Answer to the Question-01

Given,

$(N, e) = (33, 3)$

$d = 7$

$m = 19$

Here,

Ciphertext, $C = M^{e} \bmod N$

$= 19^{3} \bmod 33$

$= 6859 \bmod 33$

$= 28$

To, decrypt C,

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

$= 28^{7} \bmod 33$

$= 19$

In this way Alice can decrypt C.

Answer to the Question-02

Given,

$\{1, 2, 4, 10, 20, 40\}$ be the SIK

$m = 31$

$n = 110$

To compute General knapsack

$1 \cdot 31 \bmod 110 = 31$

$2 \cdot 31 \bmod 110 = 62$

$4 \cdot 31 \bmod 110 = 14$

$10 \cdot 31 \bmod 110 = 90$

$20 \cdot 31 \bmod 110 = 70$

$40 \cdot 31 \bmod 110 = 30$

GK: $(31, 62, 14, 90, 70, 30)$

To encrypt 100100,

$31 + 0 + 0 + 90 + 0 + 0 = 121$

Here,

$m^{-1} \bmod n = 31^{-1} \bmod 110$
$= 71$

To decrypt,

$121 \cdot 71 \bmod 110 = S$

$S = 11$

$11 = 1 + 10$ ~~(1+00+10)~~

Obtained plain text = 100100

Hence, we obtained the given plain text.