ALGORITHM PROJECT

Created By:

Vikram Patel :	1200123
Ravi Shankar Bharti :	1200128

Guided By: Dr. Kapil Ahuja

The Knapsack Algorithm and Public Key Cryptography

Project Theme:

Public key cryptography is an asymmetric-key cryptosystem, meaning that two keys are required for communication: a public key and a private key. One key tells us how to encrypt (or code) a message and this is “public” so anyone can use it. The other key allows us to decode (or decrypt) the message. This decryption code is kept secret (or “private”) so only the person who knows the key can decrypt the message.

This problem is based on the subset sum problem , a special case of the knapsack algorithm .Knapsack algorithm is used to generate public and private keys. The public key is a 'hard' knapsack and the private key is an 'easy', or superincreasing knapsack.

Problem Statement:

Given a message or plain text to be encrypted, generate public key and private key using Knapsack Algorithm, to encrypt and decrypt the plain text. Using those keys encode the message into a cyphertext and then private key and cyphertext is sent to the receiver of the message to decode the message.

Approach:

The Algorithm is divided into two parts:

- **Encryption:**

  To encrypt a plain text a easy knapsack S is generated depending on the bit length of the plain text. Randomly two integers 'm' and 'n' such that n > max(S) and m<n , are chosen for converting the easy knapsack into hard knapsack H. Easy knapsack can be converted into hard knapsack by :

  h= (m*s) mod n , where s is element of easy knapsack S and h is element of Hard knapsack.

  The hard knapsack is considered to be public key , Each term in the public key that corresponds to a 1 in the plaintext are added together and the resulting sum is the cyphertext T. This cyphertext is sent to the receiver to decode the message.

- **Decryption:**

  The Tuple(S,m,n) is sent as private key to the receiver and kept secret by the receiver . m and n are used to compute m^{-1} where m^{-1}*m=1 mod n , if n is prime then $m^{-1} = m^{n-2}$ mod n. compute $A=m^{-1}$*T mod n.

  Compute P_i such that Sumof (S_i*P_i) =A ,

  Where P_i can be 0 or 1.

  Write P_1 P_2 P_3 P_4 …

  This is Your Original Decrypted Message.