ASSIGNMENT 1

Q1] With an example differentiate mono-alphabetic and poly-alphabetic encryption techniques / ciphers.

Mono-alphabetic	Poly-alphabetic
1. A substitution cipher where each letter in the plaintext is replaced by the corresponding letter in the cipher text.	1. A cipher that uses multiple substitution alphabets to encrypt plaintext, varying the substitution.
2. The key length of this encryption technique is fixed.	2. The key length of this encryption technique is variable.
3. It is less secure, as frequency analysis can break it easily.	3. It is more secure, as frequency analysis is less effective.
4. It is limited to simple substitutions like Ceaser, Atbash.	4. It is a more complex technique including Beaufort, Enigma.
5. It is used in basic cryptography like newspaper cryptograms.	5. It is used in advanced cryptography like espionage.
6. Involves reversing the fixed shift to get the original plaintext.	6. Involves using the same keyword to reverse the shifts.

7. The pattern in the cipher text mirrors the frequency of letters in plaintext.	7. The pattern is less obvious, as the cipher uses multiple alphabets.
8. It is simple to compute & break, even by hand.	8. It is more complex, requiring time to break.
9. It is not adaptable to modern encryption techniques/needs.	9. Some are adaptable to modern principles, like block ciphers.
10. Used by Julius Ceaser for secret communications.	10. Used during wars & diplomatic communications.

- Example for Mono-Alphabetic Cipher:
- PLAIN TEXT: RESIDENT EVIL ZERO
- KEY LENGTH: 3
- CIPHER TEXT: UHVLGHQW HYLO CHUR

In the above example, the same shift is applied to each letter in the plain text.

- Example for Poly-Alphabetic Cipher:
- PLAIN TEXT: HELLO
- KEYWORD: LEMON
- CIPHER TEXT: SIXZB

In the above example, each letter is encrypted using a different shift, determined by the keyword 'LEMON', making it harder to break.

Q2] Encrypt "This is the world cup match" with playfair cipher using key 'Captain'.

PlainText: THIS IS THE WORLD CUP MATCH
Key: CAPTAIN

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

TH	IS	IS	TH	EW	OR	LD
↓	↓	↓	↓	↓	↓	↓
AL	TU	TU	AL	BY	QS	KE

CU	PM	AT	CH
↓	↓	↓	↓
IO	JK	PI	AG

CIPHER TEXT: ALTUTUALBYQSKEIOJKPIAG

Q3] Compare DES and AES.

DES	AES
1. It was developed by IBM in the 1970s.	1. It was developed by NIST in 2001.
2. DES uses a 56-bit key size.	2. AES uses 128, 192, or 256 bit key size.
3. There are a total of 16 rounds of encryption.	3. Total number of rounds vary basis on key size.
4. It is considered insecure due to small key size & vulnerable to brute-force attacks.	4. It is considered highly secure & resistant to known attacks like brute force.
5. It is slower, especially with software implementation	5. It is faster with H/W & S/W optimization.
6. The structure of DES is a Feistel Network.	6. The structure of AES is a Substitution-Permutation Network.
7. It is considered outdated & is replaced by AES.	7. It is the current encryption standard.
8. It has a 64-bit block size.	8. It has a 128-bit block size.
9. Used in banking & legacy systems.	9. Used in SSL/TLS & VPNs.

Q4] Given modulus n = 91 & public key e = 5, find the values of p, q and phi(n) and d using RSA Algorithm. Encrypt M = 25. Also perform decryption.

Given:
n = 91
e(public key) = 5
M(message) = 25

To find:
p, q, $\phi(n)$, d

Solution:

- STEP 1: Finding p and q

n = 91 is the product of two prime numbers 'p' & 'q'
∴ We factorize 91
∴ 91 = 7 X 13
Hence, p = 7 and q = 13

- STEP 2: $\phi(n)$

We know that,
$\phi(n) = (p-1) \times (q-1)$
Substitute 'p' & 'q':
$\phi(91) = (7-1) \times (13-1)$
$= 6 \times 12$
$= 72$

- STEP 3: Calculate d

We know that
$e \times d = 1 \bmod [\phi(n)]$
Substituting values
$\therefore 5 \times d = 1 \bmod [72]$
$\therefore d = 29$

- STEP 4: Encryption

We know that

$C = M^e \pmod n$
Where,
$M = 25, e = 5, n = 91$
$\therefore C = 25^5 \pmod{91}$
$= 9765625 \pmod{91}$
$= 38$
$\therefore C = 38$

- STEP 5: Decryption

We know that

$M = C^d \pmod n$
Where, $C = 38, d = 29, n = 91$
$\therefore M = 38^{29} \pmod{91}$
$= 25$
$\therefore M = 25$

- FINAL ANSWERS

① $p = 7, q = 13$
② $\phi(n) = 72$
③ $d = 2$
④ Encryption (C) = 38
⑤ Decryption (M) = 25

Q5] Explain the following:
WHOIS, dig, traceroute, nslookup, ifconfig, hostname, ping, netstat, arp and SYSTEMINFO.

① WHOIS:
- 'WHOIS' is a query/response protocol used to lookup the registration information of a domain name or IP address. It provides details about the domain owner, registrar, registration date, expiration date, & other relevant information. 'WHOIS' data is crucial for identifying the entity behind a website or network resource, & its widely used in domain management & cybersecurity.

② dig:
- 'dig' (Domain Information Groper) is a network tool used to query DNS servers and troubleshoot DNS problems. It retrieves information such as IP addresses for domain names and other DNS records. Its commonly used to verify that DNS servers are working correctly and resolving domain names as expected.

③ traceroute:
- 'traceroute' is a network diagnostic tool used to trace path packets take from a source computer to a destination across the network. It displays the sequence of devices that data passes through, along with the time taken at each hop. This helps diagnose where delays or failures occur in a network route.

④ nslookup:

- 'nslookup' is a command line tool used to query DNS servers to obtain domain name or IP address mapping information. It is used to determine the IP address of domain or to check DNS records for troubleshooting network or DNS issues. It is helpful in resolving hostname-to-IP mappings or verifying DNS configurations.

⑤ ifconfig:

- 'ifconfig' (interface configuration) is a command-line utility used to configure, manage and query the network interface settings of a system. It can be used to check the IP addresses, subnet mask, and status of network interfaces. Additionally, it allows enabling/disabling interfaces or assigning new IP addresses. It has mostly been replaced by 'ip' command in modern linux systems.

⑥ hostname:

- 'hostname' command is used to display or set the system's hostname, which is the label used to identify the machine in a network. It is crucial for network communication, as the hostname is a part of machine's network identification. It can also be used to resolve a system's domain name or FQDN (Fully Qualified Domain Name)

⑦ ping:

- 'ping' is a command line utility used to test the reachability of a host on a network by sending ICMP (Internet Control Message Protocol) echo requests packets. It measures the round-trip time for messages sent to the host and used to diagnose connectivity issues, assess network latency and determine whether a remote device is online.

⑧ netstat:

- 'netstat' is a network troubleshooting tool that displays active connections, listening ports, routing tables & various network interface statistics. It helps administrators identify which applications are using network resources, track incoming & outgoing connections & detect potential security breaches or traffic issues.

⑨ arp:

- The 'arp' command is used to view and manipulate the address resolution protocol (ARP) cache, which maps IP addresses to MAC (Media Access Control) addresses. It is useful in troubleshooting local network problems, as ARP is critical for IP communication in a LAN environment by ensuring IP packets are correctly delivered to their intended physical devices.

⑩ SYSTEMINFO:

- 'SYSTEMINFO' is a windows command line tool that provides detailed information about the system's hardware & software configuration. It displays information

such as OS version, processor type, memory details, network configuration, & other system properties. This helpful for system diagnostics, inventory management, & troubleshooting.

Q6 What are different packet sniffer tools?

- A packet sniffer, also known as a network analyzer or protocol analyzer, is a tool used to capture, analyze & monitor network traffic passing through a network interface. They can capture data packets exchanged between devices on a network, allowing network admins or security professionals to troubleshoot network issues, identify security threats & monitor traffic. They can operate in either promiscuous mode, where they capture all traffic on the network, or non-promiscuous mode, where they capture only traffic addressed to the system running the sniffer.

Packet sniffers are useful for:

① Troubleshooting network issues like latency, packet loss, or connectivity problems.
② Monitoring network usage & bandwidth consumption.
③ Analyzing traffic for security vulnerabilities or potential attacks.
④ Capturing data for compliance or investigate purposes.

Following are the different packet sniffer tools:

① Wireshark:

- Wireshark is one of the most popular packet sniffing tools. It provides user-friendly graphical interface for capturing & analyzing packets in real-time.
- Supports deep packet inspection & can analyze protocols
- Allows live traffic capture or analysis of previously saved packet data.
- Provides powerful filtering options to narrow down the captured data.
- Works on Windows, linux, macOS
- Eg: Network troubleshooting, protocol analysis.

② tcpdump:

- It is a command line packet sniffing tool used primarily on Unix-based os. It is highly efficient for capturing & analyzing packets in text-based format.
- Lightweight & ideal for quick diagnostics.
- Captures packets from network interfaces & displays the headers of packets in real time.
- Eg: log analysis.

③ Tshark:

- It is the commandline version of Wireshark. It offers similar functionality but without the graphical user interfaces.
- Allows for real-time packet capture & analysis.
- Supports a wide range of network protocols.
- Works well for batch processing.
- Eg: Basic networking analysis, automated network logging.

④ Snort:

- Snort is an open-source network intrusion detection system (NIDS) & packet sniffer. It analyzes traffic in real time & can alert admins to suspicious activities.
- Capable of real-time packets sniffing and net-work intrusion detection.
- Highly configurable & used in conjunction with other tools for network security.
- Eg: Intrusion detection, security analysis

⑤ NetworkMiner:

- It is a network forensics tool that focuses on extracting artifacts like images, documents, & other data from captured packets, rather than just packet-level data.
- Helps in forensic investigations by analyzing compromised system's network traffic.
- Extracts data from TCP/UDP streams and reconstructs files transmitted over the netwo-rk.
- Eg: Data recovery, analysis of network attacks.