

# Assignment 3

Tasnim Sakib Apon  
ID : 20241068

CSE 490  
Spring 2021

Tasnim Sakib Apon

CSE490

2024/06/8

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

Theme:

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

private key  $d = 7$

$M = 19$

We know,

$$C = M^e \text{ MOD } N$$

$$= 19^3 \text{ MOD } 33$$

$$= 6859 \text{ MOD } 33$$

$$= 28 \text{ MOD } 33.$$

Alice can decrypt also using

$$M = C^d \text{ MOD } N$$

$$= 28^7 \text{ MOD } 33$$

$$= 13492928512 \text{ MOD } 33.$$

$$\Rightarrow d = 19 \text{ MOD } 33$$

Theme:

Date: / /  
Sat Sun Mon Tue Wed Thu Fri

3. Let  $t = \{1, 2, 4, 10, 20, 30\}$  be the size.

$$m = 31$$

$$n = 110$$

so, the G.E will be

$$1. 31 \bmod 110 = 31$$

$$2. 31 \bmod 110 = 62$$

$$4. 31 \bmod 110 = 14$$

$$10. 31 \bmod 110 = 90$$

$$20. 31 \bmod 110 = 20$$

$$40. 31 \bmod 110 = 30$$

$\therefore$  General Knapsack:  $(31, 62, 14, 90, 20, 30)$ .

$$\cancel{n=110}$$

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

$$\Rightarrow 21$$

Encrypt 100100

$$31 + 20 = 121$$

Date: / /  
 Sat  Sun  Mon  Tue  Wed  Thu  Fri

Theme:

To decrypt:

$$121 \times 21 = 8591 \pmod{110} = S = 11$$

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

$\therefore$  Obtained plain text = 100100

P1 = 011 base 10. A  $\rightarrow$  Ans

00 = 001 base 10. 01

08 = 011 base 10. 02

08 = 011 base 10. 03

(00, 08, 00, 01, 02, 03) : original message

011 = N = 00100

all base 10  $\rightarrow$  a binary no.

100100

001001 + 000001

10100010

