Cryptography PYQ 2024

Q-A

a) What is Denial of Service attack? Done

b) If 40 people need to comm using Symmetric key Cryptography, then findout the no. of Symmetric keys needed.

$\therefore n = 40$, $\therefore$ the no. of keys needed $= {}^{n}C_2$

$= {}^{40}C_2$

$= \left[\frac{n(n-1)}{2}\right]$

$= \frac{40 \times 39}{2}$

$= 780$ keys

c) Difference b/w threats & attacks.

Threats	Attacks
i) defi (Done)	i) defi ~~(done)~~ An actual attempt to breach / exploit a system's security
ii) It is hypothetical (anticipated.	ii) It is real and actionable.
iii) It ~~is intention~~ indicates the possibility of harm.	iii) It carries out the ~~harf~~ harmful action.
iv) It's goal is to identify possible risks.	iv) It's goal is to compromise /disrupt the system.
Eg- Eavesdropping on comm	Eg- Performing a man-in-the-middle attatck.

d) convert the given text "EXAMINATION" into cipher text using monoalphabetic substitution with key=4.

E X A M I N A T I O N
| | | | | | | | | | |
Y C F R N S F Y R T S (C.T)

[Not this, here key = 5]

E X A M I N A T I O N
| | | | | | | | | | |
I B E G M R E X M S R

e) Define stream cipher.

It is a type of symmetric key encryption that encrypts data one bit or byte at a time, using a key stream generated by a pseudorandom no. generator.

G-B

2) Difference b/w monoalphabetic & polyalphabetic ciphers with eg.

eg - Done

Monoalphabetic C.	Polyalphabetic C.
i) It uses a single substitution rule for the entire message.	i) It uses multiple substitution rules during encryption.
ii) The key is single fixed key.	ii) multiple keys or a repeating key pattern here.
iii) one-to-one substitution happens.	iii) One-to-many substitution happens
iv) It's simple	iv) It is complex.
v) Less ~~secure~~ secure.	v) more secure.
vi) Letter freq's remain same.	vi) Letter freq's are more evenly distributed.

3) Explain the algo for generating keys in RSA algo. Perform encryption & decryption using RSA algo for the following, p=7, q=11, e=13, m=8.

a) Done

b) p = 7, q = 11, e = 13, m = 8 (P.T) — This P & P(P.T.) aren't same

~~∴ It can't be as it is a large prime no. (i.e N)~~

$N = p \times q = 7 \times 11 = 77$

~~encryption (C) = $P^e \% N$ = $7^{13} \% 77$ = 0~~

~~decryption (P) = $C^d \% N$ = $0^8 \% 77$ = 0~~

$\phi(N) = (p-1)(q-1) = 6 \times 10 = 60$

$e = 13$, $\gcd(13, 60) = 1$ & $1 < 13 < 60$

∴ co prime to $\phi(N)$

$d \cdot e \bmod \phi(N) = 1 \Rightarrow d \cdot e \equiv 1 \bmod \phi(N)$

this can be written as, $d \cdot e = 1 + k \cdot \phi(N)$

$d \times 13 = 1 + k \cdot 60$

$\Rightarrow d = \frac{1 + 60k}{13}$

k = 0: $d = \frac{1}{13} = 0.\ldots$ ✗

k = 1: $d = \frac{1+60}{13} = \frac{61}{13} = 4.\ldots$ ✗

k = 2: $d = \frac{1+120}{13} = \frac{121}{13} = 9.\ldots$ ✗

k = 3: $d = \frac{1+180}{13} = 13.\ldots$ ✗

k = 4: $d = \frac{1+240}{13} = 18.\ldots$ ✗

k = 5: d = 23. ... ✗

k = 6: d = 27. ... ✗

k = 7: d = 32. ... ✗

k = 8: d = 37 ✓

$\therefore m = 8$ (P.T.) $\rightarrow$ $e = 13$, $d = 37$, $n = 77$

$\therefore C = 8^{13} \% 77 = 0$ (encrypting)

$P = 0^{37} \% 77 = 0$ (decryption)

4) Draw & explain IPsec ESP format. Done

5) Explain DMZ H/W in details with diagram.

6) Define Ceasar cipher with example? Done

7) Differentiate b/w block & stream cipher. Done

Prove that the result of $G^{xy} \bmod N$ is same as the result of $(G^x \bmod N)^y \bmod N$ using $G=7, x=2, y=3$ & $N=11$. Done

$G^{xy} \bmod N$	$(G^x \bmod N)^y \bmod N$
$= 7^{2*3} \% 11$	$= (7^2 \% 11)^3 \% 11$
$= 4$	$= 53 \% 11$
	$= 4$

$\therefore$ Both are same (Proved).

G.C

8) Describe the DES algo with neat diagram & explain steps. Done

9) Explain main in the middle attack with diagram. diagram Done

A man-in-the-middle attack (MITM) is a type of cyber attack where an attacker secretly intercepts & possibly alters the comm b/w two poins who believe they are directly comm with e/o.

10) How TLS is different from SSL? Describe TLS protocal in details. Done

Key differences

SSL	TLS
i) Weaker, outdated.	i) Stronger, current standard
ii) Performence is slower.	ii) Performence is faster.
iii) It's not recommended today.	iii) It's widely used (HTTPS, email).
iv) It is deprecated.	iv) It is actively supported.
v) Less secure	v) More secure

11) Explain various types of active & passive attacks in details. Done

12) Illustrate public key cryptography system with neat diagram.

It's also known as asymmetric encryption. It has 2 keys:

i) Public key - Shared openly, used for encryption.

ii) Private key - Kept secret, used for decryption.

Steps -

i) Key generation - Each user generates a public-private key pair.

ii) Encryption - Bob wants to send a message to Alice. He uses Alice's public key (PK_Alice) to encrypt the message.

iii) Transmission - the encrypted message is sent over the internet.

ii) Decryption - only Alice can Decrypt the message using her private key (sk_Alice).