KULVIR SINGH
19BCE2074
CYBERSECURITY DA - 2.

(1) a) 2942 bits

last block data = 2942 mod 1024 = 894

length field = 128 bits

length field + last block data = 894 + 128 = 1022 bits.

∴ Padding required = 1024 − 1022 = $\boxed{\text{2 bits}}$

b) 2943 bits

last block data = 2943 mod 1024 = 895

length field = 128 bits

length field + last block data = 895 + 128 = 1023 bits

∴ Padding required = 1024 − 1023 = $\boxed{\text{1 bit}}$

c) 2944 bits

last block data = 2944 mod 1024 = 896

length field = 128 bits

length field + last block data = 896 + 128 = 1024 bits

∴ Padding required = 1024 − 1024 = $\boxed{\text{0 bits}}$.

(2) a) 2942 bits.

$(1024 \times 3) - 2942$

$= 3072 - 2942$

$= 130$

$\because 130 > 128$

$\therefore$ 130 bit message would require 2 input blocks

b) 2943 bits

$(1024 \times 3) - 2943$

$= 3072 - 2943$

$= 129$

$\because 129 > 128$

$\therefore$ 129 bit message would require 2 input blocks

c) 2944 bits

$(1024 \times 3) - 2944$

$= 3072 - 2944$

$= 128$

$\therefore$ 128 bit message would require 1 input block.

③ $q = 23$

$\alpha = 5.$

Public Key for Bob = $Y_B = 10$

Public key for Alice = $Y_A = 8$

Private Key fro Bob (X_B)

$$Y_B = \alpha^{X_B} \bmod q$$

$$\Rightarrow 10 = 5^{X_B} \bmod 23$$

$$\Rightarrow X_B = 3.$$

Shared Key (k)

$$k = (Y_A)^{X_B} \bmod q$$

$$= (8)^3 \bmod 23$$

$$= 512 \bmod 23$$

$$= 6$$

$$\boxed{\begin{array}{l} X_B = 3 \\ k = 6 \end{array}} \rightarrow \text{Ans.}$$

(4) $p = 881$

$d = 700$

$r = 17$

$M = 400$

$e_1 = 3$ (say)

$e_2 = e_1^{d} \bmod p$

$= 3^{700} \bmod 881$

$= (3^{384} \cdot 3^{192} \cdot 3^{96} \cdot 3^{24} \cdot 3^{4}) \bmod 881$

$= (559 \times 382 \times 826 \times 440) \bmod 881$

$= 471.$

$S_1 = e_1^{M} \bmod p$

$= 3^{17} \bmod 881$

$= (3^{12} \cdot 3^{4} \cdot 3^{1}) \bmod 881$

$= (198 \times 81 \times 3) \bmod 881$

$= 540$

$S_2 = (M - d \times S_1) r^{-1} \bmod (p-1)$

$= (400 - 700 \times 540)(17)^{-1} \bmod (881-1)$

$= (-377600 \times 673) \bmod 880$

$= (-254124800) \bmod 880$

$= 720$

5 a) Planning of Attack

Active and Passive Attacks are security attacks. In Active attack, an attacker tries to modify the content of the messages. Whereas in Passive attack, an attacker observes the messages, copy them and may use them for ~~malicious~~ malicious purposes. Website hacking by getting information about them through their social media sites. Phising attacks to use date of social media. An attack is ~~developed~~ launched when the passwords are cracked and privileges are exploited and trace backs are covered up.

b) Cyber cafe

A cyber cafe is a business which allows people to pay for access to the internet. Most cybercafes provide computers, snacks, and beverages to their customers. These systems can be used to leak out information if you don't log out ~~pro~~ properly. Also some rigged systems can store your data and can be used to hack your account and cause leaking of data. Cyber cafe usage should be very careful and logging off, deleting private data after usage is very important.