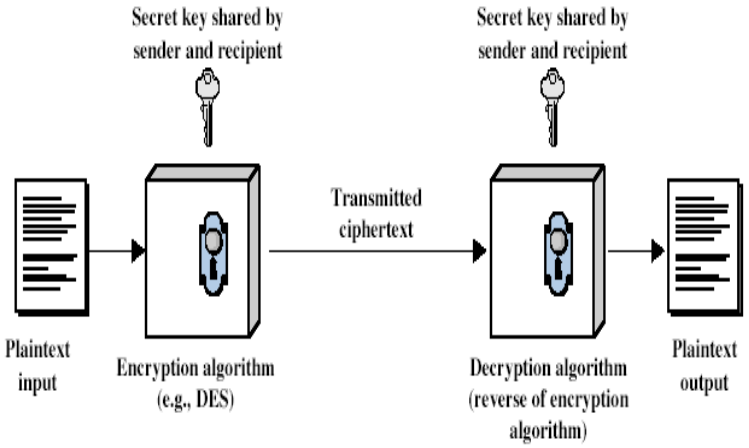
Some Basic Terminology:

- **plaintext** - original message
- **ciphertext** - coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - converting ciphertext to plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - field of both cryptography and cryptanalysis

Symmetric encryption scheme has five ingredients

- Plain text – original message or data that is fed into the algorithm as input.
- Encryption Algorithm – performs various substitutions and transformations on Plain Text.
- Secret key: - input to the encryption algorithm. Value independent of plain text.

- Cipher text: - scrambled message produced as output. Depends on the plaintext and the secret key.
- Decryption algorithm: - takes the cipher text and key to produce the original plaintext.



There are two requirements for secure use of conventional encryption:

1. a strong encryption algorithm
2. a secret key known only to **sender/receiver**

Mathematically have:

$$Y = E_K(X)$$

$$X = D_K(Y)$$

Cryptography:

S are Cryptographic system characterized along three independent dimensions:

- The type of encryption operations used
  - substitution / transposition etc,.
- The number of keys used
  - single-key or private / two-key or public
- The way in which plaintext is processed

- block cipher/ stream cipher

Cryptanalysis:

There are two general approaches to attacking conventional encryption scheme:

- Cryptanalytic attack
  - Attacks depend on algorithm + some knowledge of plaintext or plaintext-cipher text pairs.
- Brute-force attack
  - Tries every possible key on a piece of cipher text.

Types of attacks on Encrypted messages (Cryptanalytic attacks)

- Ciphertext only:- here the attacker knows the encryption algorithm and the cipher text. The attacker uses brute force approach and finds all possible keys. For large key space this cannot be used.
- Known plaintext – known CT, Enc alg, PT CT pair with secret keys
- Chosen plaintext
- Chosen ciphertext
- Chosen text

CLASSICAL SUBSTITUTION CIPHERS:

- A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols
- If plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

Some of the classical substitution ciphers

- Caesar Cipher
- Mono alphabetic Cipher
- Playfair Cipher
- Hill Cipher
- Poly alphabetic Cipher

- One time pad

Caesar Cipher:

- Earliest known substitution cipher proposed by Julius Caesar
- First used in military affairs
- Replaces each letter by 3rd letter down the alphabet.

Example:

Plain Text : meet me after the class

Cipher Text : PHHW PH DIWHU WKH FODVV

Note that the alphabet is wrapped around, so the letter following Z is A. We can define the transformation as:

PT	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
CT	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

The algorithm can be expressed as follows. For each PT p, substitute the CT c:

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

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

K is the shift which can be from 1 to 25.

Cryptanalysis of Caesar Cipher:

Disadvantage:

- only have 26 possible ciphers
- a brute force search
- given cipher text, just try all shifts of letters
- Language is known and easily traceable

Monoalphabetic Cipher:

With only 25 possible keys, the Caesar cipher is far from secure. A dramatic increase in the key space can be achieved by allowing an arbitrary substitution, where the translation alphabet can be any permutation of the 26 alphabetic characters

- ciphers in which the same plaintext letters are always replaced by the same ciphertext letters.
- Mono, meaning one, indicates that each letter has a single substitute.
- Rather than just shifting the alphabet could shuffle (jumble) the letters arbitrarily
- Each plaintext letter maps to a different random ciphertext letter
- To construct a monoalphabetic cipher, we need to create some ordering of the alphabet, such as **DKVQFIBJWPESCXHTMYAUOLRGZN**, and pair it with a plaintext alphabet,

Plain : abcdefghijklmnopqrstuvwxyz

Cipher : DKVQFIBJWPESCXHTMYAUOLRGZN

Attack - Language Redundancy and Cryptanalysis

- The relative frequency of the letters in the cipher text is determined.
- This is compared with the standard distribution for english.
- The colsely mathched ones in cipher are replaced with the characters of english.

Disadvantage:

- This attack provides result only when the text is long.
- Easy to break because they make use of frequency of occurence.
- To overcome this do multiple substitution for a single cipher called homophones.

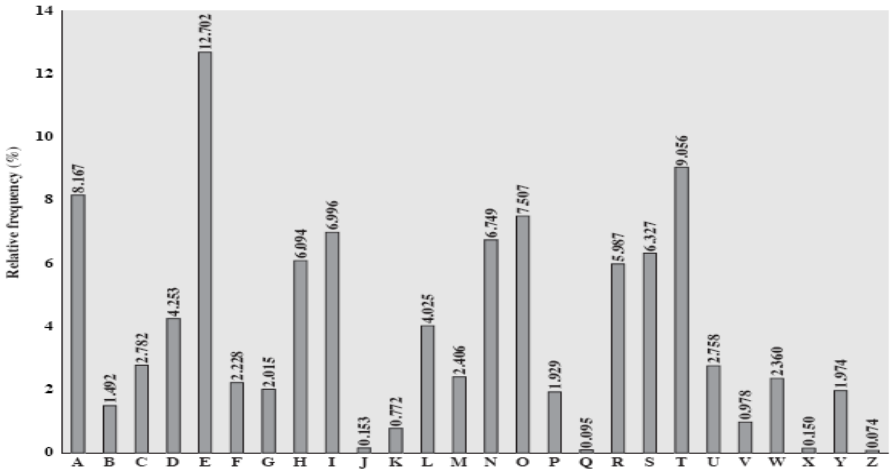


Figure 2.5 Relative Frequency of Letters in English Text

Playfair Cipher:

If we just map one letter always to another, the frequency distribution is just shuffled. One approach is to encrypt more than one letter at once.

- Multiple letter encryption cipher is the playfair cipher which treats diagrams in the plaintext as single units and translates these units into cipher text diagrams.
- Pair of letters are translated into other pairs of letters.

The playfair algorithm is based on the use of a 5x5 matrix of letters constructed using a keyword.

- Choose a Keyword that does not contain any letter more than once (eg. Keyword, Monarchy) & make sure that I and J do not both appear.
- Write the letters of that word in the first squares of a five by five matrix.
- Then finish filling up the remaining squares of the matrix with the remaining letters of the alphabet, in alphabetical order. Since there are 26 letters and only 25 squares, we assign I and J to the same square.

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

To encrypt a message:

1. divide it into pairs of letters. Pay no attention to punctuation or to spaces between words.

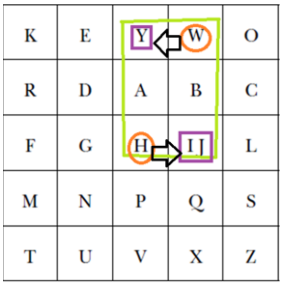
"Why, don't you?" becomes

WH YD ON TY OU

2. If both letters are the same (or only one letter is left), add an ``x" (any uncommon letter will do) after the first letter. **For example**, ``**balloon**" would be treated as ``**ba lx lo on**''.

3. Now, find each pair of letters in the matrix you made earlier. Most pairs of letters will form two corners of a smaller square or rectangle within the matrix.

- The enciphering of the pair WH is the pair at the two other corners of this rectangle, namely YI
- It's important to be consistent about the order of the new pair: the one that comes first is the one on the same row as the first of the original pair



4. If the letters appear on the same column of the table, replace them with the letters immediately below respectively.

For example, CO becomes LC.

(If one of the letters is at the end of the column, it is replaced by the top letter. OZ -> CO)

5. If the letters appear on the same row of the table, replace them with the letters to their immediate right respectively (the table wraps around).

For example EW -> YO

Polyalphabetic Cipher:

- Another way to improve the simple monoalphabetic tehcnique is to use different monoalphabetic substitutions as one proceeds through the plain text message.
- The most common method used is **Vigenère cipher**
- Vigenère cipher starts with a 26 x 26 matrix of alphabets in sequence. First row starts with 'A', second row starts with 'B', etc.

Table 2.4 The Modern Vigenere Tableau

	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

Encryption:

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

For eg. Message = SEE ME IN MALL

keyword = INFOSEC

Vigenère cipher works as follows:

Plain Text : S E E M E I N M A L L

Key : I N F O S E C I N F O

Cipher Text : A R J A W M P U N Q Z

Decryption:

- To decrypt, the receiver places the keyword characters below each ciphertext character
- Using the table, choose the row corresponding to the keyword character and look for the ciphertext character in that row
- Plaintext character is then at the top of that column

A R J A W M P U N Q Z

I N F O S E C I N F O

S E EMEIN M A L L

Improve over Vigenère Cipher:

The periodic nature of the keyword can be eliminated by using a nonrepeating keyword that is as long as the message itself. Keyword is concatenated with the plain text itself to provide a running key.

For example.

Key : **deceptive**wearediscoveredsav

Plaintext : wearediscoveredsaveyourself

Ciphertext : ZICVTWQNGKZEIIGASXSTSLVVWLA

One-Time Pad:

- Unconditional security !!!
- Proposed an improvement to the Vigenère Cipher
- Use a random key that was truly as long as the message, no repetitions.
- Produces random output that bears no statistical relationship to the plain text.
- Known Vigenère Cipher with one-time key

Given ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

Decrypt by hacker 1:

Ciphertext : ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

Key : pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih

Plaintext : mr mustard with the candlestick in the hall

Decrypt by hacker 2:

Ciphertext : ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

Key : pftgpmiydgaxgoufhklllmhsqdqogtewbqfgyovuhwt

Plaintext : miss scarlet with the knife in the library

Suppose that cryptanalyst had managed to find these two keys. Two plausible plaintexts are produced. Hard to find the correct decryption value.

Problems with one time pad:

- Problem of distribution and protection of long keys. The key has the same length as the plaintext.
- Problem of making large quantities of random keys. Supplying truly random characters in this volume is a significant task.

Hill Cipher:

- Hill cipher was invented by Lester Hill in 1929
- It is a multi-letter cipher.
- The algorithm takes m successive plaintext letters and substitutes for M cipher text letters.

$$C = E(K,P) = (KP)\text{mod}(26)$$
$$P = D(K,C) = (K^{-1}C)\text{mod}(26) = K^{-1}KP = P$$

Eg. PT = PAY (15 0 24)

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

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 15 & 0 & 24 \end{pmatrix} \text{mod}(26) = \begin{pmatrix} 375 & 819 & 486 \end{pmatrix} \text{mod}(26) = \begin{pmatrix} 11 & 13 & 18 \end{pmatrix} = LNS$$

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

$$\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \begin{pmatrix} 11 & 13 & 18 \end{pmatrix} \text{mod}(26) = \begin{pmatrix} 431 & 494 & 570 \end{pmatrix} \text{mod}(26) = \begin{pmatrix} 15 & 0 & 24 \end{pmatrix} = pay$$

TRANSPOSITION TECHNIQUES: (PERMUTATION)

- Hide the message by rearranging the letter order without altering the actual letters used
- The simplest such cipher is the **Rail Fence Cipher**
  - Write message on alternate rows, and read off cipher row by row
  - Example: (rail fence of depth 2)
    - meet me after the toga party

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

MEMATRHTGPRYETEFETEOAAT

Block (Columnar) Transposition Ciphers

- Message is written in rectangle, row by row, but read off column by column; The order of columns read off is the key
- Example:

Key: 4 3 1 2 5 6 7
Plaintext: a t t a c k p
o s t p o n e
d u n t l l t
wo a mx y z
Ciphertext:
TTNAAPTMTSUOAODWCOIXKNLYPETZ

ROTOR MACHINES:

- Each rotor corresponds to a substitution cipher
- A one-rotor machine produces a polyalphabetic cipher with period 26
- Output of each rotor is input to next rotor
- After each symbol, the "fast" rotor is rotated
- After a full rotation, the adjacent rotor is rotated (like *odometer*)
    - An *n* rotor machine produces a polyalphabetic cipher with period 26^n

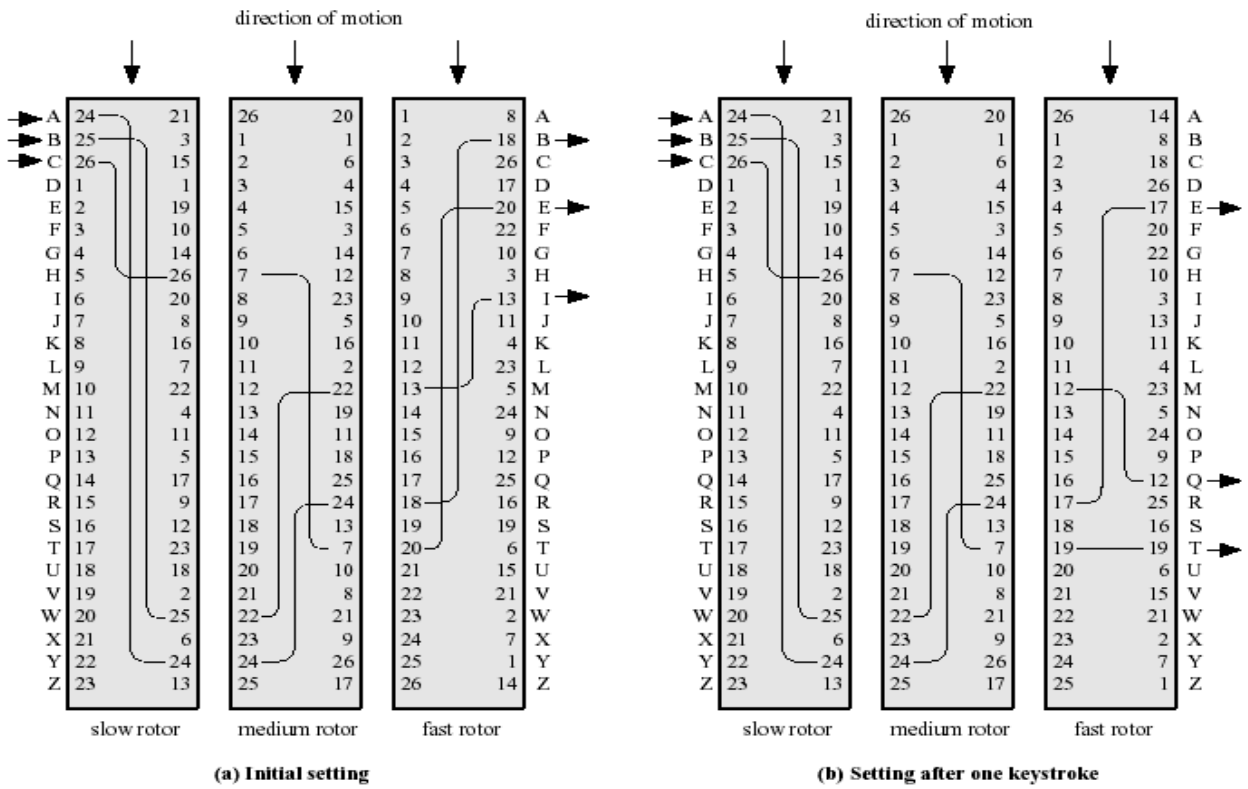


Figure 2.8 Three-Rotor Machine With Wiring Represented by Numbered Contacts

STEGANOGRAPHY:

- an alternative to encryption
- hides existence of message
- "steganography means hiding one piece of data within another".
  - Examples
    - Character marking
    - Invisible ink
    - Pin puncture
    - Typewriter correction ribbon.
- has drawbacks
  - high overhead to hide relatively few info bits