Math Camp

Public Key Cryptography

Merkle-Hellman Knapsack Algorithm

Based on the subset-sum problem.

Example:
A=(2, 3, 5,10), c = 18

A= (-7, -3, -2, 9000, 5, 8) and c = 0

A= (5, 43, 17, 9, 21, 12) and c=47

A= (295, 592, 301, 14, 28, 353, 120, 236) and c = 1129

Euclidean Algorithm

1. Find the greatest common divisor of 72, 23

2. Find the greatest common divisor of 156, and 61

Definitions

Superincreasing sequence = each element is larger than the sum of all previous elements.

Relatively prime numbers = two numbers with no common factors

X modulo C = divide X by C and take the remainder

Merkle-Hellman Knapsack Algorithm.

Set up:

1. Choose your private key: pick a superincreasing set A of 7 numbers.
2. Choose a random number C that is: larger than the sum of elements of A.
3. Choose a random number R that is relatively prime to C.
4. Construct the public key B: take A x R modulo C.
5. Publish the public key B.

How to Encrypt each letter:

1. Convert letter to binary.
2. Suppose B={b1, b2, b3, b4, b5, b6, b7}, and your letter in binary is n=z1z2z3z4z5z6z7.
3. Take the sum (z1 x b1)+(z2 x b2)+...+(z7 x b7) = m
4. Send m.

Letter	Binary
A	01000001
B	01000010
C	01000011
D	01000100
E	01000101
F	01000110
G	01000111
H	01001000
I	01001001
J	01001010
K	01001011
L	01001100
M	01001101
N	01001110
O	01001111
P	01010000
Q	01010001
R	01010010
S	01010011
T	01010100
U	01010101
V	01010110
W	01010111
X	01011000
Y	01011001
Z	01011010

An Example:

Setting Up Your Private Key

Message to send: MATH
In Binary: 1001101 / 1000001 / 1010100 / 1001000

1. Choose a super increasing sequence of length 7

   A =

2. Pick a number bigger than the sum of elements in A

   C =

3. Pick a number relatively prime to C

   R =

4. Find the remainder when you divide C by R.

5. Write xR+yC=1 for some numbers x and y

Record:
A =

C =

R =

X =

6. Calculate your public key B= A*R , then remainder dividing by C.

Now we can encrypt!

Decryption

We've been sent the cipher

m=_____

We have our private key A=
the number C= _____
and the number R=_____
used to construct the public key B.

1. We have our secret number x =

   The number x modulo C is called the inverse of r modulo C.

2. Calculate the number m' = mx modulo C.

3. Solve subset sum problem for A, m'.

4. Decrypt the message!!!