(*) Mention the basic idea of the Merkle-Hellman knapsack algorithm. Assume that the knapsacks $S = [11, 4, 1, 38, 17]$, $w = 13$, $n = 17$ and a binary message -

1100 0010 1110 1010 1110 01011

Compute (i) Hard knapsack (ii) Encrypted message (iii) Decrypted message.

Soln:

(i) Hard knapsack, $H = (S * w) \bmod n$ Home WorkS

$H = [143, 52, 13, 494, 221] \bmod 17$

$H = [7, 1, 13, 1, 0]$ ⟶ (Public key).

(ii) Given,

Binary message = 11000 01011 1001 01010 01011

$H = [7, 1, 13, 1, 0]$

Encryption, $[C = (P * H)]$ cc PH hocche 7

[11000] * H = 8

[01011] * H = 2

[10101] * H = 20

[01110] * H = 15

[01011] * H = 2

∴ C = [8, 2, 20, 15, 2] = ciphertext.

(iii) Decrypted message,

$D = (W^{-1} * C) \bmod n$

$n^{-1} = 19^{-1} \bmod 17 =$

$4 * 8 = 32 \bmod 17 = 15$ [11000]

$4 * 2 = 8 \bmod 17 = 8$ [01011]

$4 * 20 = 80 \bmod 17 = 12$ [01101]

$4 * 15 = 60 \bmod 12 = 9$ [01110]

$4 * 2 = 8 \bmod 17 = 8$ [01011]

(Ans).

stolen.

2018 | 4 | b

Basic idea of Merkle-Hellman knapsack algorithm -

① Take knapsack as private key and (n) and (w).

② Calculate the public key.

$$H = (w * s) \bmod n$$

③ Encrypt the plaintext by using public key.

$$C = P * H.$$

④ Decrypt the ciphertext by using.

$$D = (w^{-1} * C) \bmod n.$$

h:

CamScanner

Sample Math:

RSA Algorithm:

Step 1: $p = 11$

$q = 5$.

RSA modulus, $n = p \times q = 55$

Step 2: $\phi(n) = (p-1)(q-1)$

$= 10 \times 4 = 40$

Step 3: $1 < e < \phi(n)$ & co-prime to $\phi(n)$

3, 7, 9, 11, 13, 17, ...

here, $\boxed{e = 7}$ → encryption key

Step 4: Decryption key:

$de = 1 \bmod \phi(n)$

using extended Eucleadian algo,

Eucledian:

$d \times (7) = 1 \bmod 40$

now, $40 = 5(7) + 5$ → 5 বার

$7 = 1(5) + 2$ → 1 বার

$5 = 2(2) + 1$ → 2 বার

$\Rightarrow 1 = 5 - 2(2)$

$= 5 - 2\{7 - 1(5)\}$

$= 5 - 2(7) + 2(5)$

$$= 3(5) - 2(7)$$

$$= 3\{40 - 5(7)\} - 2(7)$$

$$= 3 \times 40 - 15 \times (7) - 2(7)$$

$$= 3 \times 40 - 17(7)$$

as, encryption key = 7

so, take the co-efficient of 7.

now, $d = -17 \bmod 40$

$= 23 \bmod 40$

$\therefore \boxed{d = 23}$

Step 5:

Private:

$p = 11$

$q = 5$

$\phi(n) = 40$

$d = 23$.

Public:

$n = 55$

$e = 7$.

public key = (55, 7)

private key = (55, 23)

Step 6:

encrypt HIDE

$c = m^e \bmod n$.

now,

H: m = 8, $CT = 8^7 \bmod 55$

$= 2$

I: m = 9, CT = 3

D: m = 4, CT = 49

E: m = 5, CT = 25

(2, 3, 49, 25)

decrypt

$m = c^d \bmod 55$

now,

CT = 2: m = 8 (H)

CT = 3: m = 9 (I)

CT = 49: m = 4 (D)

CT = 25: m = 5 (E)

2015 | 5 | c

Message = CUET

p = 7, q = 11.

Here,

c = 3, U = 21, E = 5, T = 20.

$n = p \times q = 7 \times 11 = 77$

$\phi(n) = (p-1) \times (q-1) = 6 \times 10 = 60.$

Choose, e such that $1 < e < \phi(n)$ and gcd(e, $\phi(n)$) = 1

$\therefore e = 7$

We know,

$de = 1 \bmod \phi(n)$

$\Rightarrow d = \frac{1 + k\phi(n)}{e} = \frac{1 + k \cdot 60}{7} = 43$

Now:

Plaintext: C U E T

Number: 3 21 5 20

Encrypted value ($c = m^e \bmod n$): 31 21 17 17

Again:

Encrypted value: 31 21 17 17

Number: 3 21 5 20

plaintext ($m = c^d \bmod n$): C U E T

$31^{43} \bmod 77$

$= (31)^{20} \times (31)^{20} \times 31^3 \bmod 77$

$= (31^5)^4 \times (31^5)^4 \times 31^3 \bmod 77$

$= (12)^4 \times (12)^4 \times 31^3 \bmod 77$

$= 23 \times 23 \times 69 \bmod 77$

$= 3$

How will you use Fermat's theorem to compute multiplicative inverse of a number? Using Fermat's theorem determine the $5^{-1} \bmod 7$.

Definition:

If p is a prime and a is a positive integer not divisible by p then,

$$a^{p-1} \equiv 1 \bmod p$$

or, $1 \equiv a^{p-1} \bmod p$.

Proof:

$$1, 2, \ldots (p-1) \equiv (a \bmod p, 2a \bmod p, \ldots (p-1)a \bmod p) \bmod p$$

$$\equiv (a, 2a, \ldots (p-1)a) \bmod p$$

$$\equiv (a^{p-1}) 1, 2, \ldots (p-1) \bmod p$$

Cancelling $1, 2, \ldots (p-1)$ on both sides we get,

$$1 \equiv a^{p-1} \bmod p$$

[We can cancel them because $\gcd(1, 2, \ldots (p-1), p) = 1$

Note: $5^{-1} \bmod 9$

We have,

$1 \equiv a^{p-1} \bmod p$

So, it is not possible because 9 is not a prime number.

2014 | 5 | 6

$9^{-1} \bmod 17$

$= 9^{17-2} \bmod 17$

$= 9^{15} \bmod 17$

$= 9^{10} \times 9^{5} \bmod 17$

$= 13 \times 8 \bmod 17$

$= 2$.

2014 | 6 | a

gcd (3615807, 2763323)

~~2763327~~ $= 3615807 = 2763323 \times 1 + 852484$

$2763327 = 852484 \times 3 + 205871$

$852484 = 205871 \times 4 + 29000$

$205871 = 29000 \times 7 + 2871$

$29000 = 2871 \times 10 + 290$

$2871 = 290 \times 9 + 261$

$290 = 261 \times 1 + 29$

$261 = 29 \times 9 + 0$

$\gcd(2763323, 36158.07) = 29.$

2020

1(c)

$d = 113$

$P = 11$

$q = 13$

$e = 17$

Ans:

$n = P * q = 143$

① $M = 5$

Cypher, $C = M^e \bmod n$

$= 5^{17} \bmod 143$

$= ((5^{10} \bmod 143) \cdot (5^7 \bmod 143)) \bmod 143$

$= 135$