DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CB3491- CRYPTOGRAPHY AND CYBER SECURITY

UNIT I INTRODUCTION TO SECURITY *Computer Security Concepts – The OSI Security Architecture – Security Attacks – Security Services and Mechanisms – A Model for Network Security – Classical encryption techniques: Substitution techniques, Transposition techniques, Steganography – Foundations of modern cryptography: Perfect security – Information Theory – Product Cryptosystem – Cryptanalysis.*

UNIT-I

1	**What is Security attack, Security mechanism and Security service?** **Security attack:** Any action that compromises the security of information owned by an organization. **Security mechanism:** A mechanism that is designed to detect, present or recover from a security attack. **Security service:** A service that enhances the security of the data processing systems and the information transfer of an organization.
2	**Define confidentiality.** Confidentiality ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties. This type of access includes printing, displaying, and other forms of disclosure.
3	**Define integrity.** Integrity ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing, deleting, creating and delaying or replaying of transmitted messages.
4	**Define Authentication, Nonrepudiation, Availability and Access control.** **Authentication:** Ensures that the origin of a message is correctly identified, with an assurance that the identity is not false. **Nonrepudiation:** Requires that neither the sender nor the receiver of a message be able to deny the transmission. **Availability:** Requires that computer system assets be available to authorized parties when needed. **Access control:** Requires that access to information resource may be controlled by or for the target system.
5	**List 4 general categories of attack.** ✓ Interruption ✓ Interception ✓ Modification ✓ Fabrication
6	**Differentiate between Interruption and Interception.**

Interruption	**Interception**
An asset of the system is destroyed or becomes unavailable or unusable	An authorized party gains access to the asset
This is an attack on availability	This is an attack on confidentiality
E.g.: Destruction of a piece of hardware, the cutting of a communication line, the disabling of the file management system.	E.g.: Wiretapping to capture data in a network, illicit copying of files or programs.

<table>
<tr><td>7</td><td colspan="2">Differentiate between Modification and Fabrication.</td></tr>
<tr><td></td><td>Interruption</td><td>Interception</td></tr>
<tr><td></td><td>An unauthorized party not only gains access to but tampers with an asset</td><td>An unauthorized party inserts counterfeit objects into the system.</td></tr>
<tr><td></td><td>This is an attack on integrity</td><td>This is an attack on authenticity</td></tr>
<tr><td></td><td>E.g.: Changing values in a data file, altering a program so that it performs differently</td><td>E.g.: Insertion or spurious message in a network or the addition of records to a file</td></tr>
<tr><td>8</td><td colspan="2">Compare active and passive attack (Dec 2020)</td></tr>
<tr><td></td><td>Active attack</td><td>Passive attack</td></tr>
<tr><td></td><td>These attacks involve some modification of the data stream or creation of false stream</td><td>They are in the nature of eavesdropping, on or monitoring of transmissions</td></tr>
<tr><td></td><td>The types of active attacks are
✓ Masquerade
✓ Replay
✓ Modification
✓ Messages</td><td>The types of passive attacks are
✓ Release of message contents
✓ Traffic analysis</td></tr>
<tr><td></td><td>It is difficult to prevent active attacks absolutely.</td><td>They are very difficult to detect (because they do not move any alternation to data). But it is feasible to prevent the success of these attacks.</td></tr>
<tr><td>9</td><td colspan="2">List the components involved in network security (i.e. Model for network security)
✓ Message
✓ Two principals (Source and Destination)
✓ Trusted third party
✓ Opponent</td></tr>
<tr><td>10</td><td colspan="2">List the 4 basic tasks in designing a particular security service.
✓ Design an algorithm for performing the security-related Transformation
✓ Generate the secret information to be used with the algorithm
✓ Develop methods for the distribution and sharing of secret information
✓ Specify a protocol to be used by the two principals.</td></tr>
<tr><td>11</td><td colspan="2">List the five main components of a conventional encryption system.
✓ Plaintext
✓ Encryption algorithm.
✓ Ciphertext
✓ Decryption algorithm</td></tr>
<tr><td>12</td><td colspan="2">Define Plaintext, Ciphertext
Plaintext: Refers to the original message that is created and sent into encryption method.
Ciphertext: It is the text that is now scrambled and ready to send. It may look like a random stream of data, and is unreadable.</td></tr>
</table>

<table>
<tr><td>13</td><td>How cryptographic systems are generally classified?
Cryptographic systems are generally classified along 3 independent dimensions.
✓ The type of operations used for transforming plaintext into ciphertext (permutation/substitution)
✓ The number of keys used (single key/different key)
✓ The way in which the plaintext is processed (Block cipher/Stream cipher)</td></tr>
<tr><td>14</td><td>Differentiate block cipher and stream cipher.
Block cipher: A block cipher processes the input one block of elements at a time, producing an output block for each input block.
Stream cipher: A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along</td></tr>
<tr><td>15</td><td>What do you mean by substitutional technique?
A substitutional technique is one in which the letters of the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.</td></tr>
<tr><td>16</td><td>List some substitution techniques
✓ Caesar Cipher
✓ Monoalphabetic Ciphers
✓ Playfair Ciphers
✓ Hill Cipher
✓ Polyalphabetic Ciphers</td></tr>
<tr><td>17</td><td>What is the difference between Monoalphabetic and polyalphabetic cipher? (Dec 2021)
<table>
<tr><th>Monoalphabetic Cipher (MAC)</th><th>Polyalphabetic Cipher (PAC)</th></tr>
<tr><td>A MAC is one where each symbol in the input is mapped to a fixed symbol in the output</td><td>A PAC is any cipher based on substitution using multiple substitution alphabets</td></tr>
<tr><td>In MAC, once a key is chosen, each alphabetic character of plain text is mapped onto a unique alphabetic character of a ciphertext.</td><td>In PAC, each alphabetic character of plaintext can be mapped onto „m“ alphabetic characters of ciphertext.</td></tr>
<tr><td>In MAC, the relationship between a character in the plaintext and the characters in the ciphertext is one-to-one.</td><td>In PAC, the relationship between a character in the plaintext and the characters in ciphertext is one-to-many</td></tr>
</table></td></tr>
<tr><td>18</td><td>List out the problems of one-time pad.
✓ Distribution of the key was a challenge.
✓ Adding numbers to the plaintext manually is a time-consuming task. It is therefore sometimes thought that OTPs are no longer considered practical</td></tr>
<tr><td>19</td><td>List the various other techniques used historically for steganography.
✓ Character marking
✓ Invisible ink
✓ Pin purchases
✓ Typewriter correction ribbon</td></tr>
</table>

20	**Calculate the ciphertext for the following using one-time pad cipher.** Plaintext: R O C K Keyword: B O T S Plaintext R O C K 17(R) 14(O) 2(C) 10(K) Key 1(B) 14(O) 19(T) 18(S) Plaintext+key 18 28 21 28 Plaintext+key 18 2 21 2 mov 26 Plaintext+key S C V C
21	**What are transposition techniques?** (Different kind of) Mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as transposition cipher Ex. Rail fence technique.
22	**What is steganography?** Steganography is the practice of concealing a file, message, image or video within another file, message, image or video. i.e. It is hiding a secret message within an ordinary message and the extraction of it at its destination.
23	**Explain the working mechanism of one-time pad.** ✓ The encryption key has at least the same length as the plaintext and consists of truly random numbers ✓ Each letter of the plaintext is mixed with one element from the OTP. ✓ This results in a ciphertext that has no relation with plaintext when the key is unknown. At the receiving end, the same OTP is used to retrieve the original plaintext.
24	**Compare steganography and cryptography.** ✓ The meaning of steganography is covered or hidden writing while cryptography signifies secret writing. ✓ Steganography is an attempt to achieve secure and undictable communication. Cryptography intends to make the message readable for only the target recipient and not by others. ✓ In steganography, the main structure of the message is not changed whereas cryptography imposes a change on the secret message before transferring it over the network. ✓ The steganography can be employed on text, and in video and image while cryptography is implemented only on the text file.
25	**What is threat? List their types.** A threat is a possible security violation that might exploit the vulnerability of a system or asset. The origin of threat may be accidental, environmental, human negligence or failure. Different types of security threats are interruption, interception, fabrication and modification.

<table>
<tr><td>26</td><td>Connect the given text “anna university” into cipher text using Rail fence technique.
Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
a n u i e s t
n a n v r i y
The encrypted message is anuiestnanvriy.</td></tr>
<tr><td>27</td><td>Differentiate between threats and attacks
✓ A threat is a possible security violation that might exploit the vulnerability of a system or asset. The origin of threat may be accidental, environmental, human negligence or failure. Different types of security threats are interruption, interception, fabrication and modification.
✓ Attack is a deliberate unauthorized action on a system or asset. Attack can be classified as active and passive attack. An attack will have a motive and will follow a method when opportunity arise.</td></tr>
<tr><td>28</td><td>Encrypt the plaintext tobeornottobe using the vigenere cipher for the key value Now. (Dec 2020).
The encryption of the original text is done using the vigenere table. The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers. At different points in the encryption process, the cipher uses a different alphabet from one of the rows. The alphabet used at each point depends on a repeating keyword.
plaintext tobeornottobe
key value Now
Transformed text hdysdobdqhdys</td></tr>
<tr><td>29</td><td>How substitution cipher is different from transposition cipher. Give example for each method (Dec 2021)
<table>
<tr><th>Substitution cipher</th><th>Transposition cipher</th></tr>
<tr><td>A substitution technique is one in which the letters of plain text are replaced by other letters or number or symbols.</td><td>Transposition cipher does not substitute one symbol for another instead it changes the location of the symbols</td></tr>
<tr><td>Monoalphabetic and Polyalphabetic substitution cipher.</td><td>Keyless and Keyed transportation cipher.</td></tr>
<tr><td>Each letter retains its position changes its identity</td><td>Each letter retains its identity but changes its position</td></tr>
<tr><td>Example: Ceaser Cipher, Hill cipher, Vigenere cipher</td><td>Example: Rail fence Cipher,</td></tr>
</table></td></tr>
</table>

30	**Give an example each for substitution and transposition ciphers** **Substitution Cipher:** (Replace the plaintext characters with other characters, numbers and equal) ✓ Caesar cipher ✓ Hill cipher ✓ Vigenere cipher **Transposition cipher:** (Rearranges the position of the characters of the plaintext) ✓ Rail fence cipher
UNIT-I / PART-B	
1	***(i)*** Explain OSI security architecture model with neat diagram (***Dec 2020, Dec 2021)*** ***(ii)*** Describe the various security mechanism ***(Dec 2020)***
2	Encrypt the following using play fair cipher using the keyword MONARCHY. "SWARAJ IS MY BIRTH RIGHT". Use X for blank spaces.
3	Describe (i) Playfair Cipher (ii) Rail fence Cipher (iii) Vignere Cipher
4	Perform encryption and decryption using Hill cipher for the following: Message PEN and key ACTIVATED ***(Dec 2021)***
5	What is steganography? Describe the various techniques used in steganography
6	What is monoalphabetic cipher? Examine how it differs from Caesar cipher (7)***(Dec 2020)*** ii) Encrypt the message "this is an exercise" using additive cipher with key = 20. Ignore the space between words. Decrypt the message to get the original plaintext. (6)
7	Explain the network security model and its important parameters with a neat block diagram
8	Solve using Playfair cipher method. Encrypt the word "Semester Result" with the keyword "Examination". Discuss the rules to be followed
9	Explain the ceaser cipher and monoalphabetic cipher.
10	Write note on different types of security attacks and services in detail
11	Explain the substitution encryption technique in detail
12	Discuss examples from real life, where the following security objectives are needed : i) Confidentiality. (5) ii) Integrity. (5) iii) Non-repudiation. (5) Suggest suitable security mechanisms to achieve them. ***(Dec 2020, Dec 2021)***
13	Discuss the rules to be followed in Playfair method. Encrypt the word"Networksecurity" with the keyword "cypto" using Playfair method. (***Dec 2021)***
UNIT II - SYMMETRIC CIPHERS ***MATHEMATICS OF SYMMETRIC KEY CRYPTOGRAPHY: Algebraic structures – Modular arithmetic-Euclid's algorithm- Congruence and matrices – Groups, Rings, Fields- Finite fields- SYMMETRIC KEY CIPHERS: SDES – Block cipher Principles of DES – Strength of DES – Differential and linear cryptanalysis – Block cipher design principles – Block cipher mode of operation – Evaluation criteria for AES – Advanced Encryption Standard – RC4 – Key distribution.***	

UNIT-II / PART-A

1 **What is symmetric key encryption?**

Symmetric key encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process.

2 **List the 5 main components of a symmetric encryption system.**

- ✓ Plaintext
- ✓ Encryption algorithm
- ✓ Secret key
- ✓ Ciphertext
- ✓ Decryption algorithm

3 **Give the 5 modes of operations of block cipher. (*Dec 2020)***

- ✓ Electronic codebook (ECB)
- ✓ Cipher block chaining (CBC)
- ✓ Cipher feedback (CFB)
- ✓ Output feedback (OFB)
- ✓ Counter (CTR)

4 **List the parameters for the 3 AES version**

Parameters	AES-128	AES-192	AES-256
Plaintext block size (bits)	128	128	128
Key size (bits)	128	192	256
Number of rounds	10	12	14

5 **Compare DES and AES**

Parameters	DES	AES
Developed	1977	2002
Key length	56 bits	128,192 or 256 bits
Cipher type	Symmetric block cipher	Symmetric block cipher
Block type	64 bits	128 bits
Security	Proven inadequate	Considered secure

6 **Brief the strengths of triple DES**

Triple DES is based on the DES algorithm, therefore it is very easy to modify existing software to use triple DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the attacks (i.e. Triple DES systems are significantly more secure than single DES)

7 **Determine the GCD of (24140,16762) using Euclid‟s algorithm**

GCD (24140, 16762) = GCD (16762, 7378)
= GCD (7378, 2006)
= GCD (2006, 1360)
= GCD (1360, 646)
= GCD (646, 68)
= GCD (68, 34) = GCD (34,0) = 34

8	**Determine the GCD of (1970,1066) using Euclid"s algorithm** GCD (1970,1066) = GCD (1066,904) = GCD (904, 162) = GCD (162, 94) = GCD (94, 68) = GCD (68, 26) = GCD (26, 16) = GCD (16,10) = GCD (10,6) = GCD (6,4) = GCD (4,2) = GCD (2,0)=2
9	**Define finite field?** A field (F, +, .) is called a finite field if the set F is finite. A field is a ring in which the multiplication operation is commutative, has no zero divisors, and includes an identity element and an inverse element.
10	**Define field and ring in number theory** ***(Dec 2020)*** A ring is a set of elements that is closed under two binary operations, addition and multiplication, with the following: the addition operation is a group that is commutative; the multiplication operation is associative and is distributive over the addition operation. A field is a ring in which the multiplication operation is commutative, has no zero divisors, and includes an identity element and an inverse element.
11	**What is the disadvantage of double DES?** Double DES is an encryption technique which uses two instances of DES on same plaintext. In both instances it uses different keys to encrypt the plain text. Both keys are required at the time of decryption. The 64-bit plaintext goes into first DES which then converts into a 64-bit middle text using the first key and then it goes to second DES instance which gives 64-bit cipher text by using second key. However double DES uses 112 bits key but gives security level of 256 not 2112 and this is because of meet-in-the middle attack which can be used to break through double DES.
12	**What is avalanche effect?** Avalanche effect is considered as one of the desirable properties of any encryption algorithm. A slight change in either the key or the plain-text should result in a significant change in the ciphertext. This property is termed as avalanche effect.
13	**Write notes on RC4.** ✓ RC4 is a stream cipher ✓ Designed by Ron Rivest for RSA security ✓ Variable key size stream cipher with byte orientated operations ✓ Algorithm is based on the use of random permutation ✓ RC4 is used in the SSL/TLS standards. Also used in WEP protocol and WPA protocol

14	**Does the set of residue classes (mod 3) form a group?** ✓ w.r.t modular addition ✓ w.r.t modular multiplication Modular addition: + 0 1 2 0 0 1 2 1 1 2 0 2 2 0 1 Identity element is 0 and inverses of 0,1,2 are 0,2,1 respectively. So, w.r.t modular addition it forms a group. Modular multiplication: × 0 1 2 0 0 0 0 1 0 1 2 2 0 2 1 Identity element is 1, but 0 has no inverse. So, w.r.t modular multiplication it does not form a group.
15	**Define confusion and diffusion** ✓ Confusion refers to making the relationship between the key and the cipher text as complex and involved as possible ✓ Diffusion refers to the property that redundancy in the statistics of the plaintext is dissipated in the statistics of plaintext.
16	**Write down the purposes of the S-box in DES** In the DES, the substitution consists of a set of 8 S-boxes, each of which accepts 6 bits as input and produces 4 bits as outputs. The first and last bits of the input to box S_i from a 2 bit binary number to select one of four substitutions defined by the 4 rows on the table S_i. The middle 4 bits selects a particular column. Ex: For input $\overset{-}{0}11001\overset{-}{0}$ (the row is 01 & column is 1100 i.e. column 12)
17	**List the properties of congruences** Congruences have the following properties. ✓ $a \equiv b \pmod n$ if $n/(a-b)$ ✓ $a \equiv b \pmod n$ implies $b \equiv a \pmod n$ ✓ $a \equiv b \pmod n$ and $b \equiv c \pmod n$ imply $a \equiv c \pmod n$
18	**List the properties of modular arithmetic.** Modular arithmetic exhibits the following properties ✓ $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$ ✓ $[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$ ✓ $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

19	**Define group** A group G, denoted by (G .) is the set of elements with a binary operation denoted by . that associates to each ordered pair (a,b) of elements in G an element (a.b) in G, such that the following axioms are obeyed ✓ **Closure:** If a and b belong to G then a.b is also in G. ✓ **Associative:** (a.b).c = a.(b.c) for all a,b,c in G ✓ **Identity element:** There is an element e in G such that a.e=e.a=a for a in all G ✓ **Inverse element:** For each a in G, there is an element a^1 in G such that $a.a^1=a^1.a=a=e$
20	**Define Finite and Infinite group** If a group has a finite number of elements, it is referred as a finite group. Otherwise, the group is an infinite group
21	**Define Abelian group** A group is said to be abelian if it satisfies the fell-condition ✓ **Closure:** If a and b belong to G then a.b is also in G. ✓ **Associative:** (a.b).c = a.(b.c) for all a,b,c in G ✓ **Identity element:** There is an element e in G such that a.e=e.a=a for a in all G ✓ **Inverse element:** For each a in G, there is an element a^1 in G such that $a.a^1=a^1.a=a=e$ ✓ **Commutative:** a.b = b.a for all a,b in G
22	**Define cyclic group** A group G is cyclic if every element of G is a power ak(k is an integer) of a fixed element $a \in G$. The element a is said to generate the group G as to be a generation of G. A cyclic group is always abelian and may be finite or infinite.
23	**List the 4 different stages of AES.** ✓ Substitute bytes ✓ Shift rows ✓ Mix column ✓ Add round key
24	**Why modular arithmetic has been used in cryptography?** One of the major reasons is that modular arithmetic allows us to easily create groups, rings and fields which are fundamental building blocks of most modern public key crypto systems. For example, Diffie-Hellman uses the multiplicative group of integers modulo a prime p.
25	**List the uses of RC4 (or) List the applications of RC4.** ✓ RC4 is known for being simple and quick ✓ RC4 is used in the SSL/TLS standards that have been defined for communication between web browsers and servers ✓ It is used in WEP &WPA protocols that are part of IEEE 802.11 WLAN standards

<table>
<tr><td>26</td><td colspan="2">Why random numbers are use in network security?
Random numbers used to generate keys
✓ Symmetric keys
✓ RSA: Prime numbers
✓ Diffie-Hellman secret values
Random numbers used for nonce
✓ Sometimes a sequence is okay
✓ But sometimes nonce must be random
Random numbers also used in
✓ simulations, statistics, etc. where numbers only need to be statistically random</td></tr>
<tr><td>27</td><td colspan="2">What is the disadvantage of ECB mode of operation?
The disadvantage of this method is a lack of diffusion. Because ECB encrypts identical plaintext blocks into identical ciphertext blocks, it does not wide patterns well.</td></tr>
<tr><td>28</td><td colspan="2">What is the difference between a block cipher and a stream cipher? (Dec 2021)</td></tr>
<tr><td></td><td>Block cipher</td><td>Stream cipher</td></tr>
<tr><td></td><td>A block cipher processes the input one block of elements at a time, producing an output block for each input block.</td><td>A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along</td></tr>
<tr><td>29</td><td colspan="2">What is the difference between diffusion and confusion? (Dec 2021)</td></tr>
<tr><td></td><td>Diffusion</td><td>Confusion</td></tr>
<tr><td></td><td>Diffusion is used to create cryptic plain texts.</td><td>Confusion is a cryptographic technique which is used to create faint cipher texts.</td></tr>
<tr><td></td><td>It is possible through transportation algorithm.</td><td>This technique is possible through substitution algorithm.</td></tr>
<tr><td></td><td>In diffusion, if one image within the plain text is modified, many or all image within the cipher text also will be modified</td><td>In confusion, if one bit within the secret‟s modified, most or all bits within the cipher text also will be modified.</td></tr>
<tr><td></td><td>The relation between the cipher text and the plain text is masked by diffusion.</td><td>The relation between the cipher text and the key is masked by confusion.</td></tr>
<tr><td></td><td>Only block cipher uses diffusion.</td><td>Both stream cipher and block cipher uses confusion.</td></tr>
<tr><td colspan="3">UNIT-II / PART-B</td></tr>
<tr><td>1</td><td colspan="2">Explain AES algorithm with all its round functions in detail</td></tr>
<tr><td>2</td><td colspan="2">Discuss the properties that are to be satisfied by groups, rings and fields</td></tr>
<tr><td>3</td><td colspan="2">(ii) Demonstrate that the set of polynomials whose coefficients forms a field is a ring. (5)
For each of the following elements of DES, indicate the comparable element in AES if available
✓ XOR of subkey material with the input to the function (4)
✓ f function (4) (Dec 2020)</td></tr>
<tr><td>4</td><td colspan="2">Describe DES algorithm with neat diagram and explain the steps. (Dec 2021)</td></tr>
<tr><td>5</td><td colspan="2">Solve GCD (98,56) using extended Euclidean algorithm. Also, write the algorithm</td></tr>
<tr><td>6</td><td colspan="2">What do you mean by AES? Diagrammatically illustrate the structure of AES and describe the steps in AES encryption process with example (Dec 2020)</td></tr>
<tr><td>7</td><td colspan="2">Describe in detail the key generation in AES algorithm and its expansion format</td></tr>
</table>

8	Describe Triple DES and its applications
9	Explain about the single round of DES algorithm
10	Describe key discarding process of DES
11	Explain the key generation, encryption and decryption of SDES algorithm in detail *(Dec 11)*
12	Write notes on birthday attack
13	Describe the working principle of simple DES with an example
14	Explain in detail about the entities in the symmetric cipher model with their requirements for secure usage of the model
15	Demonstrate that the set of polynomials where coefficients form a field is a ring
16	Write detailed note on modular arithmetic
17	Explain the following in detail ✓ Linear cryptanalysis ✓ Differential cryptanalysis ✓ Key distribution
18	Explain about RC4 algorithm with neat diagram? ***(Dec 2021)***
19	Describe LFSR sequences and finite field with their application in cryptography

UNIT III – PUBLIC KEY CRYPTOGRAPHY

MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY: Primes – Primality Testing – Factorization – Euler's totient function, Fermat's and Euler's Theorem – Chinese Remainder Theorem – Exponentiation and logarithm – ASYMMETRIC KEY CIPHERS: RSA cryptosystem – Key distribution – Key management – Diffie Hellman key exchange –Elliptic curve arithmetic-Elliptic curve cryptography.

UNIT-III/ PART-A

1	**What is public key cryptography?** Public key cryptography (or asymmetric cryptography) is an encryption scheme that uses two mathematically related, but not identical keys – a public key and a private key. Each key performs a unique function. The public key is used to encrypt and the private key is used to decrypt.
2	**What is the difference between symmetric key cryptography and public key cryptography?**

Symmetric Key Cryptography	Public Key Cryptography
Involves only one key (a secret key) to encrypt and decrypt the information	Uses a pair of keys – a public key and a private key
Speed of encryption (decryption is very fast)	Slow
Both parties should know the key	Only (public key) either one of the keys is known by the two parties
E.g.: DES, AES	E.g.: RSA, ECC

3	**Consider the RSA encryption method with $p=11$ and $q=17$ as the two primes. Find n and $\varphi(n)$.** 1) $p=11$ and $q=17$, so $n = pq = 17\times11 = 187$ 2) $\varphi(n) = (p-1)(q-1) = 16\times10 = 160$

4	**Define primitive root** A primitive root of a prime number p is one whose power modulo 0 p generate all the integers from 1 to p-1. That is if a is a primitive root of the prime number p, then the numbers a mod p, a^2 mod p,……, a^{p-1} mod p are distinct and consists of the integers from 1 through p-1 in some presentation.
5	**State Fermat‟s theorem** Fermat‟s theorem states the following: If p is prime and a is a positive integer not divisible by p, then $a^{p-1} \equiv 1 (\text{mod } p)$
6	**Check whether** **1) 2 is a primitive root of mod 5 &** **2) 4 is a primitive root of mod 5** 1) $21 \bmod 5 = 2 \bmod 5 = 2$ $22 \bmod 5 = 4 \bmod 5 = 4$ $23 \bmod 5 = 8 \bmod 5 = 3$ $2^4 \bmod 5 = 16 \bmod 5 = 1$ So, 2 is primitive root of mod 5 2) $4^1 \bmod 5 = 4 \bmod 5 = 4$ $4^2 \bmod 5 = 16 \bmod 5 = 1$ $4^3 \bmod 5 = 64 \bmod 5 = 4$ $4^4 \bmod 5 = 256 \bmod 5 = 0$ So, 4 is not a primitive root of mod 5
7	**Name any 2 methods for testing prime numbers.** ✓ Miller – Rabin test ✓ Fermat primality test ✓ Solovay – Strassen primality test ✓ Frobenius primality test
8	**Define Euler‟s totient function.** Euler‟s totient function, written $\varphi(n)$, and defined as the number if positive integers less than n and relatively prime to n. By convention $\varphi(1) = 1$
9	**State Euler‟s theorem.** Euler‟s theorem states that for energy a and n that are relatively prime: $a^{\varphi(n)} \equiv 1 (\text{mod } n)$

10	**Determine $\varphi(37)$ and $\varphi(35)$** To determine $\varphi(37)$: Because 37 is prime, all the positive integers from 1 through 36 are relatively prime to 37. So, $\varphi(37) = 36$. To determine $\varphi(35)$:List all the positive integers less than 35 that are relatively prime to it. (i.e) 1,2,3,4,6,8,9,11,12,13,16,17,18,19,22,23,24,26,27,29,31,32,33,34. There are 24 numbers on the list. So, $\varphi(35) = 24$
11	**State alternative form of Fermat"s theorem with example.** The alternative form of Fermat"s theorem: If p is prime and a is a positive integer than $a^p \equiv a(\text{mod } p)$
12	**List the 6 ingredients of public key encryption.** ✓ Plaintext ✓ Encryption algorithm ✓ Public key ✓ Private key ✓ Cipher text ✓ Decryption algorithm
13	**Perform encryption for the plaintext M=88 using the RSA algorithm. P=17, q=11 and public component e=7** i. p=17, q=11 ii. Calculate n=p*q = 17*11 =187 iii. Calculate $\varphi(n)$ = (p-1)(q-1) = 16*10=160 iv. Select e=7 v. Determine d such that de $\equiv$ 1(mod 60). The correct value of d is 23 Public key (7,187) and private key (23,187) Encryption: 88^7 mod 187 = 11
14	**Perform encryption and decryption using the RSA algorithm for the following. P=7, q=11, e=17 and M=8** i. p=7, q=11 ii. Calculate n=p*q = 7*11 =77 iii. Calculate $\varphi(n)$ = (p-1)(q-1) = 6*10=60 iv. Select e=17 v. Determine d such that de $\equiv$ 1(mod 60). The correct value of d is 53 Public key (17,77) and private key (53,77) Encryption: 8^{17} mod 77 = 56 Decryption: 56^{53} mod 77 = 8
15	**List the 5 possible approaches to attacking the RSA algorithm** ✓ Brute force ✓ Mathematical attacks ✓ Timing attacks ✓ Hardware fault-based attack ✓ Chosen ciphertext attacks

16	**Define discrete logarithm** For any integers b and a primitive r not a of prime number p, we can find a unique exponent I such that $b \equiv a^i \pmod p$ where $0 \le I \le (p-1)$ The exponent I is referred to as the discrete logarithm of b for the base a, mod p.
17	**What is the principal attraction of ECC, compared to RSA?** ***(Dec 2021)*** The principal attraction of ECC, compared to RSA, is that it appears to offer equal security for a far smaller key size, thereby reducing processing overhead. But the confidence level of ECC is not yet as high as than in RSA. (i.e. ECC is fundamentally more difficult to explain than either RSA or Diffie-Hellman
18	**What is an ellipse curve?** Elliptic curve is a plane algebraic curve defined by an equation of the form $y^2=x^3+ax+b$ which is non-singular. Formally, an elliptic curve is a smooth, projective, algebraic curve of genius arc, on which there is a specified point O.
19	**Give the significance of key control** Hierarchies of Key Distributor Center (KDC) requires for large networks. A single KDC may be responsible for a small number of users since it shares the master keys of all the entities attached to it. If two entities in different domains want to communicate, local KDCs communicate through a global KDC.
20	**Why is asymmetric cryptography bad for huge data? Specify the reasons** ***(May 18)*** ✓ Asymmetric cryptography takes more time ✓ Key management is difficult ✓ Slower encryption speed due to long keys
21	**Give the applications of the public key crypto system** ✓ To provide confidentiality (a message that a sender encrypts using the recipients public key can be decrypted only by the recipient‟s private key ✓ Digital signature (used for sender authentication) ✓ Further applications built on this include: digital cash, password authenticated key agreement, time-stamping services, non-repudiation protocol, etc.
22	**What is the use of Fermat‟s theorem** Fermat‟s theorem is a fundamental theorem in elementary number theory, which helps compute powers of integers modulo prime numbers. It is a special case of Euler‟s theorem and is important in applications of elementary number theory, including primality testing and public key cryptography.
23	**Calculate** $2110^{2020} \pmod{1009}$ **using Fermat‟s theorem.** ✓ Are 2110 and 1009 co-prime? ✓ If so, by the theorem $21101008 \equiv 1 \pmod{1009}$ ✓ By multiplication rule, $21102016 \equiv 1 \pmod{1009}$ ✓ Same as finding $21104 \pmod{1009}$ ✓ Ans – $21102020 \equiv 296 \pmod{1009}$

24	**Define primality testing.** A primality test in an algorithm for determining whether an input number is prime (i.e. Given an number n, check if it is prime or not)
25	**State whether symmetric and asymmetric cryptography algorithm needs key exchange** ✓ In symmetric key encryption all parties involved in communication have to exchange the key (a secret key) used to encrypt the data before they can decrypt it (This is the main disadvantage of symmetric encryption) ✓ Asymmetric key encryption uses two keys. A public key is made freely available to anyone who might want to send you a message. The second key, private key is kept secret.
26	**Using Fermat"s theorem find 5^{201} and mod 41** $a^{p-1} \equiv 1 \pmod{p}$ where p is prime number and a is a positive integer not divisible by p. $5^{40} \equiv 1 \pmod{41}$ $(5^{40})^5 \equiv 1 \pmod{41}$ $5^1 \equiv 5 \pmod{41}$ So, $5^{201} \equiv 5 \pmod{41}$
27	**Find the GCD of (2740, 1760) using Euclid"s Algorithm.** ***(Dec 2020)*** GCD (2740,1760) = GCD (1760,980) = GCD (980, 780) = GCD (780, 200) = GCD (200, 180) = GCD (180, 20) = GCD (20, 0) = 20
28	**For p = 11 and q = 19 and choose d = 17. Apply RSA algorithm where Cipher message = 80 and thus find the plain text.** ***(Dec 2020)*** n = pq = 11 × 19 = 209. $C=M^e \bmod n$; $C=5^{17} \bmod 209$; C = 80 mod 209. So the plain text is 5
29	**What is meet in the Middle Attack?** ***(Dec 2021)*** ➢ A Meet-in-the-Middle (MitM) Attack is a kind of cryptanalytic attack where the attacker uses some kind of space or time tradeoff to aid the attack. ➢ MitMs can take the form of dividing the target communication into two so that each piece can be addressed individually. ➢ It could mean transforming an attack requiring X amount of time into one requiring Y time and Z space. The aim is to significantly reduce the effort needed to perform a brute-force attack.
	UNIT-III / PART-B
1	State Chinese Remainder Theorem and find X for the given set of congruent equations using CRT X = 2 (mod 3) X = 3 (mod 5) X = 2 (mod 7)

2	State and prove Fermat‟s theorem.
3	Explain RSA algorithm, perform encryption and decryption to the system with p=7, q=11, e=17, M=8
4	Users Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q=83 and a primitive root α=5. i. If Alice has a private key X_A=6, what is Alice‟s public key Y_A? ii. If Bob has a private key X_B=10, what is Bob‟s public key Y_B? iii. What is the shared secret key?
5	State Chinese Remainder Theorem and find X for the given set of congruent equations using CRT ***(Dec 2020)*** X=1 (mod 5) X=2 (mod 7) X=3 (mod 9) X=4 (mod 11)
6	Explain Diffie-Hellman key exchange algorithm in detail
7	Perform encryption and decryption using RSA algorithm for p=17, q=11, e=7 and u=88
8	Why ECC is better than RSA? However, why is it not widely used? Defend it.
9	State and prove Chinese remainder theorem. What are the last two digits of 49^{19}?
10	(ii) With a neat sketch explain the Elliptic curve cryptography with an example (8) (ii) Alice and Bob use the Diffie – Hellman key exchange technique with a common prime number 11 and a primitive root of 2. If Alice and Bob choose distinct secret integers as 9 and 3, respectively, then compute the shared secret key. (5) ***(Dec 2020)***
11	Describe RSA algorithm & Perform encryption and decryption using RSA algorithm for the following: p=7, q=11, e=7, M=9
12	Explain briefly about Diffie-Hellman key exchange algorithm with its merits and demerits.
13	Explain public key cryptography and when it is preferred?
14	Explain the working of RSA and chose an application of your choice for RSA and explain how encryption and decryption is carried out?
15	Prove Fermat‟s theorem and Euler‟s theorem
16	Demonstrate encryption and decryption for the RSA algorithm: Parameters – p=3, q=11, e=7, d=?, M=5
17	Demonstrate encryption and decryption for the RSA algorithm: Parameters – p=7, q=13, e=5, d=?, M=10
18	In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext M. ***(Dec 2021)***
19	Given prime number q=17, Primitive root a=6, private key of A, X_A =5, message m=13, random number k=10. Perform encryption & decryption using Elgamal cryptosystem. (Dec 2021)
	UNIT-IV INTEGRITY AND AUTHENTICATION ALGORITHMS *Authentication requirement – Authentication function – MAC – Hash function – Security of hash* ***function: HMAC, CMAC – SHA – Digital signature and authentication protocols – DSS – Schnorr Digital Signature Scheme – ElGamal cryptosystem – Entity Authentication: Biometrics, Passwords, Challenge Response protocols – Authentication applications – Kerberos*** MUTUAL TRUST: Key management and distribution – Symmetric key distribution using symmetric and asymmetric encryption – Distribution of public keys – X.509 Certificates
PART - A	

<table>
<tr><td>1</td><td>What is digital signature?
A digital signature is an authentication technique that also includes measures to counter repudiation by either source or destination.</td></tr>
<tr><td>2</td><td>What are the requirements for (message) authentication?
✓ Disclosure: Release of message contents to any person or process not possessing the appropriate cryptographic key.
✓ Traffic analysis: Discovery of the pattern of traffic between parties (The frequency and duration of connections; the number and length of messages)
✓ Masquerade: Insertion of messages into the network from a fraudulent source. This includes the creation of messages by an opponent that are purported to come from an authorized entity.
✓ Content Modification: Changes to the contents of a message, including insertion, deletion, transposition and modification.
✓ Sequence modification: Any modification to a sequence of messages between parties, including insertion, deletion and recording.
✓ Repudiation: Denial of receipt of message by destination or denial of transmission of message by source.</td></tr>
<tr><td>3</td><td>List the types of functions that may be used to produce an authenticator.
✓ Message encryption: The ciphertext of the entire message serves as its authenticator.
✓ Message Authentication Code(MAC): A public function of the message and a secret key that produces a fixed length value that serves as the authenticator.
✓ Hash function: A public function that maps a message of any length into fixed-length hash value, which serves as the authenticator.</td></tr>
<tr><td>4</td><td>What is hash(function) in cryptography?
A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.</td></tr>
<tr><td>5</td><td>Define the term „Message Digest".
A hash function accepts a variable size message M as input and produces a fixed size length hash code H(M), called a message digest, as output. So the values returned by a hash function are called message digest or simply hash values.</td></tr>
<tr><td>6</td><td>What is MAC? Mention the requirement of MAC (Dec 2020)
A MAC sometimes known as tag is a block of few bytes that is used to authenticate a message. The receiver can check this block and be sure that the message hasn"t modified by third party.</td></tr>
<tr><td>7</td><td>Compare MAC and hash function
<table>
<tr><th>MAC</th><th>Hash function</th></tr>
<tr><td>MAC guarantees the integrity and authentication.</td><td>Hash function guarantees the integrity of data</td></tr>
<tr><td>MAC uses a private key.</td><td>Hash doesn"t use keys</td></tr>
</table></td></tr>
</table>

	Did not provide confidentiality.	Did not provide confidentiality.
	Fast in processing speed	Quite fast in processing

8 **Compare Hash Practices, MAC and digital signature.**

Properties	Hash	MAC	Digital Signature
Integrity	Yes	Yes	Yes
Authentication	No	Yes	Yes
Non-Repudiation	No	No	Yes

9 **How is the security of a MAC function expressed?**

The security of a MAC function is generally expressed in terms of the probability of successful forgery with a given amount of time spent by the forger and a given number of message-tag pairs created with the same key

10 **Mention the significance of signature function in DSS approach**

- ✓ Signature function in DSS gets the input with random number generated for a particular signature.
- ✓ Signature function also depends on the sender‟s private key(P_{Ra}) and a set of parameters known to a group of communicating principals.
- ✓ The signature function is such that only the sender, with the knowledge of the private key, could have produced the valid signature

11 **What is the role of compression function in hash function?**

The compression function is a function that transforms two fixed length inputs into a fixed length output. The transformation is one-way, meaning that it is difficult given a particular output to compute inputs which compress to that output. One-way compression function are not related to conventional data compression algorithm, which instead can be inverted exactly or approximately to the original data.

12 **Specify the various types of authentication protocol**

An authentication protocol is a type of computer communication protocol or cryptographic protocol specifically designed for transfer of authentication data between two entities. Different types are

- ✓ Password Authentication Protocol (PAP)
- ✓ Challenge Handshake Authentication Protocol (CHAP)
- ✓ Extensible Authentication Protocol (EAP)
- ✓ Remote Authentication Dial-In User Service (RADIUS)
- ✓ Kerberos (Protocols)

13 **List any two applications of X.509 certificates**

- ✓ X.509 is a standard defining the format of public-key certificates
- ✓ X.509 certificates are used in many internet protocols, including TLS/SSL which is the basis for HTTPS, the secure protocol for browsing the web
- ✓ X.509 are also used in offline applications like electronic signatures.

14 **Write a simple authentication dialogue used in Kerberos.**

(1) $C \rightarrow AS \quad 1D_c||P_c||1D_v$

(2) $AS \rightarrow C \quad Ticket$

(3) $C \rightarrow V \quad 1D_c||Ticket$

$Ticket = E_{Kv}\ [1D_c||AD_c||1D_v]$

where

C= Client

A= Authentication server

V= Server

$1D_c$= Identifier of user on C

$1D_v$= Identifier of user on V

P_c= Password of user on C

AD_c= Network address of C

K_V= Secret encryption key shared by A, S and V.

||= Concatenation

15 **Contrast various SHA algorithms.**

Properties	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Message Digest Size	160	224	256	384	512
Message Size	$<2^{64}$	$<2^{64}$	$<2^{64}$	$<2^{128}$	$<2^{128}$
Block size	512	512	512	1024	1024
Word size	32	32	32	64	64

16 **What is digital signature?**

A digital signature is an authentication mechanism that allows the sender to attach an electronic code with the message in order to ensure its authenticity and integrity. This electronic code acts as the signature of the sender and, hence is named digital signature. Digital signature uses the public-key cryptographic technique. The sender uses his private key and a signing algorithm creates a digital signature, and the signed document can be made public. The receiver uses the public key of the sender and a verifying algorithm to verify the digital signature.

17 **What is realm in Kerberos?**

A Kerberos realm is a set of managed nodes that share the same Kerberos database. The Kerberos database resides on the Kerberos master computer system, which should be kept in a physically secure room. A read-only copy of the Kerberos database might also reside on other Kerberos computer systems. However, all changes to the database must be made on the master computer system. Changing or accessing the contents of a Kerberos database requires the Kerberos master password.

18 **What entities constitute a full service in Kerberos environment?**

A full-service environment consists of a

- ✓ Kerberos server
- ✓ A number of clients
- ✓ A number of application servers

<table>
<tr><td>19</td><td colspan="2">How digital signatures differ from authenticator protocols? (Dec 2021)</td></tr>
<tr><td></td><td>Digital signature</td><td>Authentication Protocol</td></tr>
<tr><td></td><td>➢ A digital signature is an authentication mechanism that allows the sender to attach an electronic code with the message in order to ensure its authenticity and integrity.
➢ This electronic code acts as the signature of the sender and, hence is named digital signature. Digital signature uses the public-key cryptographic technique.
➢ The sender uses his private key and a signing algorithm to create a digital signature, and the signed document can be made public.
➢ The receiver uses the public key of the sender and a verifying algorithm to verify the digital signature</td><td>➢ Used to convince parties of each other identity and to exchange session keys.
➢ May be one-way or mutual
➢ Key issues are
• Confidentiality – to protect session keys
• Timeliness – to prevent replay attacks Digital signature:</td></tr>
<tr><td>20</td><td colspan="2">State the requirements of a digital signature
✓ The signature must be a bit pattern that depends on the message being signed.
✓ The signature must use some information unique to the sender to prevent both forgery and denial.
✓ It must be relatively easy to produce the digital signature.
✓ It must be relatively easy to recognize and verify the digital signature.
✓ It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message.
✓ It must be practical to retain a copy of the digital signature in storage.</td></tr>
<tr><td>21</td><td colspan="2">Show how SHA is more secure than MD5
✓ It produces a largest digest (160-bit compared to 128 bits, so a brute force attack would be more difficult to carry out)
✓ No known collisions have been formed for SHA
✓ Never version have been introduced in SHA (SHA-256, SHA-384, SHA-512) that are much more secure than the original.</td></tr>
<tr><td>22</td><td colspan="2">What do you mean by one-way properly in hash function?
One-way function is easy to compute but it is very difficult to compute their inverse functions. Thus, having data n, it is easy to calculate f(n) but, knowing the value of f(n) it is quite difficult to calculate the value of X,
✓ One-way hash functions fulfill all conditions of one-way functions.
✓ A one-way hash function should be collision-free
✓ Algorithms of one-way hash functions are often to the public.</td></tr>
<tr><td>23</td><td colspan="2">What is weak collision resistance?
Given n, is infeasible to find y such that H(y)=H(n)</td></tr>
</table>

24	**What is replay attack?** A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence.
25	**State Birthday Problem.** ***(Dec 2020)*** Birthday attack is a type of cryptographic attack that belongs to a class of brute force attacks. It exploits the mathematics behind the birthday problem in probability theory. The success of this attack largely depends upon the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations
26	**Identify and write the requirements defined by Kerberos.** ***(Dec 2021)*** ✓ Secure ✓ Reliable ✓ Transparent ✓ Scalable
	UNIT-IV / PART-B
1	Compare the uses of MAC and hash function. Represent them using appropriate diagrams ***(Dec 19)***
2	List out the advantages of MD5 and SHA algorithms
3	Suggest and explain about an authentication scheme for mutual authentication between the user and the server which relies on symmetric encryption
4	Explain digital signature standard with necessary diagrams in detail
5	Discuss client server mutual authentication, with example flow diagram
6	Write down the steps involved in (i) Elgamal digital signature scheme (ii) Schnorr digital signature scheme used for authenticating a person
7	With a neat diagram, explain the steps involved in SHA algorithm for encrypting a message with maximum length of less than 2^{128} bits and produces as output a 512-bit message digest.
8	Discuss the different methods involved in authentication of source.
9	Write about how the integrity of message is ensured without source authentication.
10	Explain the concepts of digital signature algorithm with key generation and verification in detail.
11	Explain SHA2 in detail
12	Explain Elgamal digital signature schemes.
13	How hash function algorithm m is designed? Explain their features and properties ***(May 18)***
14	Explain briefly about the architecture and certification mechanism in Kerberos and X.509
15	What is Kerberos? Explain how it provides authenticated services

16	Explain the format of the X.509 certificate in detail ***(Dec 2021)***
17	Explain Kerberos version 4 in detail
18	Briefly explain the steps of message digest generation in Whirlpool with a block diagram ***(Dec 2020)***
19	Explain PKI management model and its operations with the help of a diagram. ***(Dec 2020)***
20	Describe digital signature algorithm and show how signing and verification is done using DSS. ***(Dec 2021)***
21	Consider a banking application that is expected to provide cryptographic functionalities. Assume that this application is running on top of another application wherein the end customers can perform a single task of fund transfer. The application requires cryptographic requirements based on the amount of transfer. ***(Dec 2020)***

Transfer Amount	**Cryptography functions required**
1 – 2000	Message Digest
2001 – 5000	Digital Signature
5000 and above	Digital Signature and Encryption

Suggest the security scheme to be adopted in client and server side to accommodate the above requirements and justify your recommendations.

UNIT V CYBER CRIMES AND CYBER SECURITY

Cyber Crime and Information Security – classifications of Cyber Crimes – Tools and Methods – Password Cracking, Key loggers, Spywares, SQL Injection – Network Access Control – Cloud Security – Web Security – Wireless Security

UNIT-V / PART-A

1	**Define Cybercrime.** Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device .Cybercrime is committed by cybercriminals or hackers who want to Make money. Cybercrime is carried out by individuals or organizations.
2	**Define Information Security.** Information security means to consider available countermeasures or controls stimulated through uncovered vulnerabilities and identify an area where more work is needed. The purpose of data security management is to make sure business continuity and scale back business injury by preventing and minimizing the impact of security incidents.
3	**List the need for information Security** ✓ Protecting the functionality of the organization ✓ Enabling the safe operation of applications ✓ Protecting the data that the organization collects and use ✓ Safeguarding technology assets in organizations

4	**What are the category of cybercrime?** ✓ Cybercrimes against persons. ✓ Cybercrimes against property. ✓ Cybercrimes against government.
5	**What is the purpose of password cracking?** ✓ To recover a forgotten password. ✓ As a preventive measure by system administrators to check for easily crack able passwords. ✓ To gain unauthorized access to a system,
6	**What are the types of password cracking attacks?** ✓ Online attacks ✓ Offline attacks ✓ Non-electronic attacks
7	**Define Key loggers**. Keystroke logging, often called keylogging, is the practice of noting (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is Unaware that such action are being monitored. It can be classified as software key logger and hardware key logger.
8	*Define Software Key loggers.* Software keyloggers are software programs installed on the computer systems which usuallyare located between the OS and the keyboard hardware, and every keystroke is recorded. Software keyloggers are installed on a computer system by Trojans or viruseswithout the knowledge of the user.
9	What is Hardware Key loggers. Hardware keyloggers are small hardware devices. These are connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device. Cybercriminals install such devices on ATM machines to capture ATM Cards' PINs. Each Key press on the keyboard of the ATM is registered by these key loggers.
10	**Define Spyware.** Spyware is a type of malware that is installed on computers which collects information about users without their knowledge. It is clearly understood from the term Spyware that it secretly monitors the user. The features and functions of such Spywares are beyond simple monitoring.
11	**Define SQL injection.** SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.

12	**What are the Types of SQL Injections** ✓ In-band SQLi ✓ Error-based SQLi ✓ Union-based SQLi ✓ Inferential (Blind) SQLi ✓ Out-of-band SQLi
13	**What is network access control?** Network access control (NAC), also known as network admission control, is the process of restricting unauthorized users and devices from gaining access to a corporate or private network. NAC ensures that only users who are authenticated and devices that are authorized and compliant with security policies can enter the network.
14	**What Are the Advantages of Network Access Control?** ✓ Control the users entering the corporate network ✓ Control access to the applications and resources users aim to access ✓ Allow contractors, partners, and guests to enter the network as needed but restrict their access ✓ Segment employees into groups based on their job function and build role-based access policies ✓ Protect against cyberattacks by putting in place systems and controls that detect unusual or suspicious activity ✓ Automate incident response ✓ Generate reports and insights on attempted access across the organization
15	**What is Cloud Security** Cloud security is a responsibility that is shared between the cloud provider and the customer. There are basically three categories of responsibilities in the Shared Responsibility Model: responsibilities that are always the provider's, responsibilities that are always the customer's, and responsibilities that vary depending on the service model, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service(SaaS), such as cloud email.
16	**What are the Challenges of Advanced Cloud Security?** ✓ Increased Attack Surface ✓ Lack of Visibility and Tracking ✓ Ever-Changing Workloads ✓ DevOps, DevSecOps and Automation ✓ Granular Privilege and Key Management ✓ Complex Environments ✓ Cloud Compliance and Governance
17	**Write short notes on Web Security.** Web Security deals with the security of data over the internet/network or web or while it is being transferred to the internet. For e.g. when you are transferring data between client and server and you have to protect that data that security of data is your web security**.**
18	**What are the different types of Security Threats** **Cross-site scripting (XSS)** SQL Injection, Phishing, Ransomware, Code Injection Viruses and worms, Spyware, Denial of Service

19	**Define Wireless Security**. Wireless security is the prevention of unauthorized access or damage to computers or data using wireless networks, which include Wi-Fi networks. The term may also refer to the protection of the wireless network itself from adversaries seeking to damage the confidentiality, integrity, or availability of the network.
20	**What are the security considerations in web security?** ✓ Updated Software ✓ Beware of SQL Injection ✓ Cross-Site Scripting ✓ Error Messages ✓ Data Validation ✓ Password
	PART - B
1	Briefly Explain about the Cybercrime and Information security
2	Explain in detail about the classification of cybercrimes.
3	Explain in detail about the types of cyber-attacks.
4	Explain in detail about the password cracking and types of attacks in password cracking
5	Write short notes on key-logger and explain in detail about types of Key-logger?
6	Explain briefly about the spywares.
7	Explain in detail about the SQL injection and its types.
8	Explain in detail about the cloud security.
9	Explain in detail about the web security
10	Explain in detail about the wireless security