IV/IV B.Tech (Regular) DEGREE EXAMINATION

Nov, 2022 **Institutional Elective (Common to all branches)**

Seventh Semester **Cyber Security**

Time: Three hours **maximum:** 50 Marks

Answer question No.1 compulsorily. (1*10=10 Marks)

Answer one question from each unit (4*10=40 Marks)

1. Answer the following

a) Define Computer Security. **1M**

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources. Such as hardware, software, firmware, information/data, and telecommunications

b) Memorize Passive Attack. **1M**

A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring transmission.

c) State man in the middle attack **1M**

A man-in-the-middle (MiTM) attack is a type of cyber attack in which the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other. The attack is a type of eavesdropping in which the attacker intercepts and then controls the entire conversation.

d) Recall the applications of public key cryptosystems. **1M**

Encryption /decryption: The sender encrypts a message with the recipient's public key.

Digital signature: The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.

Key exchange: Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties.

e) What is public key and private key? **1M**

Public Key: In a Public key, two keys are used one key is used for encryption and another key is used for decryption. One key (public key) is used to encrypt the plain text to convert it into cipher text and another key (private key) is used by the receiver to decrypt the cipher text to read the message.

Private Key: In the Private key, the same key (secret key) is used for encryption and decryption. In this key is symmetric because the only key is copied or shared by another party to decrypt the cipher text. It is faster than public-key cryptography.

f) What is the use of Diffie Hellman key exchange? **1M**

Diffie-Hellman key exchange's goal is to securely establish a channel to create and share a key for symmetric key algorithms. Generally, it's used for encryption, password-authenticated key agreement and forward security. Password-authenticated key agreements are used to prevent man-in-the-middle (MitM) attacks.

g) Who is gray hat hacker? **1M**

A gray hat hacker is someone who may violate ethical standards or principles, but without the malicious intent ascribed to black hat hackers. Gray hat hackers may engage in practices that seem less than completely above board, but are often operating for the common good.

h) Define privacy in cyberspace. **1M**

Cyberspace is shorthand for the web of consumer electronics, computers, and communication networks that interconnects the world. Privacy is the need of people to choose freely under what conditions and to what extent they will expose themselves, their approach and their conduct to others.

i) Define a Malware. **1M**

Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network or server.

j) What is meant by information gathering? **1M**

Information Gathering is the act of gathering different kinds of information against the targeted victim or system. Information gathering is not just a phase of security testing; it is an art that every penetration-tester (pen-tester) and hacker should master for a better experience in penetration testing.

UNIT-1

2.a) Explain security services. **5M**

Each security service---1M

Authentication

The authentication service is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from.

Two specific authentication services are defined in X.800:

• **Peer entity authentication:** Provides for the corroboration of the identity of a peer entity in an association. Two entities are considered peers if they implement to same protocol in different systems.

• **Data origin authentication**: Provides for the corroboration of the source of a data unit. It does not provide protection against the duplication or modification of data units.

Access Control

In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

Data Confidentiality

Confidentiality is the protection of transmitted data from passive attacks. With respect to the content of a data transmission, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time.

Data Integrity

As with confidentiality, integrity can apply to a stream of messages, a single message, or selected fields within a message. Again, the most useful and straightforward approach is total stream protection. A connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays.

Non-repudiation

Non-repudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

b) Illustrate the symmetric cipher model and explain. 5M

Diagram---1M Explanation-- 4M

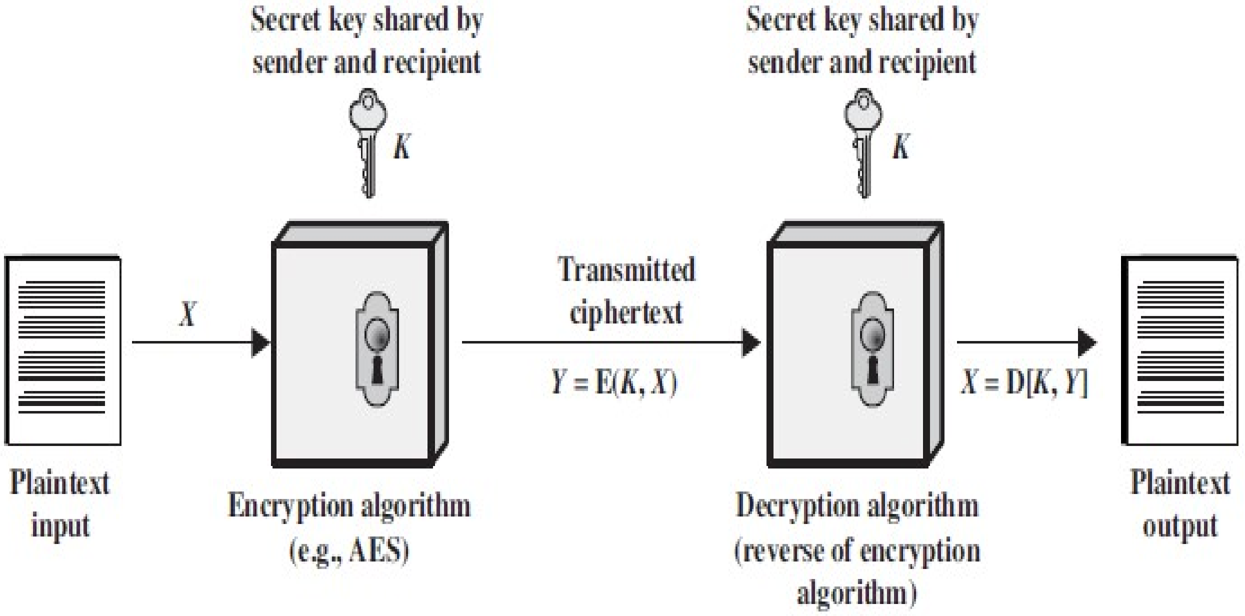
A symmetric encryption scheme has five ingredients

- **Plaintext**: This is the original intelligible message or data that is fed into the algorithm as input.
- **Encryption algorithm**: The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key:** The secret key is also input to the encryption algorithm.The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time.The exact substitutions and transformations performed by the algorithm depend on the key.
- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher texts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

There are two requirements for secure use of conventional encryption:

1. We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key.This requirement is usually stated in a stronger form:The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.

2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

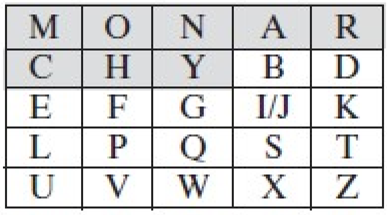

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

3.a) Discuss the following classical substitution techniques i) Monoalphabetic Cipher ii) Playfair Cipher 4M

Monoalphabetic Cipher---2M Playfair Cipher---2M

Monoalphabetic Cipher: 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 occurrence in that plaintext, 'A' will always get encrypted to 'D'.

Playfair Cipher The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.The Playfair algorithm is based on the use of a 5 × 5 matrix of letters constructed using a keyword.



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

In this case, the keyword is *monarchy*. The matrix is constructed by filling in the letters of the keyword (minus duplicates) 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. Plaintext is encrypted two letters at a time, according to the following rules:

1. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.

2. Two 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 example, ar is encrypted as RM.

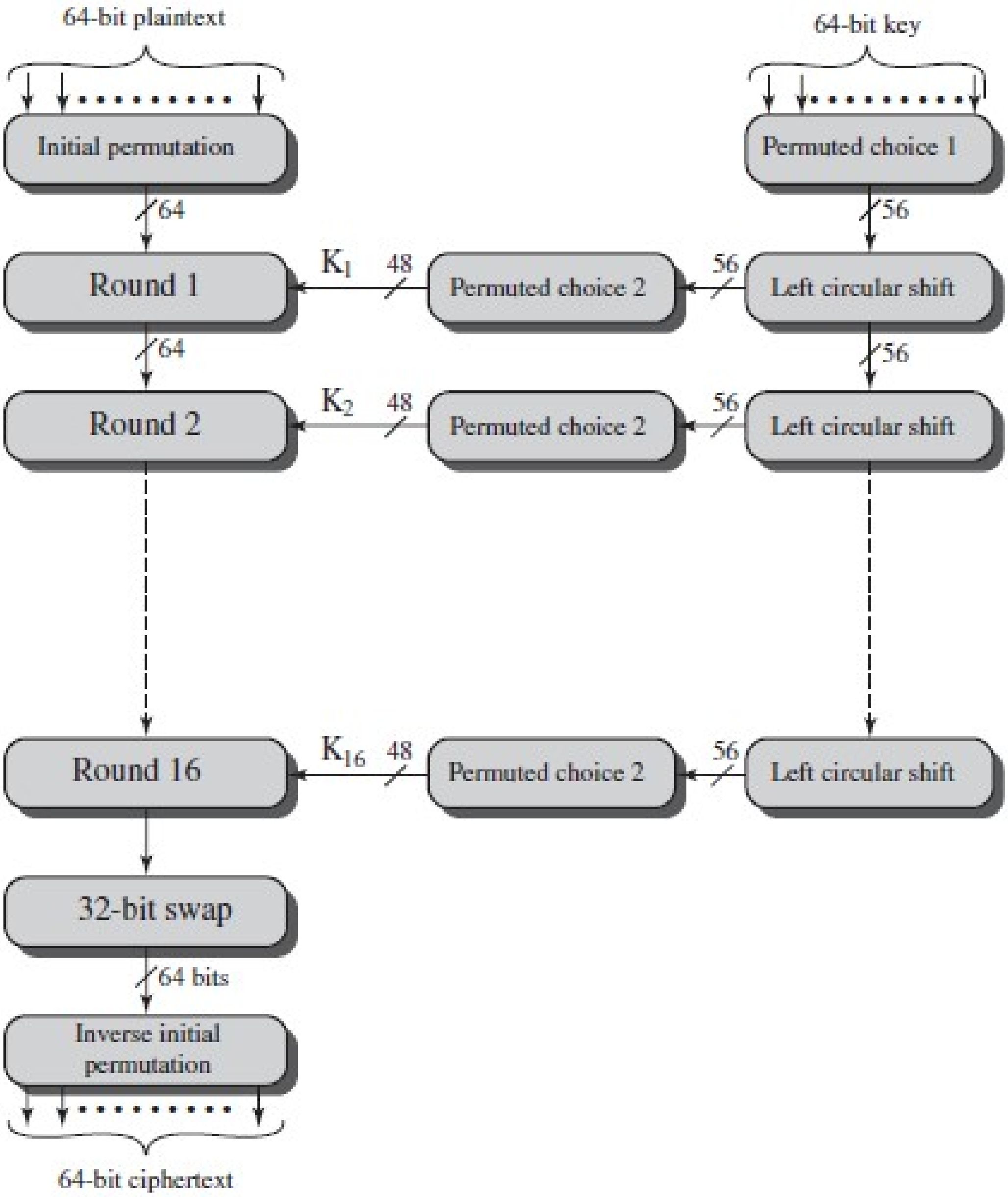
3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, mu is encrypted as CM.

4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

b) Explain DES encryption algorithm with neat sketch. 6M

Diagram---2M Explanation---4M

The overall scheme for DES encryption is illustrated in Figure As with any encryption scheme, there are two inputs to the encryption function: the plaintext to be encrypted and the key. In this case, the plaintext must be 64 bits in length and the key is 56 bits in length.



Looking at the left-hand side of the figure, we can see that the processing of the plaintext proceeds in three phases. First, the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the *permuted input*.

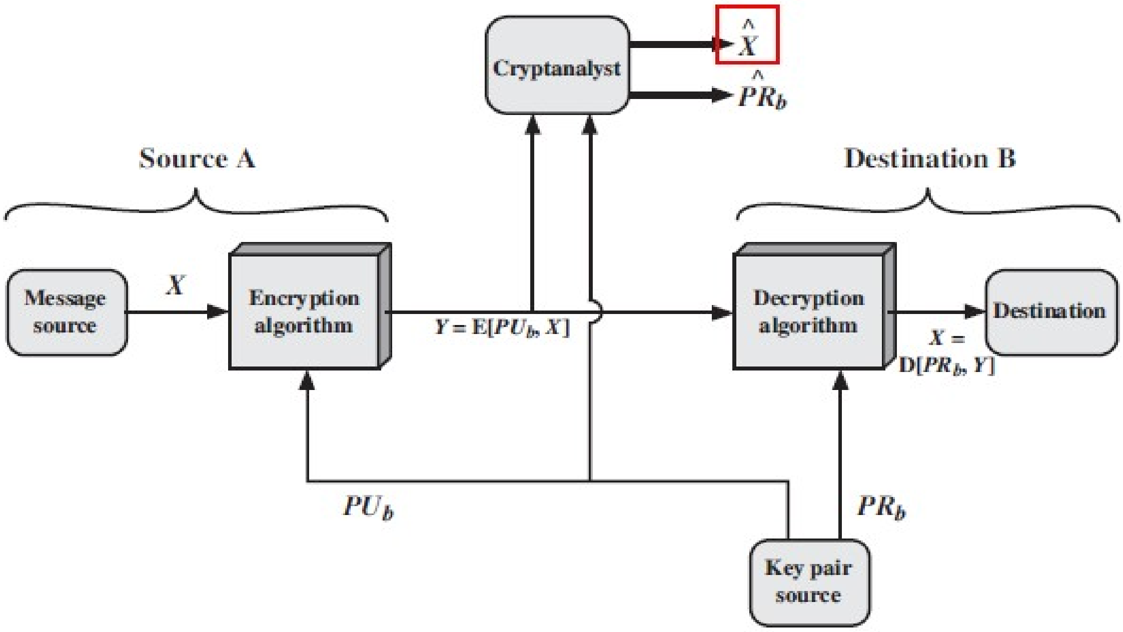
This is followed by a phase consisting of sixteen rounds of the same function, which involves both permutation and substitution functions.The output of the last (sixteenth) round consists of 64 bits that are a function of the input plaintext and the key. The left and right halves of the output are swapped to produce the **preoutput**. Finally, the preoutput is passed through a permutation that is theinverse of the initial permutation function, to produce the 64-bit ciphertext

The right-hand portion of Figure 3.5 shows the way in which the 56-bit key is used. Initially, the key is passed through a permutation function.Then, for each of the sixteen rounds, a subkey (Ki) is produced by the combination of a left circular shift and a permutation. The permutation function is the same for each round, but a different subkey is produced because of the repeated shifts of the key bits.

4.a) Write a brief note on public key cryptosystems-Confidentiality and Authentication 6M

Diagrams---2M Explanation---4M

Public key cryptosystems



Let us take a closer look at the essential elements of a public-key encryption scheme, using Figure. There is some source A that produces a message in plaintext, $X = [X1, X2, . . . ,XM]$. The M elements of X are letters in some finite alphabet. The message is intended for destination B. B generates a related pair of keys: a public key, *PUb*, and a private key, *PRb*. *PRb* is known only to B, whereas *PUb* is publicly available and therefore accessible by A.

With the message X and the encryption key *PUb* as input, A forms the ciphertext $Y = [Y1, Y2, . . . , YN]$:

$$Y = E(PUb, X)$$

The intended receiver, in possession of the matching private key, is able to invert the transformation:

$$X = D(PRb, Y)$$

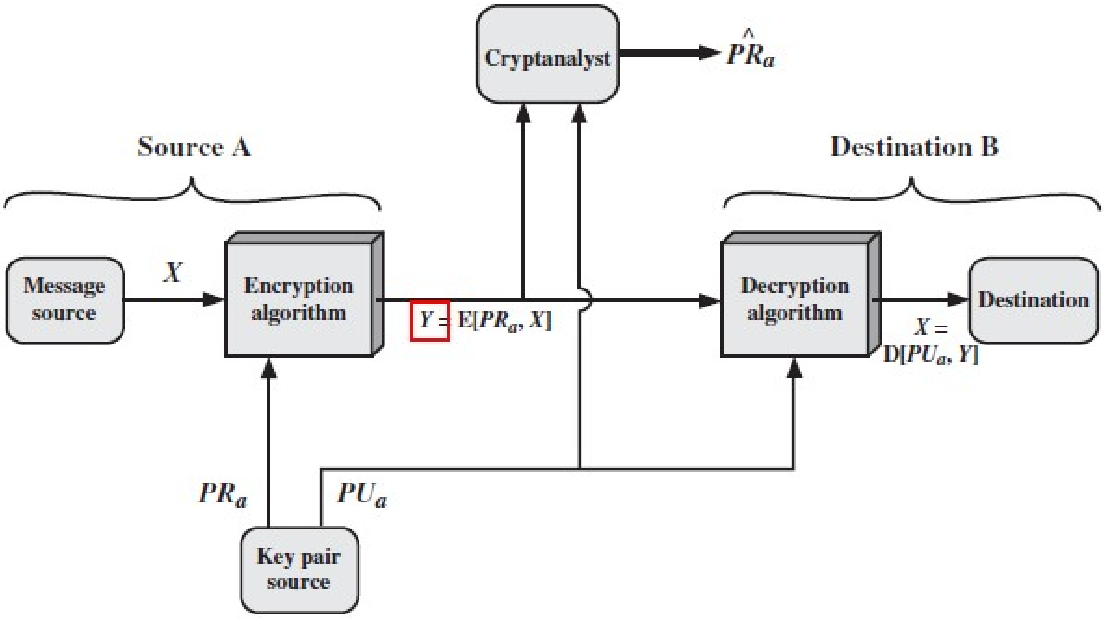
An adversary, observing Y and having access to *PUb*, but not having access to *PRb* or X, must attempt to recover X and/or *PRb*. It is assumed that the adversary does have knowledge of the encryption (E) and decryption (D) algorithms. If the adversary is interested only in this particular message, then the focus of effort is to recover X by generating a plaintext estimate $X\,\hat{}$. Often, however, the adversary is interested in being able to read future messages as well, in which case an attempt is made to recover *PRb* by generating an estimate *PRˆb*.

We mentioned earlier that either of the two related keys can be used for encryption, with the other being used for decryption.This enables a rather different cryptographic scheme to be implemented.

Authentication

$$Y = E(PRa, X)$$
$$X = D(PUa, Y)$$

In this case,A prepares a message to B and encrypts it using A’s private key before transmitting it. B can decrypt the message using A’s public key. Because the message was encrypted using A’s private key, only A could have prepared the message. Therefore, the entire encrypted message serves as a digital signature. In addition, it is impossible to alter the message without access to A's private key, so the message is authenticated both in terms of source and in terms of data integrity.



the entire message is encrypted, which, although validating both author and contents, requires a great deal of storage. Each document must be kept in plaintext to be used for practical purposes.A copy also must be stored in ciphertext so that the origin and contents can be verified in case of adispute. A more efficient way of achieving the same results is to encrypt a small block of bits that is a function of the document. Such a block, called an authenticator, must have the property that it is infeasible to change the document without changing the authenticator. If the authenticator is encrypted with the sender's private key, it serves as a signature that verifies origin, content, and sequencing.

b) Describe the countermeasures to be used against timing attack 4M

Although the timing attack is a serious threat, there are simple countermeasures that can be used, including the following.

• **Constant exponentiation time:** Ensure that all exponentiations take the same amount of time before returning a result.This is a simple fix but does degrade performance.

• **Random delay:** Better performance could be achieved by adding a random delay to the exponentiation algorithm to confuse the timing attack. Kocher points out that if defenders don't add enough noise, attackers could still succeed by collecting additional measurements to compensate for the random delays.

• **Blinding:** Multiply the ciphertext by a random number before performing exponentiation.This process prevents the attacker from knowing what ciphertext bits are being processed inside the computer and therefore prevents thebit-by-bit analysis essential to the timing attack.

5. a) Summarize RSA algorithm 5M

RSA makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n.That is, the block size must be less than or equal to log2(n) + 1; in practice, the block size is i bits, where $2i\ 6\ n \leq 2i+1$. Encryption and decryption are of the following form, for some plaintext block M and ciphertext block C.

$$C = Me \; mod \; n$$

$$M = Cd \bmod n = 1Me2d \bmod n = Med \bmod n$$

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of $PU = \{e, n\}$ and a private key of $PR = \{d, n\}$.

For this algorithm to be satisfactory for public-key encryption, the following requirements must be met.

1. It is possible to find values of e, d, n such that $Med \bmod n = M$ for all $M < n$.

2. It is relatively easy to calculate $Me \bmod n$ and $Cd \bmod n$ for all values of $M < n$.

3. It is infeasible to determine d given e and n.

For now, we focus on the first requirement and consider the other questions later.We need to find a relationship of the form $Med \bmod n = M$

The preceding relationship holds if e and d are multiplicative inverses modulo φ(n), where φ(n) is the Euler totient function. It is shown in Chapter 8 that for p, q prime, $\varphi\ (pq) = (p - 1)(q - 1)$. The relationship between e and d can be expressed as

$$ed \bmod \varphi(n) = 1$$

That is, e and d are multiplicative inverses mod f(n). Note that, according to the rules of modular arithmetic, this is true only if d (and therefore e) is relatively prime to f(n). Equivalently, gcd(f(n), d) = 1. See Appendix 9A for a proof that Equation satisfies the requirement for RSA.

We are now ready to state the RSA scheme.The ingredients are the following:

p, q, two prime numbers (private, chosen)
$n = pq$ (public, calculated)
e, with gcd(f(n), e) = 1; $1 < e <$ f(n) (public, chosen)
d K e-1 (mod f(n)) (private, calculated)

The private key consists of $\{d, n\}$ and the public key consists of $\{e, n\}$. Suppose that user A has published its public key and that user B wishes to send the message M to A.Then B calculates $C = Me \bmod n$ and transmits C. On receipt of this ciphertext, user A decrypts by calculating $M = Cd \bmod n$.

b) Perform Encryption and decryption using RSA algorithm P=3,Q=7,e=5 and M=10 5M

Key Generation:

P=3, Q=7
Calculate n=P*Q=3*7=21
n=21
Calculate Ø(n)=(p-1)(q-1)
=2*6
Ø(n) =12
Given e=5
Calculate $d=e^{-1}$(mod Ø(n))
$=5^{-1}$(mod(Ø(n))
d=5
Public key **PU= {5,21}**
Private key **PR= {5,21}**
Encryption: M<N
Given M=10
Cipher text $C=10^5$ mod21
C=19
Decryption: C=19
Plain text $M=19^5$ mod21
M=10
As we got the encryption and decryption same result hence the RSA algorithm is successfully executed.

6.a) Describe various phases of Hacking? 5M

Each phase ---1M

Reconnaissance

- Reconnaissance refers to the preparatory phase where an attacker seeks to gather information about a target prior to launching an attack.
- Reconnaissance target range may include the target organization's clients, employees, operations, network, and systems.

Reconnaissance Types:

Passive Reconnaissance:

- Passive Reconnaissance involves acquiring information without directly interacting with the target.
- For example, searching public records or news releases.

Active Reconnaissance:

- Active Reconnaissance involves interacting with the target directly by any means.
- For example, telephone calls to the help desk or technical department.

Scanning

- ✓ **Pre-Attacks Phase**: Scanning refers to the pre-attack phase when the attacker scans the network for specific information on the basis of information gathered during reconnaissance.
- ✓ **Port Scanner:** Scanning can include use of dialers, port scanners, network mappers, ping tools, vulnerability scanners, etc.
- ✓ **Extract Information:** Attackers extract information such as live machines, port, port status, OS details, device type, system uptime, etc. to launch attack.

Gaining Access

- ✓ Gaining access refers to the point where the attacker obtains access to the operating system or applications on the computer or network.
- ✓ The attacker can gain access at operating system level, application level, or network level.
- ✓ Examples include password cracking, buffer overflows, denial of service, session hijacking, etc.

Maintaining Access

- ✓ Maintaining access refers to the phase when the attacker tries to retain his or her ownership of the system.
- ✓ Attackers may prevent the system from being owned by other attackers by securing their exclusive access with Backdoors, RootKits, or Trojans.

Clearing Tracks

- ✓ Covering tracks refers to the activities carried out by an attacker to hide malicious acts.
- ✓ The attacker's intentions include: Continuing access to the victim's system, remaining unnoticed and uncaught, deleting evidence that might lead to his prosecution.

b) What are the roles of an Ethical Hacker? Give examples 5M

Role of an Ethical Hacker

- ❖ Ethical hackers are technical professionals and have immense knowledge of system and security. They attack their own organisational system with permission and try to find ways through which their system can be attacked. Ethical hackers are very important for organisations from security and safety purpose.

- ❖ In-depth Knowledge of Security: Ethical hackers should be well versed with potential threats and vulnerabilities that can hack organisational systems. Ethical hackers are hired by organisations for their expertise skills and quick resolution to security vulnerabilities. They should be cyber security professionals having knowledge of the computer systems, network and security.

- ❖ Think like Hackers: The primary role of Ethical hackers is to attack the system like hackers, without adopting authorised methods. They are supposed to think like hackers who want to steal confidential data /information. Ethical hackers look for areas that are most likely to be attacked and the different ways in which attack can take place.

- ❖ In-depth Knowledge of the Organisation they intend to provide Service: Ethical hackers should be well versed with the services of the functional working of the organisation they are associated with. It should have the knowledge about the information that is extremely safe and needs to be protected. Ethical hackers should be capable of finding the attack methods for accessing the sensitive content of the organisation.

➢ **Skill Required to be an Ethical Hacker:**

✓ Knowledge about Networking

✓ Expert in Scripting

✓ Good hands-on programming

✓ Exposure to multiple operating systems: Windows, Linux

✓ Knowledge of the backend database

✓ Experience with servers and search engines Well-versed with available tools in market

7.a) What are the principles of Privacy and why web security is important? 5M

<u>Principles of Privacy---2M Web Security---3M</u>

Principles of Privacy

- **Collection limitation.** Data should be obtained lawfully and fairly.
- **Data quality.** Data should be relevant to their purposes, accurate, complete, and up to date.
- **Purpose specification.** The purposes for which data will be used should be identified and the data destroyed if no longer necessary to serve that purpose.
- **Use limitation.** Use for purposes other than those specified is authorized only with consent of the data subject or by authority of law.
- **Security safeguards**. Procedures to guard against loss, corruption, destruction, or misuse of data should be established.
- **Openness.** It should be possible to acquire information about the collection, storage, and use of personal data systems.
- **Individual participation**. The data subjects normally have a right to access and to challenge data relating to them.
- **Accountability.** A data controller should be designated and accountable for complying with the measures to effect the principles.

Web Security

The Internet is sometimes viewed as the greatest threat to privacy an advantage of the Internet, which is also a disadvantage, is anonymity. A user can visit websites, send messages, and interact with applications without revealing an identity. At least that is what we would like to think. Unfortunately, because of things like cookies, adware, spybots, and malicious code, the anonymity is superficial and largely one-sided.

Sophisticated web applications can know a lot about a user, but the user knows relatively little about the application.

The topic is clearly of great interest: a recent Google search returned over 7 billion hits for the terms “web” and “privacy” together, and 634,000 hits for the phrase “web privacy.”

In this section we investigate some of the ways a user’s privacy is lost on the Internet.

Understanding the Online Environment

The Internet is like a big, unregulated bazaar. Every word you speak can be heard by many others. And the merchants' tents are not what they seem: the spice merchant actually runs a gambling den, and the kind woman selling scarves is really three pirate brothers and a tiger. You reach into your pocket for money only to find that your wallet has been emptied. Then the police tell you that they would love to help but, sadly, no laws apply.

Payments on the Web

Customers of online merchants must be able to pay online for purchases. There are two basic approaches: Customers give their credit card information to the merchant or they arrange payment through an online payment system such as PayPal.

Third-Party Ads

You visit the Yahoo! Sports web page or app, and you might see advertisements for mortgages, banking, auto loans, and sports magazines, a cable television offer, and a discount coupon for a fast food chain. You click one of the links, and you either go directly to a "buy here now" form or you get a special coupon worth something on your purchase in person. Web advertising is much more connected to the vendor: You see the ad, you click on it, and both the purchaser and web page owner know the ad did its job by attracting your attention.

b) Relate the impact of privacy on Emerging Technologies. 5M

We look at the privacy implications of several emerging technologies. Nothing inherent in the technologies affects privacy, but their applications have risk. The first is a broadcast technology that can be used for tracking objects or people. Second is a group of technologies to facilitate elections. The third technology involves the changing methods for providing voice-grade telephone calls.

Radio frequency identification (**RFID**) is a technology that uses small, low-power wireless radio transmitters called **RFID tags**. The devices can be as small as a grain of sand and can cost less than a penny apiece. Tags are tuned to a particular frequency and each has a unique ID number. When a tag receives its signal from a remote product, it sends its ID number signal in response. Many tags have no power supply of their own and receive the power to send a signal from the very act of receiving a signal. Thus, these devices can be passive until they receive a signal from an interrogating reader.

Some tags can be surgically implanted under the skin of humans or animals. Others can be embedded in a credit card or identity badge, and others can be placed in a shipping or inventory label. The distance at which they can receive and broadcast a receivable signal varies from roughly five centimeters (the least powerful) to several meters (the most powerful). Some transmitters have their own power supply (usually a battery, but it can be a solar collector or other associated device) and can transmit over an even greater distance.

Electronic Voting

Voting is another area in which privacy is important. We want votes to be private, but at the same time we want a way to demonstrate that all collected votes are authentic. With careful control of paper ballots, we can largely satisfy both those requirements, but the efficiency of such systems is poor. We would like to use computerized voting systems to improve efficiency without sacrificing privacy or accuracy.

VoIP and Skype

Privacy aspects of traditional telephony were fairly well understood: Telephone companies were regulated monopolies that needed to preserve the confidentiality of their clients' communications. Exceptions occurred under statutorily defined circumstances for law enforcement purposes and in emergencies. Furthermore, the technology was relatively resistant to eavesdropping, with the greatest exposure at the end points.

Conclusions on Emerging Technologies

Technologies continue to emerge and mature, and we have provided only a few examples of great technological promise but considerable privacy risks. Should you be thinking of adopting such technology, be sure to evaluate the privacy implications and then follow them carefully as the technology evolves. Our experience with security has shown that if we consider security early in a system' s life, wider options are available for security. The other thing experience has repeatedly shown is that adding security to a nearly complete system is difficult, if not impossible.

8.a) Write a brief note on Net discover and N-Map tools 6M

Net discover---3M NMap---3M

Net discover

- Net discover is an active/passive address reconnaissance tool, mainly developed for those wireless networks without DHCP server, when you are war driving. It can be also used on hub/switched networks.
- sage: netdiscover [-i device] [-r range | -p] [-s time] [-n node] [-c count] [-f] [-S]

Ex: bt ~ # netdiscover -i ath0 -r 192.168.1.0/24

bt ~ # netdiscover -i ath1 –p (scan common networks)

- -i device: your network device
- -r range: scan a given range instead of auto scan. 192.168.6.0/24,/16,/8
- -p passive mode do not send anything, only sniff
- -s time: time to sleep between each arp request (miliseconds)
- -c count: number of times to send each arp reques (for nets with packet loss)
- -n node: last ip octet used for scanning (from 2 to 253)
- -S enable sleep time supression betwen each request (hardcore mode)
- -f enable fast mode scan, saves a lot of time, recommended for auto
- If -p or -r aren't enabled, netdiscover will scan for common lan addresses

Ok so let's look at the flags so that we know what we are dealing with.
"-i" simply put is the network card

"-r" the range to scan that you will insert on the command later
"-p" send no packets out on the network
"-s" time to sleep between the arp requests simply means how long

netdiscover should wait.
"-c" count is the number or arp requests to send each time
"-n" node again this is a number you will insert on the command latter.
"-S" this will prevent netdiscover from "sleeping" between arp requests"
"-f" fast as stated above

N-Map

- Nmap is a free, open-source port scanner available for both UNIX and Windows. It has an optional graphical front-end, NmapFE, and supports a wide variety of scan types

Basic Scan Types [-sT, -sS]

- **TCP connect() Scan [-sT]**
- **SYN Stealth Scan [-sS]**
- **FIN, Null and Xmas Tree Scans [-sF, -sN, -sX]**

Ex: # nmap -sS 127.0.0.1

- **Ping Scan [-sP]**
- **UDP Scan [-sU]**
- **IP Protocol Scans [-sO]**

Ex: # nmap -sO 127.0.0.1

- **Idle Scanning [-sI]**
- **Version Detection [-sV]**
- **ACK Scan [-sA]**
- **Window Scan, RPC Scan, List Scan [-sW, -sR, -sL]**

b) What are the advantages of Recon-ng tool? 4M

Advantages of Recon-ng tool----4M

Information Gathering is the act of gathering different kinds of information against the targeted victim or system. Information gathering is not just a phase of security testing; it is an art that every penetration-tester (pen-tester) and hacker should master for a better experience in penetration testing.

Any basic cyber security information gathering process often includes these two types of data collection goals:

1. Collecting network data: Such as public, private and associated domain names, network hosts, public and private IP blocks, routing tables, TCP and UDP running services, SSL certificates, open ports and more.

2. Collecting system-related information: This includes user enumeration, system groups, OS hostnames, OS system type (probably by fingerprinting), system banners (as seen in the banner grabbing blog post), etc.

Recon-ng tool

- Recon-ng is a framework. It is a very powerful, flexible, and has moving parts similar to the Metasploit framework. Recon-ng is an interactive framework that is not a menu driven UI. Recon-ng uses many different sources to gather data.
- **Installing recon-ng on Kali Linux**
- We are going to install recon-ng on Kali Linux. To install recon-ng and place it in the opt directory, we are going to use git clone by typing in the following command in the terminal window.
- *cd /opt; git clone https://LaNMaSteR53@bitbucket.org/LaNMaSteR53/recon-ng.git*
- *cd /opt/recon-ng*

./recon-ng

advantages of Recon-ng tool

- Recon-ng is a complete package of Information gathering tools.
- Recon-ng can be used to find IP Addresses of target.
- Recon-ng can be used to look for error based SQL injections.
- Recon-ng can be used to find sensitive files such as robots.txt.
- Recon-ng can be used to find information about Geo-IP lookup, Banner grabbing, DNS lookup, port scanning, sub-domain information, reverse IP using WHOIS lookup .
- Recon-ng can be used to detects Content Management Systems (CMS) in use of a target web application,
- InfoSploit can be used for WHOIS data collection, Geo-IP lookup, Banner grabbing, DNS lookup, port scanning, sub-domain information, reverse IP, and MX records lookup
- Recon-ng is a complete package (TOOL) for information gathering.

9.a) What are the various types of Network Scanning? 4M

<u>Any two can be considered---4M</u>

Network Scanning

- Network scanning refers to a set of procedures for identifying hosts, ports, and services in a network.
- Network scanning is one of the components of intelligence gathering an attacker uses to create a profile of the target organization.

Various types of Network Scanning

- **Checking for Live Systems - ICMP Scanning**
- Ping scan involves sending ICMP ECHO requests to a host. If the host is live, it will return an ICMP ECHO reply.
- This scan is useful for locating active devices or determining if ICMP is passing through a firewall.
- **Ping Sweep**
- Ping sweep is used to determine the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts. If a host is live, it will return an ICMP ECHO reply.
- Attackers calculate subnet masks using Subnet Mask Calculators to identify the number of hosts present in the subnet.
- Attackers then use ping sweep to create an inventory of live systems in the subnet.

SSDP Scanning

- The Simple Service Discovery Protocol (SSDP) is a network protocol that works in conjunction with UPnP to detect plug and play devices available in a network.
- Vulnerabilities in UPnP may allow attackers to launch Buffer overflow or DoS attacks.
- Attacker may use UPnP SSDP M-SEARCH information discovery tool to check if the machine is vulnerable to UPnP exploits or not.
- **Scanning Tool: Nmap**
- Network administrators can use Nmap for network inventory, managing service upgrade schedules, and monitoring host or service uptime.
- Attacker uses Nmap to extract information such as live hosts on the network, services type of packet filters/firewalls, operating systems and
- OS versions.

b) Explain about Password Attacks? 6M

Password Attacks Explanation---6M

Most widely used types of attacks are

- **Password Guessing**
  The most common type of attack is password guessing. Attackers can guess passwords locally or remotely using either a manual or automated approach. Password guessing isn't always as difficult as you'd expect.
- **Password Resetting**
  Attackers often find it much easier to reset passwords than to guess them. Many password cracking programs are actually password resetters.

- **Password sniffing**

  Some password crackers can sniff authentication traffic between a client and server and extract password hashes or enough authentication information to begin the cracking process.

- **PasswordCapturing**
  Many attackers capture passwords simply by installing a keyboard-sniffing Trojan horse or one of the many physical keyboard-logging hardware devices for sale on the internet. Symantec reports that 82 percent of the most commonly used malware programs steal confidential information.

- **Password cracking**

  It is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach (brute-force attack) is to repeatedly try guesses for the password and to check them against an available cryptographic hash of the password. The purpose of password cracking might be to help a user recover a forgotten password (installing an entirely new password is less of a security risk, but it involves System Administration privileges), to gain unauthorized access to a system, or to act as a preventive measure whereby system administrators check for easily crackable passwords.

Scheme prepared by Signature of the HOD, IT Dept.

Paper Evaluators:

S.No	**Name Of the College**	**Name of the Faculty**	**Signature**