

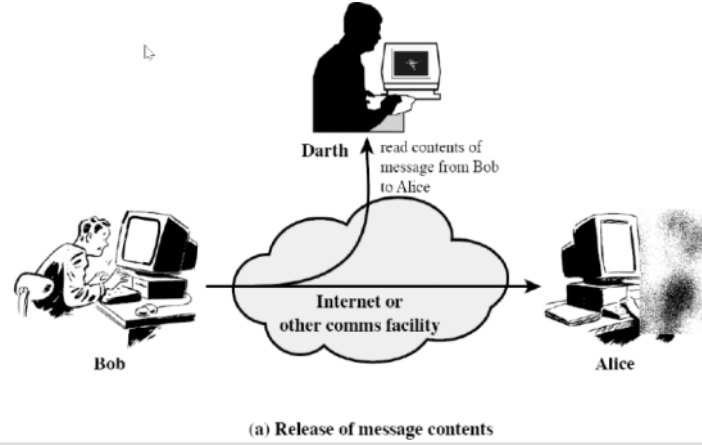
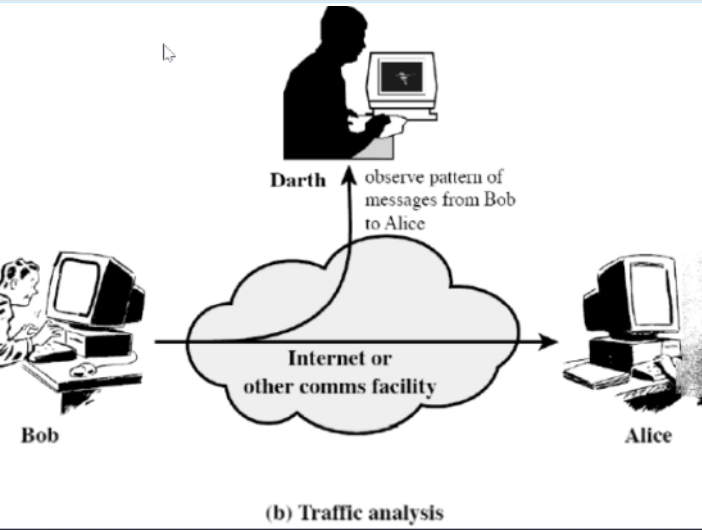
IS U1 Overview and Classical Encryption Techniques

Tuesday, November 9, 2021 14:01

1. What are the examples of security attacks?

a. Passive

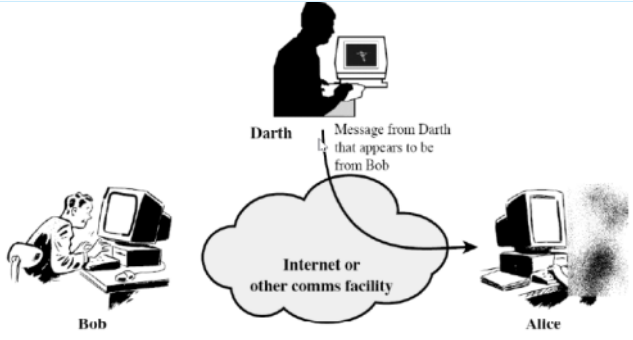
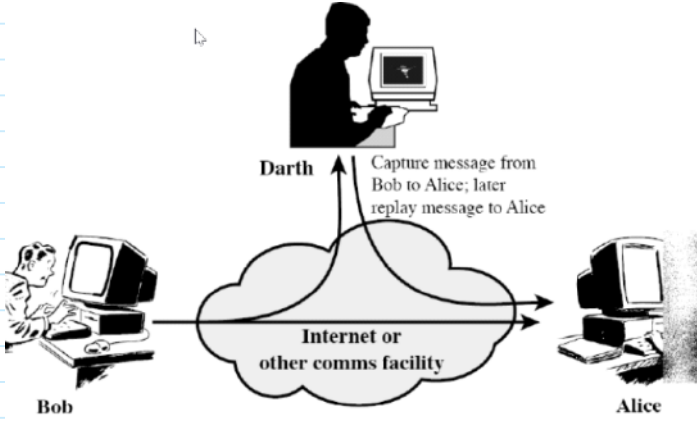
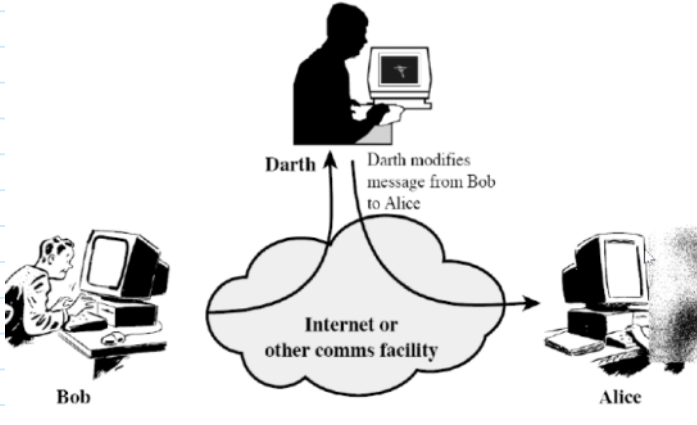
- i. Eavesdrop, monitor transmission
- ii. Obtain information being transmitted
- iii. Very difficult to detect; since no alteration of data

	Types	Description	
1	Release of message contents	a) tap on phone line to hear conversation b) get unauthorized copy of email message	 <p>(a) Release of message contents</p>
2	Traffic analysis	a) observe message pattern, even if encrypted b) determine location and identity of parties	 <p>(b) Traffic analysis</p>

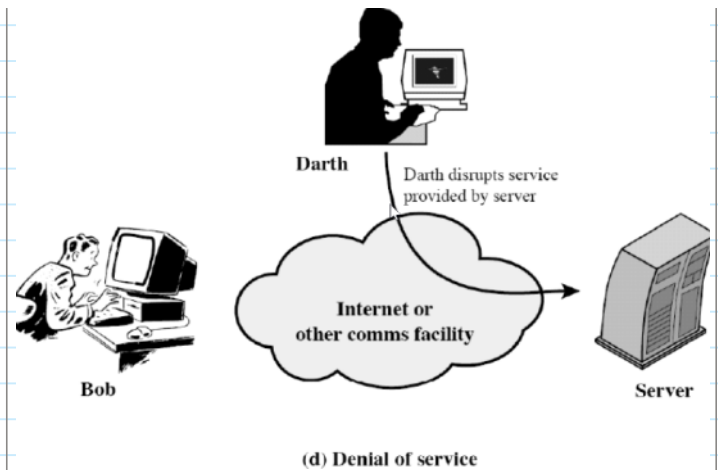
b. Active

- i. Modification of transmitted data or creating false data: subdivided into four categories

	Types	Description	
--	-------	-------------	--

1	Masquerade	pretend to be a different entity	 <p>(a) Masquerade</p>
2	Replay	capture data for subsequent retransmission	 <p>(b) Replay</p>
3	Modification of message	some portion of legitimate message is altered	 <p>(c) Modification of messages</p>

4	Denial of service	disruption of network by disabling or overloading
---	-------------------	---



2. List and briefly define categories of security services.

- Security services include authentication, access control, data confidentiality, data integrity, nonrepudiation, and availability.
- These enhance security of data processing systems and information transfers of an organization
- These are intended to counter security attacks using one or more security mechanisms.
- These often replicates functions normally associated with physical documents which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

X.800	a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfer
RFC 2828	a processing or communication service provided by a system to give a specific kind of protection to system resources

e. X.800 defines it in 5 major categories

1	Authentication	assurance that the communicating entity is the one claimed 1. Peer Entity Authentication - Used in association with a logical connection to provide confidence in the identity of the entities connected 2. Data-Origin Authentication - In a connectionless transfer, provides assurance that the source of received data is as claimed.
2	Access Control	prevention of the unauthorized use of a resource
3	Data Confidentiality	protection of data from unauthorized disclosure 1. Connection Confidentiality - The protection of all user data on a connection. 2. Connectionless Confidentiality - The protection of all user data in a single data block 3. Selective-Field Confidentiality - The confidentiality of selected fields within the user data on a connection or in a single data block. 4. Traffic-Flow Confidentiality - The protection of the information that might be derived from observation of traffic flows.
4	Data Integrity	assurance that data received is as sent by an authorized entity 1. 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. 2. Connection Integrity - As above, but provides only detection without recovery.

		<p>3. 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.</p> <p>4. 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.</p> <p>5. 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.</p>
5	Non-Repudiation	<p>protection against denial by one of the parties in a communication</p> <p>1. Nonrepudiation, Origin - Proof that the message was sent by the specified party.</p> <p>2. Nonrepudiation, Destination - Proof that the message was received by the specified party.</p>

3. Explain X.800 security mechanism?

- a. Page no 35
- b. feature designed to detect, prevent, or recover from a security attack
- c. no single mechanism that will support all services required
- d. however one particular element underlies many of the security mechanisms in use: cryptographic techniques
- e. X.800 distinguishes between reversible encipherment mechanisms and irreversible encipherment mechanisms.
- f. A reversible encipherment mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted
- g. Irreversible encipherment mechanisms include hash algorithms and message authentication codes, which are used in digital signature and message authentication applications.
- h. The X.800 security mechanism is divided into 2 parts -
 - i. specific security mechanisms
 - ii. Pervasive security mechanisms

SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
<p>May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.</p> <p>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.</p> <p>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).</p> <p>Access Control A variety of mechanisms that enforce access rights to resources.</p> <p>Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.</p> <p>Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.</p> <p>Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.</p> <p>Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.</p> <p>Notarization The use of a trusted third party to assure certain properties of a data exchange.</p>	<p>Mechanisms that are not specific to any particular OSI security service or protocol layer.</p> <p>Trusted Functionality That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).</p> <p>Security Label The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.</p> <p>Event Detection Detection of security-relevant events.</p> <p>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.</p> <p>Security Recovery Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.</p>

4. Explain model for network security?

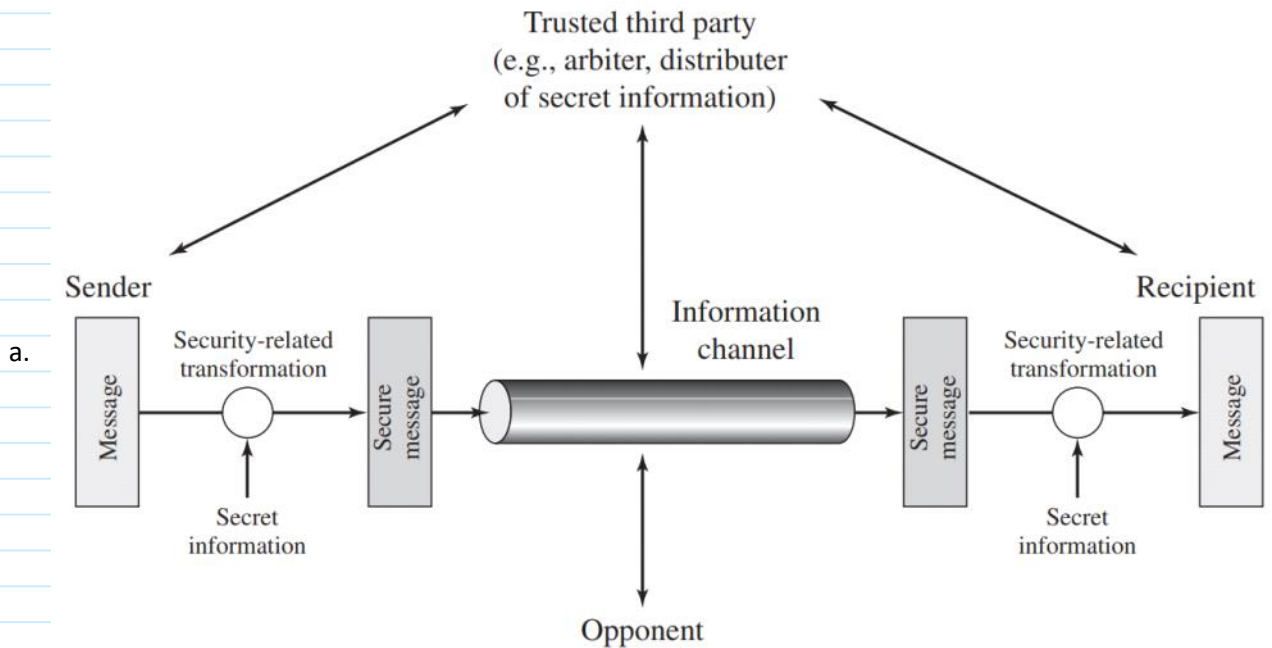


Figure 1.4 Model for Network Security

- b. All the techniques for providing security have two components
 - i. A security-related transformation on the information to be sent. Examples include the encryption of the message and the addition of a code to verify the identity of the sender
 - ii. Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used.
- c. Using this model requires us to:
 - i. design a suitable algorithm for the security transformation
 - ii. generate the secret information (keys) used by the algorithm
 - iii. develop methods to distribute and share the secret information
 - iv. specify a protocol enabling the principals to use the transformation and secret information for a security service

d. Network Access Security Model

- i. using this model requires us to:
 - 1) select appropriate gatekeeper functions to identify users
 - 2) implement security controls to ensure only authorized users access designated information or resources
- ii. trusted computer systems may be useful to help implement this mode

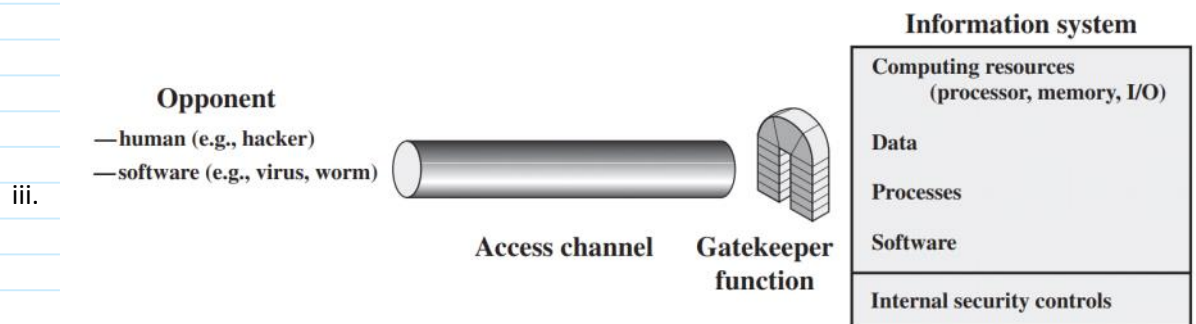


Figure 1.5 Network Access Security Model

5. Explain types of attacks on encrypted message.

6. List and briefly define types of cryptanalytic attacks based on what is

known to the attacker.

a. Cryptanalysis

- i. exploit characteristics of algorithm to deduce plaintext or encryption key
- ii. may use **pairs of plaintext, ciphertext**
- iii. Attempt to deduce specific plaintext or key
- iv. Rely on
 - 1) nature of algorithm
 - 2) some knowledge of plaintext characteristics
- v. Examples
 - 1) some file types have common header
 - 2) exploit statistics of human language
 - 3) power consumed by encryption algorithm

Cryptanalysis Attacks	
Types of Attacks on Encrypted Messages	
Type of Attack	Known to Cryptanalyst
Ciphertext Only	<ul style="list-style-type: none">• Encryption algorithm• Ciphertext
Known Plaintext	<ul style="list-style-type: none">• Encryption algorithm• Ciphertext• One or more plaintext–ciphertext pairs formed with the secret key
Chosen Plaintext	<ul style="list-style-type: none">• Encryption algorithm• Ciphertext• Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	<ul style="list-style-type: none">• Encryption algorithm• Ciphertext• Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	<ul style="list-style-type: none">• Encryption algorithm• Ciphertext• Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key• Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

7. Explain substitution ciphers Caesar, Monoalphabetic, Playfair, and Hill.

a. Caesar Cipher

b. Monoalphabetic Cipher

c. Playfair Cipher

d. Hill Cipher

- i. developed by the mathematician Lester Hill in 1929
- ii. The encryption algorithm takes **m successive plaintext letters and substitutes for them m ciphertext letters**
- iii. The substitution is determined by m linear equations in which each character is assigned a numerical value ($a = 0, b = 1, \dots, z = 25$).
- iv. Hill cipher is that it completely hides single-letter frequencies
- v. the use of a larger matrix hides more frequency information.
- vi. Thus a 3 X 3 Hill cipher hides not only single-letter but two-letter frequency information.

8. Explain Polyalphabetic substitution ciphers, Vigenère, autokey, and one-time pad.

1. Polyalphabetic substitution ciphers

- This approach **uses multiple cipher alphabets**.
- A set of related monoalphabetic substitution rule is used (consists of 26 Caesar Ciphers)
- A key determines which particular rule is chosen for a given transformation
- makes **cryptanalysis harder with more alphabets** to guess and **flatter frequency distribution**
- Uses a **key to select which alphabet is used for each letter of the message**
- Uses each alphabet in turn
- Repeats from start when end of key is reached

2. Vigenère

- simplest polyalphabetic substitution cipher is the Vigenère Cipher
- effectively multiple caesar ciphers
- key is multiple letters long $K = k_1 k_2 \dots K_d$
- 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

3. Autokey

- Ideally we 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.
- It is used in turn on the rest of the message
- Autokey has **frequency characteristics to attack**

eg. given key *deceptive*

- | | | | | |
|-------------|---------------------------------|-------------------|------|--|
| key: | deceptive | we are discovered | save | |
| plaintext: | we are discovered save yourself | | | |
| ciphertext: | ZICVTWQNGKZEIIGASXSTSLVVWLA | | | |

4. One-Time Pad

- if a truly random key as long as the message is used, the cipher will be secure
- 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
- One-Time Pad has a **problem of making large quantities of keys, safe distribution of keys**

9. Briefly define the Caesar cipher.

- It is one of the Substitution Techniques
- Ciphertext letter = plaintext letter + 3 (or k)
- Letters wrap around, Z is next after A
- cipher by Julius Caesar used in military affairs
- replaces each letter by 3rd letter on

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
0 1 2 3 4 5 6 7 8 9 10 11 12
n o p q r s t u v w x y z
13 14 15 16 17 18 19 20 21 22 23 24 25

f.

then have **Caesar** cipher as:

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

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

p-plain text letter

k-position down the alphabet value in the range 1 to 25

10. Briefly define the monoalphabetic cipher.

- a. Arbitrary substitution of letters
- b. rather than just shifting the alphabet could shuffle (jumble) the letters arbitrarily
- c. each plaintext letter maps to a different random ciphertext letter hence key is 26 letters long
- d. Regularities in the language can be exploited

e. Monoalphabetic Cipher Security

- i. Number of keys $26 \times 25 \times \dots \times 1 = 26!$ (Over 4×10^{26})
- ii. Due to language characteristics, this is insecure even though this has so many keys
- iii. human languages are redundant. The letters are not equally, commonly used
- iv. In English e is by far the most common letter then T,R,N,I,O,A,S
- v. Other letters are fairly rare e.g. Z,J,K,Q,X
- vi. This cipher has tables of single, double & triple letter frequencies

f. Use in Cryptanalysis

- i. key concept - monoalphabetic substitution ciphers **do not change relative letter frequencies**
- ii. calculate letter frequencies for ciphertext
- iii. compare counts/plots against known values
- iv. for monoalphabetic must identify each letter – tables of common double/triple letters help
- v. Monoalphabetic ciphers are **easy to break because they reflect the frequency data of the original text**

11. Briefly define the Playfair cipher.

Substitution Techniques

- i. Letters in plaintext is replaced by
 - 1) other letters
 - 2) numbers
 - 3) symbols
- ii. Plaintext bit-sequence is replaced by a ciphertext sequence

1. Playfair cipher

- i. This is one of the substitution techniques
- ii. not even the large number of keys in a monoalphabetic cipher provides security
- iii. one approach to improving security was to encrypt multiple letters
- iv. invented in **1854**. It was used for tactical purposes by British forces in the World War I.
- v. In playfair cipher unlike traditional cipher we **encrypt a pair of alphabets(digraphs) instead of a single alphabet.**
- vi. **Playfair Key Matrix**

- 1) a 5X5 matrix of letters based on a keyword

vii. Advantages

- 1) **26×26 diagrams (two letter combinations)**
- 2) Possible keys? (key consists of the alphabet (reduced to 25 letters) spread on a 5x5 square, that's **25!25! Keys**)

viii. Disadvantages

- 1) still leaves much of language structure
- 2) **few 100s of ciphertext letters are enough** for cryptanalysis

ix. Security of the Playfair Cipher

- 1) security much **improved over monoalphabetic** (frequency of two letter combinations)
- 2) would **need a 676 entry frequency table to analyze** (verses 26 for a monoalphabetic) and correspondingly more ciphertext
- 3) it **can be broken**, given a few hundred letters since still has **much of plaintext structure**

12. Explain transposition techniques.

- a. Traditional (pre-computer) symmetric ciphers use transposition techniques.
- b. Transposition techniques systematically **transpose the positions of plaintext elements**.
- c. Transposition: elements in plain text are rearranged.
- d. It is classical transposition or permutation ciphers
- e. these **hide the message by rearranging the letter order without altering the actual letters**
- f. can recognize these since have the **same frequency distribution as the original text**

o -----

- [Transposition techniques | Working & List Of Transposition Techniques \(educba.com\)](https://educba.com/transposition-techniques/)

1. Rail-Fence Technique

- i. Rail-Fence is the simple Transposition technique that involves writing **plain text as a sequence of diagonals and then reading it row by row** to produce the ciphertext.
- ii. The Rail-Fence technique is quite **easy to break**

2. Simple columnar transposition techniques

- i. The simple columnar transposition technique can be categorized into two parts – Basic technique and multiple rounds.
- ii. Simple columnar transposition technique – basic technique. The simple columnar transposition technique simply arranges the **plain text in a sequence of rows of a rectangle and reads it in a columnar manner**.

3. Simple columnar transposition technique – Multiple rounds

- i. Simple columnar transposition technique with multiple rounds is the same as basic; only the difference is that we **iterate the process multiple times in multiple rounds**.

4. Vernam Cipher

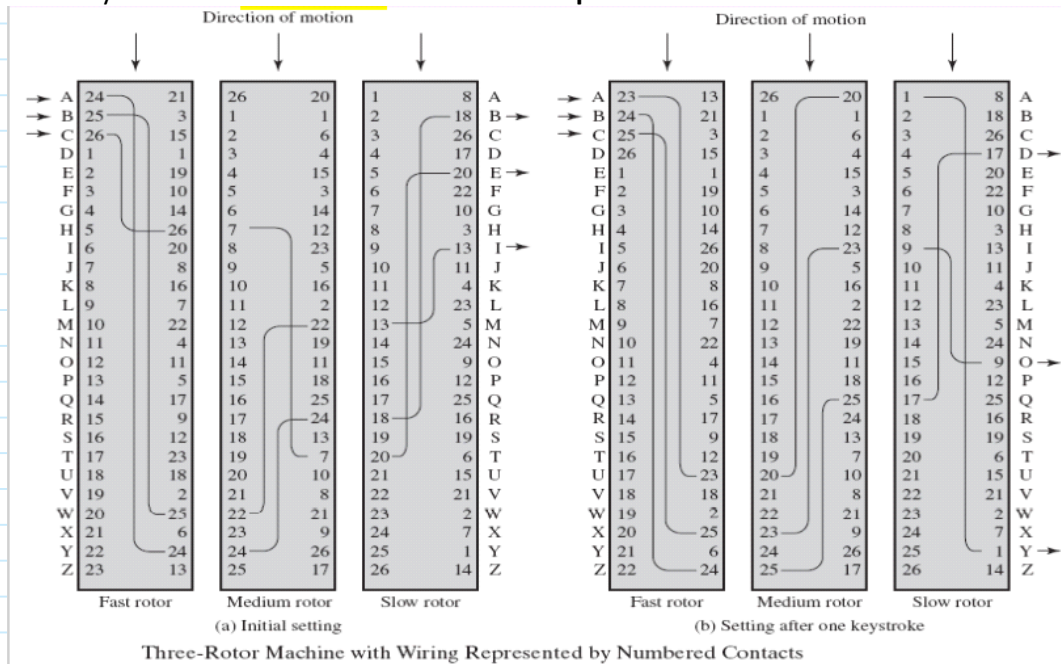
- i. A subset of Vernam cipher is called a one-time pad because it is implemented using a **random set of nonrepeating characters as an input ciphertext**.

13. Explain operation of Rotor machine.

- a. Rotor machines are sophisticated pre-computer hardware devices that use **substitution** techniques.
- b. **multiple stages of encryption** can produce an algorithm that is significantly more difficult to cryptanalyze.
- c. Before DES, rotor machines using multiple stages of encryption
- d. machine consists of a **set of independently rotating cylinders** through which **electrical pulses can flow**.
- e. Each cylinder has **26 input pins and 26 output pins**, with internal wiring that connects **each input pin to a unique output pin**.
- f. single cylinder defines a **monoalphabetic substitution**
- g. **before modern** ciphers, rotor machines were most **common product cipher**
- h. implemented a **very complex, varying substitution cipher**

- i. used a series of cylinders, each giving one substitution, which **rotated and changed after each letter was encrypted**
- j. with 3 cylinders have **$26^3=17576$ substitution alphabets**

k.



14.