Assignment 3

Tasnim Sakib Apon
ID : 20241068

CSE 490
Spring 2021

Tasnim Sakib Apon CSE490

20241068

Theme: Date: / /

□Sat □Sun □Mon □Tue □wed □Thu □Fri

1. Here,

Alice's RSA Public key $(N, c) = (33, 3)$

private key, $d = x$

$M = 19$.

we know,

$$C = M^c \bmod N$$

$$= 19^3 \bmod N$$

$$= 6859 \bmod 33$$

$$= 28 \bmod 33.$$

Alice can decrypt also using

$$M = C^d \bmod N$$

$$= 28^x \bmod 33$$

$$= 13492928512 \bmod 33.$$

$$d = 19 \bmod 33$$

Theme:

Date: / /
☐Sat ☐Sun ☐Mon ☐Tue ☐Wed ☐Thu ☐Fri

3. Let = {1, 2, 4, 10, 20, 40} be the size.

m = 31
n = 110

So, the GK will be

1.31 mod 110 = 31
2.31 mod 110 = 62
4.31 mod 110 = 14
10.31 mod 110 = 90
20.31 mod 110 = 20
40.31 mod 110 = 30

∴ General knapsack : (31, 62, 14, 90, 20, 30).

n = 110.

$m^{-1} \bmod n \rightarrow 31^{-1} \bmod 110$

$\Rightarrow 71$

Encrypt 100100.

31 + 90 = 121

Date: / /
☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Theme:

To decrypt:

$121 \times 21 = 8591 \bmod 110 = 5 = 11$

$11 = 1 + 0 + 0 + 10 + 0 + 0.$

$\therefore$ Obtained plain text = 100100

[Ans]