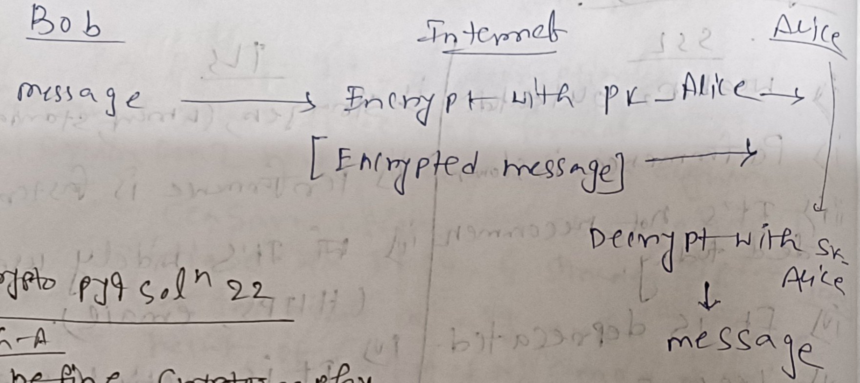
ii) Decryption - only Alice can decrypt the message using her private key (sk-Alice).



Crypto pyq soln 22

Q-A

1) Define Cryptography.

It is a practice of securing info & comm^n through the use of mathematical concepts & algos to convert data into an unreadable format (encryption) & back into a readable format (decryption).

2) Differentiate b/w threats & attacks. Done (pyq 24)

3) What is block cipher?

It's a type of encryption algo that operates on fixed-sized blocks of data (usually 64/128 bits) to produce cipher text.

4) What is nonce? Done

5) What is passive attack? Done

Q-B

1. Encrypt the following message using monoalphabetic substitution with key 4.

TODAY IS MONDAY.

| | | | | | | | | | | | |

X S H E C m W Q S R H E C

2. Describe digital signature. Done

Q-B

3) Explain transportational cipher with eg. Done

It is also called transposition cipher. It is a type of cipher where the positions of the chars in the pt are rearranged acc. to a specific system/key. It has some common egs that are:-

i) Rail fence cipher - It arranges text in a zigzag pattern accross multiple 'rails' & reads it row by row.

ii) Single columnar transposition cipher - It writes text in rows under a keyword & reads it col by col in the order of the keyword's letters.

4) Explain various types of passive attack. Done

5) Explain various types of firewall. Done

6) Explain role of Security Association in IPsec. Done (Add IPSec's dig)

Q-C

1) Explain the RSA algo, perform encryption & decryption to the system with $p=7, q=11, e=17, m=8$.

Done

$N = 7 \times 11 = 77$, $e = 17$, $\phi(N) = 6 \times 10 = 60$

$1 < 17 < 60$ & $\gcd(17, 60) = 1$

$d \cdot e \equiv 1 \mod \phi(N)$

$\Rightarrow d = \dfrac{1 + k \cdot \phi(N)}{e}$

$k=0$, $d = \frac{1}{c} = 0$ — ×

$k=1$, $d = \frac{1+0}{17} = 3$ … ×

$k=2$, $d = \frac{1+120}{17} = 7$ … ×

$k=3$, $d = \frac{1+180}{17} = 10$ — ×

$k=4$, $d = \frac{1+240}{17} = 14$ — ×

$k=5$, $d = 17$ — ×

$k=6$, $d = 21$ — ×

$k=7$, $d = 24$ — ×

$k=8$, $d = 28$ — ×

$k=9$, $d = 31$ — ×

$k=10$, $d = 35$ — ×

$k=11$, $d = 38$ — ×

$k=12$, $d = 42$ — ×

$k=13$, $d = 45$ — ×

$k=15$, $d = 53$ ✓

∴ $d = 53$

∴ encryption, $C = 8^{17} \% 77 = 57$

decryption, $P = 57^{53} \% 77 = 8 (=m)$

2) Describe the DES algo with neat diagram & explain the steps. $\boxed{\text{Done}}$

3) Explain PGP Protocol. $\boxed{\text{Done}}$

4) Write short note on HTTPS, S/MIME & AH Protocol. $\boxed{\text{Done}}$ $\boxed{\text{Done}}$

HTTPS Protocol - It stands for hypertext transfer protocol secure. It is a secure version of HTTP that uses encryption to protect data exchange b/w a web browser & a server.

It ensures confidentiality, integrity & authentication of the transmitted info.

TODAY IS MON

XSHEC MW QSRHEC

2. Describe digital signature. $\boxed{\text{Done}}$