Page No. 1.1
Date 30/03/2022

Assignment-1

Part-A

Q.1 From the option below, which of them is not a threat to information Security?

Ans Unchanged default Password

Q.2 Lack of access control policy is a ...

Ans Vulnerability

Q.3 Possible threat to any information cannot be ...

Ans ignored

Q.4 Risk mitigation includes all of the following except.

Ans Protected

Q.5 ..... is the Science and art of transforming message to make them Secure and immune to attacks.

Ans Cryptography

Q.6 In Symmetric-key cryptography, the key locks and unlocks the box is.

Ans Same

Q.7 The acronym DES Stands for

Ans Data encryption Standard (Digital Encryption Standard)

Q.8 Encryption strength is based on..

Ans (D) All of the above (A.) length of key
(b) secrecy of key
(c) strength of Algorithm

Q 9 The - . . . is the original message before transfor
Ans Cryptography
(2) None of the above.

Q 10 Encode the following plain text using transposition method. (Assume key = Four)
Plain Text = Information Security and Cyber law

Ans Key = FOUR
Order = FOUR = 1243
Encrypted Message -
⇒ IRIENBANMOCTDELWEANU
YCROTSRAYL

4	2	3	1
F	O	U	R
I	N	F	O
R	M	A	T
I	O	N	S
E	C	U	R
I	T	Y	A
N	D	C	Y
B	E	R	L
A	W		

Q 11 Which of the following type of attack can actively modify communication or data?
Ans Active attack

Q 12 Interception is an attack on?
Ans Confidentiality

Q 13 Which are called the block cipher?
Ans All of the mentioned

Q 14 Cryptography is the specialized area of . . .
Ans Cyber Security

Q.15 In which type of cryptography same key is used as encryption and decryption.

Ans. Symmetric Cryptography.

Part - B

Q.1 What is the purpose of Security.

Ans. The goal of IT Security is to protect these assets, devices and services from being disrupted, stolen or exploited by the unauthorized users, otherwise known as threat actors. These threats can be external or internal and malicious or accidental in both origin and nature.

Q.2 What is the difference between plain text and ciphertext.

Ans. Plain text :- This is the message or data in the natural format and in readable form. plaintext is human readable and extremely vulnerable from a confidentiality perspective. plain text is also called clear text. Plaintext is a message or data that has not been turned into a secret.

Cipher Text :- This is the altered form of plaintext message so as to be unreadable for anyone except the intended recipients in other words, it has been turned into a secret. An eavesdropper or an attacker seeing the ciphertext would be unable to easily read the message or determine its content.

Q 3 What is attack? How it can be prevented.

Ans An attack is an information Security threat that involves an effort to use information to obtain, alter destroy, remove implant or reveal information without authorized access or permission. It happen to both individual and organizations. There are many different kinds of attacks including but not limited to passive, active, targeted, distjacking, transjacking, botnet, phishing, Spamming, inside and outside.

The four recommended steps to prevent attacks or reduce vulnerabilities.

Provide a Simple Security network architecture develop a culture of Security develop Security policy.

Q 4 What is difference between Confidentiality and Authorization

Ans Authorization ⇒ Authorization is about establishing what particular user is permitted to do. So, it follows that authentication always happens before authorization. Authorization covers things like confidentiality (as the person allowed to see this data?), but also things such as is this person allowed to modify this data, so can they delete it.

Confidentiality ⇐ Confidentiality is used to make sure that nobody in between Site A and Site B is able to read what data or information is sent between the two sites To achieve this encryption algorithm are used. There are two kind

encryption algorithms, Symmetric and also asymmetric ones. Symmetric algorithms allow encryption and decryption with the same key. With asymmetric algorithms you have to kinds of keys a public one and also a private one.

Q.5 Give two differences between Block cipher and Stream cipher.

Ans. Block cipher :-

- Block cipher converts the plain text into cipher text taking plain text's block at a time.
- Block cipher uses either 64 bits or more than 64 bit. The complexity of block cipher is simple.

- Stream cipher :-

- Stream cipher converts the plain text into cipher text taking 1 byte of plain text at a time.
- While stream cipher uses 8 bits.
- Stream cipher is more complex.

Part - C

Q.1 Define key size and key range in cryptography.

Ans. Key Size :- In cryptography, key size, key length, or key space is the number of bits in a key used by a cryptographic algorithm (such as a cipher)

Indeed most symmetric key algorithm are designed to have security equal to their key length. However after design a new attack might be discovered

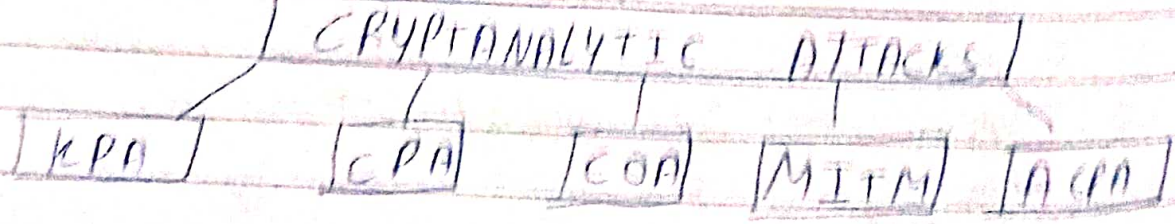
- Key Range :- key range is total number of key from smallest to largest available key of attacker usually is arise with the knowledge of the cryptographic algorithm and the encrypted range, he only the actual key value remains the challenge for the attacker.

Q2 Explain cryptanalytic attacks.

Ans Cryptanalysis which is the study of the cryptographic algorithm and the breaking of those secret code. The process practicing cryptanalysis is called a cryptanalyst. It helps us to better understand the cryptosystem and also helps us improve the system by finding any weak point and thus work on the algorithm to create a more secure secret code.

For example:- a cryptanalyst might try to decipher a cipher text to derive the plaintext. It can help us to deduce the plaintext or the encryption key.

Types of cryptanalytic attacks :-



- Known - plaintext Analysis (KPA) :-
In this type of attack, some plaintext - ciphertext pair are already known. Attacker maps them in order to find the encryption key. This attack is easier to use as a lot of information is already available.

- Chosen - Plaintext Analysis (CPA) :-
In this type of attack, the attacker chooses random plaintext and obtains the corresponding ciphertext and tries to find the encryption key. It very simple to implement like KPA but the success rate is quite low.

- Ciphertext - Only Analysis (COA) :-
In this type of attack, only some cipher - text is known and attacker tries to find the corresponding encryption key and plaintext. It is the hardest to implement but is the most probable attack as only ciphertext is required.

- Man - In - The - Middle (MITM) Attack :-
In this type of attack, attacker intercepts the message key between two communicating parties through a secure channel.

- Adaptive chosen - Plaintext Analysis (ACPA) :-
This attack is similar CPA. Here the attacker requires the cipher. text of additional plaintext after they have ciphertexts for some texts.

Q.3 Differentiate between Substitution cipher and Transposition cipher.

	Substitution Cipher	Transposition Cipher
1	In this technique, plain text character are replaced with other character, numbers & Symbols	In this technique, plain text character are rearranged with respect to the position
2	Substitution cipher's forms are mono alphabetic substitution cipher and poly alphabetic substitution cipher.	Transposition cipher's forms are: key-less transposition cipher and keyed transposition cipher
3.	In this technique character identity is changed while its position remains unchanged.	In this technique the position of the character is changed but character's identity is not chang
4.	In this technique, the letter with low frequency can detect plain text.	In this technique the keys that are nearer to correct key can disclose plain text.
5	The example of this technique is Caesar cipher	The example of this technique is Rail fence cipher.

Q.4 What do you understand by Substitution technique.

Ans Substitution technique is a classical encryption approach where the characters present in the initial message are restored by the user other character or number or by symbols. If the plain text is treated as the string of bits, thus the substitution technique would restore bit pattern of plain text with the bit pattern of cipher text.

Q4 There are various type of substitution cipher which are as follows:
Monoalphabetic cipher
Polyalphabetic cipher

Q5 Differentiate between Symmetric key cryptography and asymmetric key cryptography.

Ans.	Symmetric key Cryptography	Asymmetric key cryptography
1.	There is only one key is used and the similar key can be used to encrypt and decrypt the message	There are two different cryptography keys known as the public and the private keys. are used for encryption and decryption. It is
2.	It is effective as this technique is recommended for high amount of text	Inefficient as this approach is used only for short messages.
3	Symmetric encryption is generally used to transmit bulk information	It is generally used in smaller transactions. It is used to make a secure connection channel before transferring the actual information
4.	The length of the key used is frequently 128 or 256 bits, based on the security need.	The length of the keys is much higher such as the recommended RSA key size is 2048 bits or higher.
5.	Symmetric key cryptography is also known as secret key cryptography or private key cryptography	Assymetric key cryptography is also know as public key cryptography or a conventional cryptography system.

Page No. 16
Date / /

Part - D

Q1 Explain network security attacks on the basis of Sec

Ans

Network attacks are unauthorized actions on the dig
attack within an organization. Network, malicious: pro
usually execute network attacks to alter, destroy
steal private data. While you are uploading yo
data on the internet and thinking it is safe a
Secure attacker can breach this data and lea
confidential information or steal money. This is why it
necessary to secure your network. Network
security is an important part of cyber security and
helps in protecting your network and data from
unauthorized breaches, Software and hardware intru
and more. Network Security defines a set of
rules regulation and configuration that
controls network use accessibility and complet
and Security. Network Security is responsible
for preventing these attacks on the networ
infrastructure.

Type of attacks in Network Security

1. Virus
2. malware
3. Worm
4. Packet sniffer
5. Phishing
6. Compromised key
7. Bothet
8. DOS

Page No. 11
Date / /

Q.2 Explain play fair cipher with example, encrypt HIDE MONEY using playfair.

Ans Play fair cipher :-

The playfair cipher was the first practical digraph substitution cipher in playfair cipher unlike traditional cipher we encrypt a pair of alphabets instead of a single alphabet.

It was used for tactical purposes by British forces in the Second Boer war and in World War I and for the same purpose by the Australians during world war II.

The playfair cipher encryption Algorithm:

The algorithm consists of 2 steps:

1. Generate the key square (5×5):
- The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually I) is omitted from the table (as the table can hold only 25 alphabets) if a plaintext contains I then it is replaced by I.
- The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

2. Algorithm to encrypt the plain text:

The plain text is split into pairs of two letters (digrams). If there is an odd number of letters a Z is added to the last letter.

Ex: Plain Text: "Instruments"
After split: 'in' 'st' 'ru' 'me' 'nt' 's2'
Cipher text = gallmzclostx

→ HIDE MONEY
after split: 'HI' 'DE' 'MO' 'NE' 'Y2'

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

Encrypted Text:

H - F
I - B
D - I
E - M
M - G
O - T
N - U
E - N
Y - F
2 - X

Assignment-2

Part-A

Q.1 Des is an _____
(a) Symmetric key (b) asymmetric key
(c) either (a) or (b) (d) neither (a) nor (b)
Ans a) Symmetric key

Q.2 DES has an initial and rounds.
Ans (c) 16

Q.3 DES uses a key generates
Ans (b) 48 bits

Q.4 AES has ____ different
Ans (b) Three

Q.5 ECB and CBC are ____
(a) block (b) Stream
(c) field (d) none of the above
Ans (a) block

Q.6 The ____ method parties
Ans (a) Diffie Haffman

Q.7 The acronym DES stands for
Ans (b) Data encryption standard (Digital Encryption Standard)

Q.8 What are the allowable values of word size in bit for

RC5 algorithm?

Ans (b) 16, 32, 64

Q.9 Calculate the number of subkeys required in RC5 for 18 rounds of computation.

Ans (b) 38

Q.10 Data encryption standard is a block cipher and encrypts data in block of size of ___ each.

Ans (b) 64 bits

Q.11 The process of decryption of an AES ciphertext is similar to the encryption process in the ___

Ans (a) Reverse order

Q.12 AES stands for Advanced encryption standard.

Ans (a) True

Q.13 Which are called the block cipher?

Ans (d) All of the mentioned

Q.14 When do we compare the AES with DES, which of the following function from DES does not have an equivalent AES function in cryptography?

Ans (c) swapping of halves

Q.15 The number of tests required to break the DES algorithm are.

Ans (d) 7.2×10^{16}

Part-B

Q1 what is the purpose of Symmetric encryption?

Ans Symmetric encryption is the process of converting plaintext into ciphertext and vice versa using the same key. An encryption key is a random string of bits used to encrypt or decrypt data. It is therefore important that key is transferred between the sender and receipient using secure methods. The benefit of Symmetric key encryption is that it is fast and convenient to setup.

Q2 Explain the concept of Feistel Block cipher.

Ans Feistal cipher is a design model designed to create different block ciphers, such as DES. The model uses substitution and permutation alternatively. The cipher structure is based on the Shannon model proposed in 1945, demonstrating the confusion and diffusion implementation processes. Confusion produce a complex relationship between the ciphertext and encryption key which is done by using a substitution algorithm. On the other hand, diffusion creates a complex relationship between plaintext and ciphertext by using a permutation algorithm.

Q3 Explain blowfish algorithm.

Ans Blowfish feature a 64 bit block size and take a variable length key, from 32 bit to 448 bit. It consists of 16 feistal like iterations where each iteration operates on 64 bit block that is split into two 32 bits words.

Part-B

Q.1 what is the purpose of Symmetric encryption?

Ans Symmetric encryption is the process of converting plain text into cipher text and vice versa using the same key. An encryption key is a random string of bits used to encrypt or decrypt data.. it is therefore important that key is transferred between the sender and receipient using secure methods. The benefit of Symmetric key encryption is that it is fast and convienent to setup.

Q.2 Explain the concept of Feistel Block cipher.

Ans Fiestal cipher is a design model deigned to creat different block cipher, such as DES, The model uses substitution and permutation alternatively. This Cipher structure is based on the shannan model proposed in 1945, Emanstating the confusion and diffusion implementation processes. Confusion produces a complex relationship between the cipher text and encrypted key, which is done by using a substitution algorithm on the other hand, diffusion creates a complex relationship between plain text and cipher text by using a permutation algorithm.

Q.3 Explain blowfish algorithm.

Ans. Blowfish features a 64 bit block size and takes a variable length key, from 32 bit to 448 bit. It consists of 16 fiestal like iterations where each iteration operates on 64 bit. block that is split into two 32 bits words.

Q.4 Explain how the concept of IDEA cryptography?

Ans The international data encryption algorithm (IDEA) is a symmetric key block cipher encryption algorithm design to encrypt text to a unreadable form for transmission via the Internet.

Q.5 Give two difference between block cipher and stream cipher?

Ans • Block cipher converts plain text into cipher text by taking plain text block at a time. Stream cipher converts the plain text into cipher text by taking 1 bytes of plain text at a time.

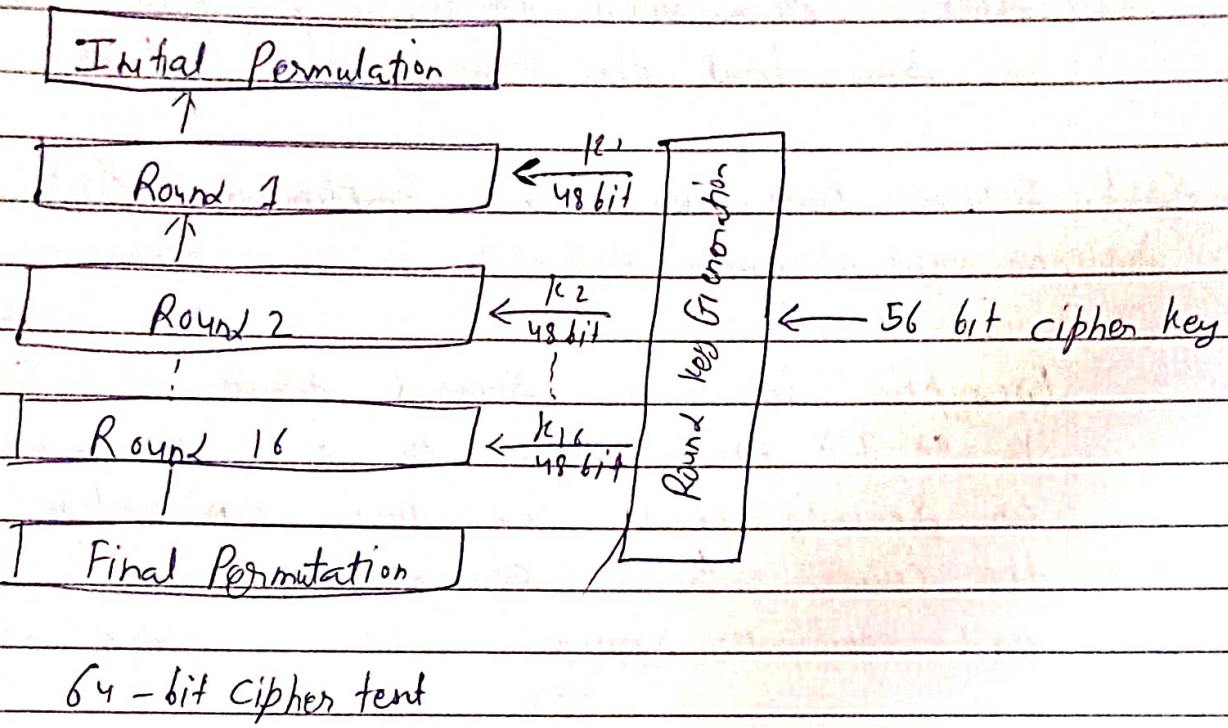
- Block cipher use either 64 bits or more than 64 bits.
- while stream cipher use 8 bits.

Part - C

Q.1 Explain the concept of DES?

Ans The Data encryption standard (DES) is a symmetric key block cipher published by the National Institute of Standard and Technology (NIST).

DES is an implementation of a feistel cipher, it use 16 round feistel structure. The Block size of 64 bit. Though, key length is 64-bit, DES has an effective key length of 56 bits. (Since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General structure of DES is depicted in the following illustration.



Since DES is based on the Feistel cipher, all that is required to specify DES is -

- Round function
- key Schedule
- Any additional processing - Initial and final permutation

Q.2 Explain the concept of Confusion and Diffusion.

Ans Confusion :- Confusion means that each binary digit (bit) of the cipher text should depend on several parts of the key obscuring the connections between the two the property of confusion hides the relationship between the cipher text and the key

Diffusion :- Diffusion means that if we change a character of plain text, then several characters of cipher text should change, and

Similarly, if we change of the ciphertext, the several characters of the plaintext should c
we saw that the if is cipher has this propert

Q-3 Discuss how encryption happen in RC5.

Ans Encryption using RC5

Encryption involved several rounds of simple
12 or 20 rounds seem to be recommended defa
on security needs and time considerations. We
the counter to 1 and perform some permuta
and combination using addition and XOR

The algorithm works into two phase
a. First it starts with phase one
b. output of phase one become input of phase two
divide the plaintext block into two equal parts
Then They are XOR with two subkeys S[0] a

$C = A + S[0]$

$D = B + S[1]$

for $i = 1$ to r do

1: $C \oplus D = E$

2- Perform circular left shift on E by D

3: add E and $S[2 \times i]$ and store the
in F which is input for step 4

4. $D \oplus F = G$

5. Perform circular left shift on G
bits

6. Add G and $S[2 \times i + 1]$ and stor
in it

7. If i < 9
Call F as C and H as D and Repeat the steps from 1 to 7
else stop.

- Once both the phase are completed the counts is incremented and we check if it is greater than the number of rounds, if yes then the algorithm terminates and if no then the algorithm starts.

Q.4 How does the one time initialization step work in AES?

Ans. As AES requires 10 rounds, it will need 10 keys and 1 more key for OTR.

- In all eleven keys are required
- So the 16 byte key is expanded to get the actual block the 16 byte key is explained into a key containing 4×4 entries.
- out of the 11 keys 1 key is used for OTR and the remaining 10 keys are used for 10 rounds.
- The next step is to take the plaintext block called as state and represent into 4*4 matrix.
- While copying the elements in the matrix the order should be column-wise.

Q. 5 illustrate the steps of RSA algorithm?

Ans 1.) choose two large prime number (p and q)
2.) calculate $n = p * q$ and $z = (p-1)(q-1)$
3.) choose a number e where $1 < e < z$
4.) Calculate $d = e^{-1} \bmod (p-1)(q-1)$
5.) you can bundle private key pair as (n, d)
6.) you can bundle public key pair as (n, e)

Part - D

Q.1 Explain the basic purpose of IDEA. How IDEA works?

Ans The international Data encryption Algorithm (IDEA) is a symmetric key block cipher encryption algorithm designed to encrypt text to an incoadable form for transmission via the internet. It uses a block size of 128 bits and takes 64 bit input, i.e. 64-bit data. IDEA performs 8.5 encryption and decryption rounds using 52 different subkeys. It uses four keys for each transformation.

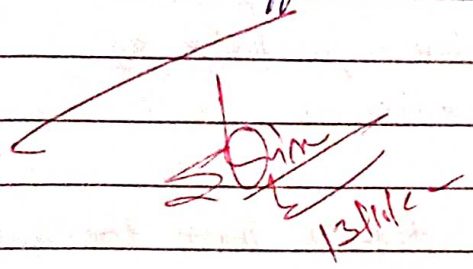
By using a 128-bits key. text - IDEA encrypts 64-bit block of plain text one process partitions plain text block into four 16-bit subblock for of the eight complete rows namely R1, R2, R3, Depending on input plain text blocks.

Q.2 Describe the difference b/w Double DES and Triple DES

Ans Double DES :- It is an encryption technique uses two instance of DES on same text. In both instances it uses different keys encrypt the plain text. Both keys are required the time to decryption. The 64 bit plain text into first DES instance which then converted into 64 bit middle text using the first key and goes to second DES instance which gives 64

cipher text by using second key

Triple DES ⇒ Triple DES is a encryption technique which uses three instance of DES on same plain text. It uses three different types of key. choosing technique in first all used keys are different and in second two keys are same and one is different and in third all keys are same.



Assignment -3

Part -A

Q.1 If A and B want to communicate securely with e other, B must not know?
Ans (c) B's private key

Q.2 If the sender encrypts the message with his private key, it achieves the purpose of
Ans (b) confidentially and Authentication

Q.3 When two different message digests have the same it is called as,
Ans (b) collision

Q.4 To verify a digital signature, we need the.
Ans (b) Sender's public key

Q.5 To decrypt a message encrypted using RSA, we u
Ans (a) Receiver's private key

Q.6 .... are required to conduct commercial transac over the Internet.
Ans (c) digital signature

Q.7 A digital certificate binds a user with.
Ans (b) The User's public key

Q.8 A can issue digital certificates.
Ans (a) CA

Q.9 To solver the problem of trust, the is used.
Ans (c) private key

Q.10 RSA stands for
Ans (b) Rivest, Shamir, Adleman

Q.11 In asymmetric key cryptography although RSA can be used to encrypt and decrypt actual message it is very slow if the message is.
Ans (b) long

Q.12 Public key encryption uses or creates - in its algorithm.
Ans (d) All of these answers are correct

Q.13 Using Rivest, Shamir, Adleman cryptosystem with P=7, and q = 9. encrypt M=24 to find ciphertext. The ciphertext is:
Ans (c) 114

Q.14 RSA algorithm is --- cryptography algorithm.
Ans (b) Symmetric

Q.15 Private key algorithm is used for --- encryption and public key algorithm is used for - + - encryption.
Ans (a) Message, Session key

Section-B

Q.1 What are the disadvantage of asymmetric cryptography
Ans- Slower than Symmetric key.

- The encrypted text is larger than a symmetric
- Point to multi-point does not scale
- If an individual loses his private key, he c
decrypt the messages he receives.
- Because public keys aren't authenticated,

Q. 2 Mention any one technique of attacking RSA.

Ans Plain Text Attack :-

Plain text attacks are classifie
three categories
1) short message attack
2) cycling attack
3.) Unconcealed message attac

⇒ RSA attacks :-
(1) Brute force
(2) Timing attacks
(3) other RSA vulnerabilities

Q. 3 What primitive Operations is used in RC5?

Ans There are Three primitive operations:
1) integer addition
2) bitwise XOR - (exclusive - or)
3) Variable relation

Q. 4 What are the properties a digital signatures s

Ans 1) Authenticity
2) Unforgeability
3) Non-re-usability
4) Non-repudiation
5) Integrity

Q.5 Differentiate between Asymmetric Cryptography and Symmetric Cryptography.

Ans

Symmetric Cryptography	Asymmetric Cryptography
1) There is only one key is used between sender and receiver	There are a group of pairs is used between sender and receiver (public and private key)
2) It is effective as this technique is recommended for high amount of data.	It is inefficient as this technique is used for short message.
3) The length of key used is frequently 128 or 256 bits, based on the security level	The length of the key must higher such as the recommended RSA key size is 2048 bits or higher
4) It is also known as symmetric key / secret key Cryptography	It is also known as public key or conventional public system

Section-C

Q.1 What is the Real crux of RSA?

Ans The Real crux of RSA algorithm is:
- The knowledge of the public key does not reveal the secret key.

Q.2 What is the important aspect that establish trust in digital Signatures.

Ans A digital Signature a type of electronic Signature is a mathematical algorithm routinely used to validate the authenticity and integrity of a message. Digital Signature create a virtual fingerprint that is unique. To identify users and project information in digital message or documents.

⇒ Integrity :-
The digital Signature preserves the integrity of
because if any malicious attack intercepts
and partially or totally changes a then the
message would be impossible.

⇒ Authentication :-
We can use the following reasoning to show
message is authenticated, if a intruder (user
Sends a message pretending that it is
from someone else (user A), user X uses
own private key to encrypt the message.
message is decrypted by using the public k
user A. Therefore this makes the message

⇒ Non-Repudiation :-
Digital Signature also provides non-repudiati
the sender denies sending the message t
private key corresponding to her public key
tested on the plaintext : If the decrypted
is the same as the original message, then
know that the sender has sent the me

Q3 Which two type of key does asymmetric
cryptography use.

Ans Asymmetric key cryptography, also known as publi
cryptography, is a process that uses a pair
related keys - one public key and privat
to encrypt and decrypt a message and
a from unauthorized access

→ A public key is a cryptographic key that can be used by any person to encrypt a message so that it can only be decrypt by the intended receipent with their private key.
A private key also known as a secret key is shared only with key's initiator.

Q.4 What is the role of a CA and a RA? Name the four key access key steps in the creation of a digital certificate?

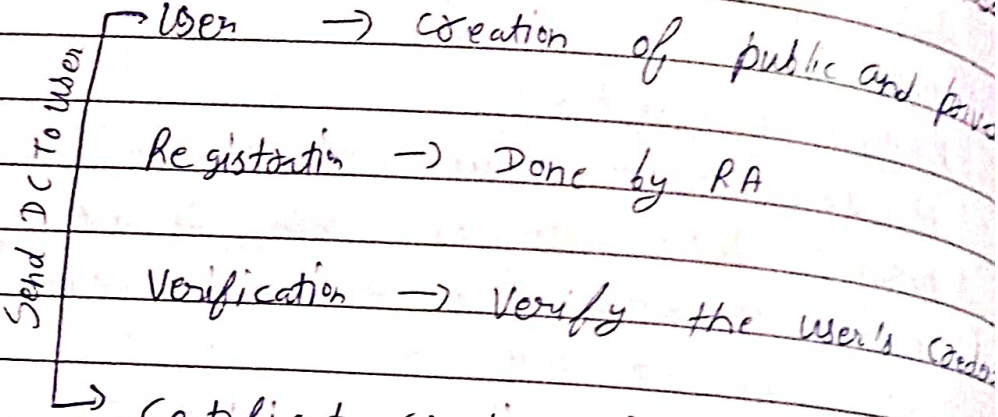
Ans Registration Authority :-
A registration authority is an authority in a network that verifies user request for a digital certificate and tells the certificate authority (CA) to issue it RA are part of a public key infrastructure (PKI), a networked system that enables companies and users to exchange information and money safely and securely.

Certificate Authority :- (CA)
A certificate Authority (CA) is a trusted entity that issues secure Sockets layer (SSL) certificates

Step 1 :- Key generation is done by either user or registration authority. The public key which is generated is sent to the registration authority and private key is kept secret by users.
Step 2 :- In the next step the registraction authority registers the user.

Step3 :- Next step 3 Verification which is registration authority in which the user check that the user who send the public have corresponding private key or not.

Step 4 :- In this step the details and Sent certificate authority by registration a who creates the digital certificate an it to users and also keeps a copy th



Q.5 How do you calculate RSA algorithm.

Ans Let us take an example

→ choose two large prime numbers P and Q
let P=47, Q=17

→ Calculated N = P×Q
we have N = 7×17 = 119

→ choose the public key (i.e. the encryption key) E s
that it is not an element of (P-1) × (Q-1)

→ Let us first (7-1) * (17-1) = 6×16 = 96

→ The factor of 96 are 2, 2, 2, 2, 2 and 3 (because
2×2×2×2×2×3)

→ Therefore it can select E such that one of the
of E is 2 and 3 we cannot choose E as 4 (beca

has 2 as a factor), 15 (because it has 3 as a factor) and 6 (because it has 2 and 3 both as factor)
- let us choose E as 5 (it can have been any other number that does not its factors as 2 and 3)
- choose the private key (this is the decryption key) D including the following equation i.e true.
  $(D \times E) \bmod (P-1)\times(Q-1) = 1$

let us substitute the value of E, P and Q in the equation we have $(D \times 5) \bmod (7-1) \times (17-1) = 1$
that is $(D \times 5) \bmod (96) = 1$
after some calculation, let us take D = 77 the the following is true $(D \times 5) \bmod (96) = 385 \bmod 96 = 1$ which is what we wanted

- For encryption calculated the ciphertext (CT) from the plain text (PT) as follows:
  $CT = PT^E \bmod N$
  let us assume, that we want to encrypt plaintext 10 then we have $CT = 10^5 \bmod 119 = 100000 \bmod 119 = 40$
  Send CT as the cipher text to the receiver
  Send 40 as the cipher text to the receiver
  for decryption. calculate the plaintext (PT) from the cipher text (CT) as follows:
  $PT = CT^D \bmod N$
  it performs the following
  $PT = CT^D \bmod N$
  that is
  $PT = 40^{77} \bmod 119 = 10$, which was the original plaintext of Step 5

Section-D

Q1 What is knapsack encryption algorithm in cryptography

The knapsack encryption algorithm is the first general public key cryptography algorithm it is developed by Ra Merkle and Martin Heltman in 1978 as it is a pu key cryptography it needs two different keys one and other one is private key which is used for Decrypti process in this algo. We will two different process in one is easy and other one is hard the easy knapsac used as the private key and the hard knap is used as the public key. The easy knapsack is u to derived the hard knapsack.

For the easy knapsack, we will choose a super increa knapsack problem.

Q2 Perform encryption and decryption using RSA algorithm the following.

P = 5 ; q = 11 ; e = 17 ; M = 8

Ans $n = P \times q = 7 \times 11 = 77$

$phi(n) = (P-1) \times (q-1) = 6 \times 10 = 60$

$gcd(Phi(d, e) = gcd(60, 17) = 1$

$d * e = 1 \pmod{Phi(n)}$

$d * e \pmod{phi(n)} = 1$

$17 - d \pmod{60} = 1$

$d = 51$

So private key $pu = \{e, n\} = \{17, 77\}$

private key $Pr = \{d, n\} = \{53, 77\}$

- encryption :-

$C = M \uparrow e \pmod{n} = 8 \uparrow 17 \pmod{77} = 57$

- Decryption :-

$M = C \uparrow d \pmod{n}$

Assignment-4

Section - A

Q.1 Digital Certificate Solve the problem of key exchange.
Ans 49

Q.2 The latest Version of X.509 standard is -
Ans

Q.3 A CA has to provide Services of -
Ans

Q.4 A digital certificate associate.
Ans User public key

Q.5 X.509 protocol is used to specify -
Ans It's own private key.

Q.6 The CA Signs a Digital Certificate with -
Ans It's owen private key

Q.7 Requesting for a certificate result into the creation of a file.
Ans

Q.8 The of the User Should never appear in a certificate.
Ans

Q.9 We trust a digital certificate because it contains -
Ans (b) CA's Signature

Q 10 OCSP is -

Ans

Q 11 Which of these systems use timestamps ... date?

Ans (a) Public key certificates

Q 12 Which of them is not a major way of stealing ... information?

Ans (b) Reverse Engineering

Q 13 Which of them is not a proper method for email ...

Ans (d) Click on unknown links to explore.

Q 14 WAP is a ... type of protocol?

Ans (b) Packet Switching

Q 15 Which of the following is not a strong security ...

Ans (c) SMTP

Section-B

Q 1 Define the format of Digital certificate

Ans Digital Certificate

- Owner's Distinguished Name
- Owner's public key
- Owner's CA Distinguished Name
- Issuer's Signature

Q 2 How RA reduce the work load of CA ?

Ans RA verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it.

Q 3 Discuss the step used in creation of digital certificate.

Ans You send a document for signature in three easy steps:
1.) **Upload your document**: into the electronic signature application.
2.) Drag in the signature, text and date fields where the recipient needs to take action.
3.) Click Send: The electronic signature application will email a link to the recipient so they can access the document and sign.

Q 4 Discuss any one mechanism used by a RA for checking the user's proof of possession of the private key.

Ans RA can use open SSL to show proof-of-possession (PoP) of a private key by signing a test file with it. This method works for both RSA and ECC keys.

Q 5 What is the idea behind Certification Authority hierarchy

Ans A CA hierarchy enables you to have a level of segmentation between different use cases for the PKI. This applies both to administration and the role of certificate authority. Separating administration roles allows different people or functions to manage a certificate authority.

Section-C

Q 1 A digital certificate should be self-signed. Explain the cause.

Ans. A self-signed SSL certificate is a digital cert that's not signed by a publicly trusted Certificate Authority (CA). Self-signed certificates are different from traditional CA signed certificates because they are created, issued, and signed by the company or developer who is responsible for the certificate or software associated with the certificate. They are free rather than a CA; they are available at no cost and can be requested easily by any developer. They can be implemented on your own timetable.

Self-signed certificates do not expire or need to be renewed after a set period of time, as is the case by a CA certificate. Although this seems convenient, it is one of the major concerns with this option because they cannot comply with security updates in a timely manner to discovered vulnerabilities, nor meet the certificate agility needed to secure today's modern enterprise. As such, this method of authentication is rarely recommended.

Q. 2 Describe how cross-certification is useful.

Ans A certificate issued from a certificate authority (CA) that signs the public key of another CA within its trust hierarchy that establishes a trust relationship between the two CA's. Cross-certification provide a means to create a chain of trust from a single, trusted, root CA to multiple other CAs

Q 3 What are the common cause for revoking a digital certificate?

Ans: The validity period ends
- The issuing CA has been compromised
- The certificate owner no longer owns the domain for which it was issued.
- The certificate owner has ceased operations entirely
- The original certificate has been replaced with a new certificate from another issuer.

Q 4 What are the broad level differences between CRL, OCSP and SCVP?

Ans ⇒ CRL (Certificate Revocation List) - A CRL is a list of revoked certificate that is downloaded from the certificate Authority (CA)

⇒ OCSP (Online Certificate Status Protocol) - OCSP is a protocol for checking revocation of a single certificate interactively using an online service called an OCSP responder

⇒ Simple Certificate Validation Protocol (SCVP) SCVP Status reporting protocol. it is quite similar to the OCSP

	OCSP	CRL
(1)	OCSP can be used to get the status of a single certificate.	A CRL is a list with multiple lines that has to be downloaded by the browser
(2)	Status of a certificate is fetched by making a request to an OCSP Responder.	A CRL is distributed using a CDP Point which can be an HTTP link or an LDAP server.
(3)	Has less effect on the client and network resources.	Has a big effect on client resource.
(4)	Is the industry standard for certificate Lifecycle management	Used to be the only solution for certificate Lifecycle management.

Q 15 List out the public key cryptography Standards (PKCS) a purpose

Ans

PKCS	Title
-	RSA Cryptography Standard
-	Diffie-Hellman Key Agreement Standard
-	Password-Based cryptography Standard
-	Extended-certificate Syntax standard
-	cryptography Message Syntax Standard
-	Private-key information Syntax Standard
-	Selected object classes and Attribute Types.
-	certificate Request Syntax standard
-	Cryptographic Token Interface Standard
-	Personal Information Exchange Syntax Standard
-	(reserved for ECC)
-	(reserved for pseudo-random number generation)
-	Cryptographic Token Information Syntax Standard.

Section - D

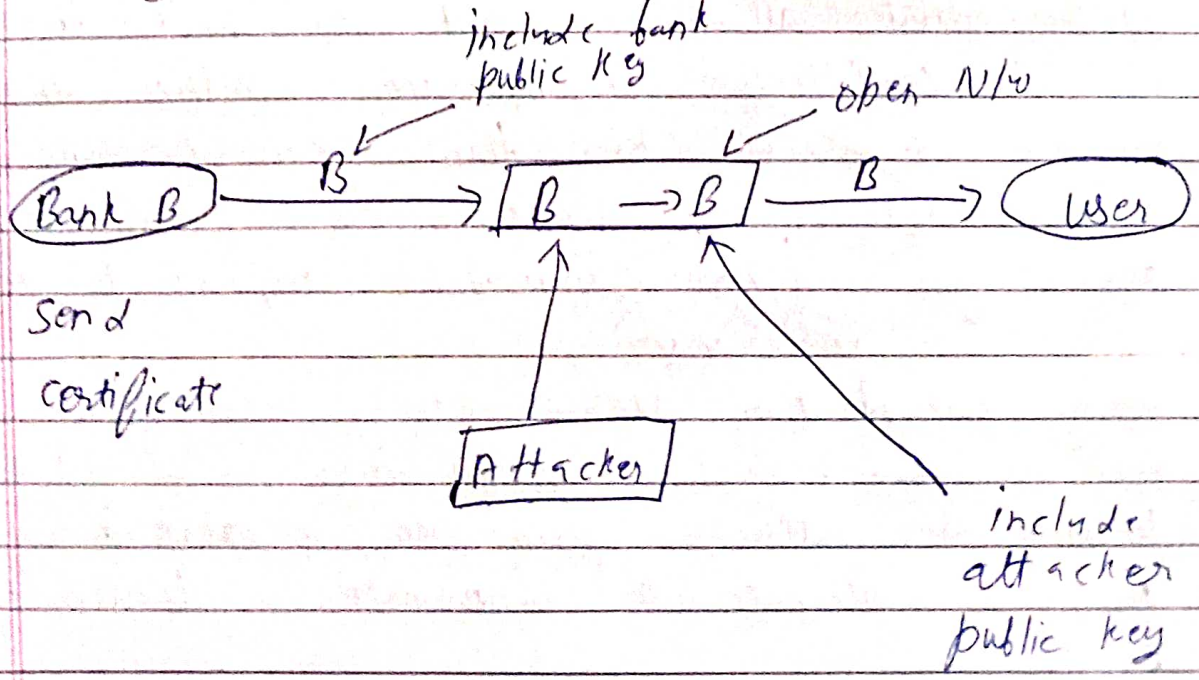
Q 1 Consider a situation: an attacker A creates a puts a genuine organizations name, say bank B and puts the attacker's own public key. You get this certificate from the attacker, without knowing t attacker is sending it. You think it is from bank B. How can this be prevented or resolved?

Ans one way to prevent this type of attack is t use certificate validation when you rece a certificate. certificate validation is the p of verifying that a certificate is genuine a issued by a trusted CA. when you re

a certificate, you can use a certificate validation library or tool to check the certificate against a list of trusted root certificates and ensure that it is valid. this can help you detect if the certificate has been tampered with or issued fraudulently.

other way is to prevent this type of attack is to use public key infrastructure (PKI) to secure your communication. PKI is a system that uses a combination of public and private keys to establish trust and secure communication. When you receive a certificates, you can use the public key in the certificate to verify the identify of the sender and ensure that the communication is secure.

you should also report the issue to the appropriate authorities, such as issuing CA or your organization security team



12 In the other situation, the attacker A cha... bank's genuine certificate B by replacing ... bank's public key in the certificate with ... own. How can this be prevented or resolv...

Ans There are a few ways prevent or resolve ... situation:

1. Certification revocation lists (CRLs): When an SSL certificate is issued, it is added to a CRL ... by the certificate authority (CA), if a certif... compromised or otherwise needs to be revoked ... be added to the CRL, which is checked by ... software when a connection is made to a ... this can help prevent the use of a notif... certificate, as the client will be able to dete... that it has been revoked.

2. Online Certificate Status Protocol (OCSR): OCSR is ... protocol that allows a client to check the s... of a certificate in real-time, rather than ... relying on a CRLs this can provide ... timely detection of compromised certificates ... allows for a more immediate response to rev...

3. Strong authentication: Using strong authentication ... such as two-factor authentication (2FA), ca... prevent an attacker from being able to use ... modified certificate to impersonate a legitimate ... entity.

Assignment-5

Part-A

Q.1 Intellectual Property Rights are an important aspect in International trade. Which of the following is covered under IPR?

Ans All of these

Q.2 On a school computer, Jamie learned how to copy programs. A classmate asked her to copy a program for his home use. Her most ethical response would be which of the following?

Ans I can't copy it because it'll break copyright law.

Q.3 Patent can be granted for . . . ?

Ans Both product and process

Q.4 Government may order the non-advertisement of any patent application in the case of invention related to . . .

Ans Defence technology

Q.5 Patent Act is passed by . .

Ans Central / federal Government

Q.6 Can lecture delivered in the classroom be copyrighted?

Ans Yes

Q.7 In the case of infrigement of patent, the court may award . . .

Ans Damages and account of profits

Q.8 Which of the following is not the infringinent of copyr
Ans To make backup copies

Q.9 Any person who knowingly makes use on a computer of an infringing copy of a computer programme shall be punishable under Section.
Ans Section 66B

Q.10 which of the following protect against software Piracy
Ans ~~Section 66F~~ All of above

Q.11 which Section deals with Cyber terrorism?
Ans Section 66F

Q.12 what is the penalty for destroying computer source code?
Ans

Q.13 Does online sexual harassment come under Cyber stalking?
Ans Yes

Q.14 following are about to credit card "skimming"!
Ans

Q.15 Section 66 C IT Act, 2000 says -
Ans. Whoever by fraudulently or dishonestly use a document which he know to be false shall be punished with the same punishment as forged such document

Part-B

Q.1 Define Pornography.

Ans Pornography (often shortened to porn or porno) is the portrayal of sexual subject matter for the exclusive purpose of sexual arousal. Primarily intended for adults, pornography is presented in a variety of media, including magazines, sex literature, photography, audio, film, animation, and video games.

Q.2 What do you mean by IPR infringement?

Ans Intellectual property infringement is basically using someone else's Intellectual property without the consent of the owner of that Intellectual property.

Q.3 Differentiate between Cyber stacking and Cyber bulling.

Ans Cyber-stalking is an act when an individual tries to gain information about a person like their birthdays, address, pictures of where they have been and who they meet using social media apps without ever meeting them, taking to them or knowing them. Cyber-bullying is an act of harming or harassing an individual or a group by posting insulting remarks, sending threatening messages send by text message or email, spreading damaging rumours, posting embarrassing and private photos and videos on social media sites.

Q. 4 Define Software piracy.

Ans Software piracy is the illegal copying, installing, distribution, or sale of software in any way other than that is expressed in the license agreement.

Q. 5 What are the works conferred under Section 13 of the copyright Act 1957, Copyright protection.

Ans Works conferred under Section 13 of the Copyright Act 1957, Copyright protection are called literacy, dramatic, musical and artistic works and cinematography films and sound recordings from unauthorized use.

Part-C

Q. 1 Explain the remedies for IPR.

Ans • Injunctions: An injunction is the most common remedy for all IPR infringements. Injunctions are court orders that require named individuals to refrain from doing certain specified acts (eg. using the IPR owner's intellectual property).

- Damages or account of profits: Where a profit has been made as a result of the IPR infringement the IPR owner may be entitled to compensation.
- Award of costs: An award of costs is a court order stating that one party has to pay to another party the costs incurred in issuing legal proceedings.

- Delivery and destruction of infringing items: While there is no automatic entitlement to the delivery up or destruction of infringing items.
- Tracing order: The courts may also make tracing orders which order the infringing party to provide information on where they acquired the infringing items.

Q.2 In case of a criminal proceeding in trademark infringement, what types of punishment dictated by the court?

Ans In the case of a criminal proceeding, the court dictates the following punishment.

1. Imprisonment for a period not less than six month that may extend to three years.
2. A fine that is not less than RS. 50,00,000 that may extend to Rs 2 lakh.

Q.3 What are different measures for detecting and preventing credit card fraud?

Ans Here are a few credit card fraud detection tips to follow:

- Review billing statement on your cards carefully every month.
- Look out for suspicious, inconsistencies, inexplicable, and unauthorized transactions.
- Don't use public wi-Fi to make online transaction.

- Don't engage in these transactions in public places.
- Shred all card-related document before discarding them.
- Strengthen passwords and PINs on all cards and related accounts. Always avoid defaults and obvious passwords.

Q.4 To prevent yourself from being the victim of Cyberstalking, what habits you should follows?

Ans- Keep your professional account different from your personal account
- Do not share address, phone number or email id on social media
- Do not post your live location
- Keep the GPS location off of your mobile or other electronic appliances
- Keep your IP address safe with VPN (Virtual Private Network)
- Do not answer unknown people's messages
- check the privacy settings before sharing or posting
- Know the legal remedies
- Keep your passwords and software updated
- Refrain from keeping your private pictures in cloud services.

Q.5 What is the need of Copyright act. How is it useful for consumers?

Ans The copyright Act 1957 protect original literacy, dramatic musical and artistic works and cinematograph films and sound recordings from unauthorized uses. Unlikes the case with patents, copyright protects the expression

and not the idea.
There is no copyright in an idea.
The copyright Act provides an economic right to the author to reproduce the work, to issue copies to the public, to communication it to the public, to make any cinematograph film or sound recording or to make any adaptation or translation of the work.

Part - D

Q.1 Explain economic rights of the author, and moral rights of the author in perspective of copyright protection.

Ans Economic Rights :- The copyright subsists in original literary, dramatic, musical and artistic works, cinematograph films and sound recordings. The authors of copyright in the aforesaid works enjoy economic right u/s 14 of Act.

Moral Right : Section 57 of the Act defines the two basic "moral right" of an author. These are :
(i) The right of paternity
(ii) Right of integrity

The right of paternity refers to the right of an author to claim authorship of work and a right to prevent all from claiming authorship of his work. The right of integrity empowers the author to prevent distortion, mutilation or other alterations of his work, or any other action in relation to said work which would be prejudicial to his honor or reputation.

Q 2 Explain types of trademark infringements.

Ans Direct Infringment :-

Section 29 of the Trademark Act, 1999 lays down the law related to direct infringment of the trademark. As per the law, direct infringment has been defined as in the following cases:

(i) Similar or Deceptive :- falls under direct infringment

(ii) Used without owner's Permission: If the use of a registered trademark has been done without the owner's authorization

(iii) Use of a similar trademark in the same class.

In direct Infringement :-

(i) Vicarious Infringment

(ii) Contributory Infringement