Knapsack Cryptosystem (Algorithm)

$$A \longrightarrow B$$

Sender   reciever

[1] KEY GENERATION:

Private Key : $\langle a_1, a_2, \cdots, a_n \rangle \leftarrow$ super increasing sequence

selects a modulus m

selects a multiplier $a < m$ s.t $\gcd(a, m) = 1$

Calculates $a a_i \equiv b_i \bmod m$

publishes a sequence $\langle b_1, b_2, b_3, b_4, b_5 \rangle$ in public directory

$\therefore$ Encryption key is $\langle b_1, b_2, b_3, b_4, b_5 \rangle$

Decryption key is $\langle a_1, a_2, a_3, a_4, a_5 \rangle$

[2] Encryption: A : takes $\langle b_1, b_2, \cdots, b_n \rangle$

Convert the Message into binary equivalent digits and divide this string into blocks of equal size as no of elements in sequence say $\underline{n}$

then ciphertext $C_T = \cancel{c_1 x_1 + c_2} \; c_1 \; c_2 \; c_3 \; c_4 \cdots$

where $c_j = \sum_1^n b_i x_i$, $j = 1, 2, \cdots$

send C_T to B.

[3] Decryption: To read, B does as follows;

B solves $ax \equiv 1 \bmod m$ say $x = c \bmod m$

computes $v_1 = c c_1 \bmod m = c \sum_1 b_i x_i \bmod m$

$= (c b_1 x_1 + c b_2 x_2 + \cdots + c b_n x_n) \bmod m$

$= c(a a_1) x_1 + c(a a_2) x_2 + \cdots + (a c_n x_n) \bmod$

$= ca [a_1 x_1 + \cdots + a_n x_n] \bmod m$

$v_1 = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \bmod m$

find the string in 0,1 for v_1

thus can read the message

continue - - -

now blocks of digits are formed and no of ~~blocks~~ digits in blocks depend on the number of elements in the sequence.

String 00111 00100 01011 01111 10100 10010

$\therefore$ $M \equiv$ ~~010~~ $\boxed{0\,0\,1\,1\,1}$ $\boxed{0\,0\,1\,0\,0}$ $\boxed{0\,1\,0\,1\,1}$ $\boxed{0\,1\,1\,1\,1}$ $\boxed{1\,0\,1\,0\,0}$ $\boxed{1\,0\,0\,1\,0}$

$x_1\ x_2\ x_3\ x_4\ x_5$

→ using the listed public key $\langle b_1, b_2, b_3, b_4, b_5 \rangle$, sender A transforms the successive blocks into

$b_1 \times x_1 + b_2 \times x_2 + b_3 \times x_3 + b_4 \times x_4 + b_5 \times x_5 = V$

$\langle b_1, b_2, b_3, b_4, b_5 \rangle$

$\langle 47, 50, 59, 30, 19 \rangle$

$47\times0 + 50\times0 + 59\times1 + 30\times1 + 19\times1 = 108$

$47\times0 + 50\times0 + 59\times1 + 30\times0 + 19\times0 = 59$

$47\times0 + 50\times0 + 59\times1 + 30\times0 + 19\times1 = 99$

$47\times0 + 50\times1 + 59\times0 + 30\times1 + 19\times1 = 158$

$47\times0 + 50\times1 + 59\times1 + 30\times1 + 19\times1 = 158$

$47\times0 + 50\times1 + 59\times1 + 30\times1 + 19\times0 = 106$

$47\times1 + 50\times0 + 59\times1 + 30\times0 + 19\times0 = 77$

$47\times1 + 50\times0 + 59\times0 + 30\times1 + 19\times0$

thus sender A transcripts the ciphertext 108 59 99 158 106 77 to B

CT: $\underset{C_1}{108}$ $\underset{C_2}{59}$ $\underset{C_3}{99}$ $\underset{C_4}{158}$ $\underset{C_5}{106}$ $\underset{C_6}{77}$

Step 3: To read the message B does as follows:

D
E
C
O
D
I
N
G

(i) solves $44x \equiv 1 \bmod 85$ $\quad (ax \equiv 1 \bmod m)$

$\Rightarrow x \equiv 29 \bmod 85$ (say $x \equiv C$)

$\therefore \boxed{C = 29}$

(ii) $C_i C \bmod 85 \equiv V_i \equiv \Sigma a_i x_i \bmod m$ thus sol^n x_i gives plaintext

$C_1 C \bmod 85 \equiv (108)(29) \bmod 85 \equiv 72 \equiv 3x_1 + 5x_2 + 11x_3 + 20x_4 + 41x_5$

$\therefore x_1 = x_2 = 0,\ x_3 = x_4 = x_5 = 1$ $\boxed{0\,0\,1\,1\,1}$ H

$C_2 C \bmod 85 \equiv (59)(29) \equiv 3x_1 + 5x_2 + 11x_3 + 20x_4 + 41x_5$

$x_1 = 0;\ x_2 = 0,\ x_3 = 1,\ x_4 = 0,\ x_5 = 0$ $\boxed{0\,0\,1\,0\,0}$ E

$\boxed{0\,1\,0\,1\,1}$ L

$\boxed{0\,1\,1\,1\,1}$ P

$\boxed{1\,0\,1\,0\,0}$ U

$\boxed{1\,0\,0\,1\,0}$ S

HELP US

Example: Suppose user of Knapsack cryptosystem wants to be messaged only through using it. what it will do?

User is B and A wants to send a message to B in secure way using Knapsack cryptosystem.

Step I User B selects a superincreasing sequence as its private key say 3, 5, 11, 20, 41 $\langle a_1, a_2, a_3, a_4, a_5 \rangle$

Private Key + Public Key Generation

→ also selects a modulus $m = 85$

multiplier $a = 44 \bmod m$

s.t. $\gcd(a, m) = 1$

→ reduces superincreasing sequence to random sequence by calculating

$$b_i \equiv a a_i \bmod m$$

$\therefore$

$$b_1 = a a_1 \bmod m = (44)(3) \bmod 85 \equiv 47$$
$$b_2 \equiv a a_2 \bmod m \equiv (44)(5) \bmod 85 \equiv 50$$
$$b_3 \equiv a a_3 \bmod m \equiv (44)(11) \bmod 85 \equiv 59$$
$$b_4 \equiv a a_4 \bmod m \equiv (44)(20) \bmod 85 \equiv 30$$
$$b_5 \equiv a a_5 \bmod m \equiv (44)(41) \bmod 85 \equiv 19$$

now user B publishes $\langle b_1, b_2, b_3, b_4, b_5 \rangle$ as public key (encryption key) ~~on~~ in the public directory

Step ② Suppose A wants to send message (Plaintext) to B such as m = HELP US

ENCODING

So A does as follows: A converts it into the string in 0's and 1's

	H	E	L	P	U	S
	↓ 7	4	11	15	20	18
binary equivalent	00111	00100	01011	01111	10100	10010