Public Key Cryptography with Knapsack Systems

Komal Sachdeva

Abstract- The Paper Public Key Cryptography with Knapsack Systems involves the introduction to the Conventional Cryptography describing the concept of Plain Text, Cipher Text, Encryption, Decryption, Keys, Substitution, Transposition, Symmetric Key and Asymmetric Key Systems. The main focus is on Public Key Cryptography and one such technique for the encryption and decryption of the message, Knapsack Systems is discussed in the paper with the mathematical description.

I. INTRODUCTION

Cryptography is the science of protecting transmitted information from unauthorized interception. Cryptography allows storing or transmitting sensitive information across insecure networks, so that the information is read only by the intended recipient. Cryptanalysis is the science of breaking the secret codes and replacing it with some other information.

II. CONVENTIONAL CRYPTOGRAPHY

Conventional cryptography is also called as symmetric key encryption; one key is used for encryption and decryption. Suppose there are two factors who want to communicate with each other over an insecure channel such as internet or a cell phone called as Alice and Bob. And a third person is there by the name Eve who wants to know about the information getting exchanged between Alice and Bob and who is able to see the whole communication and to inject her own messages in the channel. Alice and Bob have access to the key, but Eve does not know anything about the key.

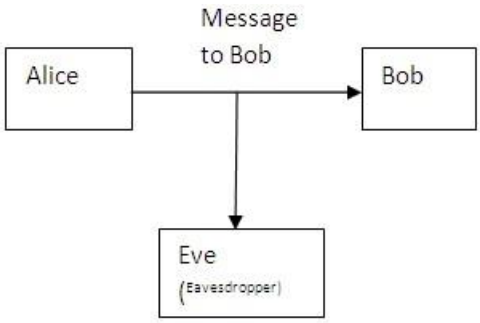

Figure 1 Alice and Bob Communication

III. SOME TERMS DEFINED

The two persons who want to interact with each other are Alice and Bob and the person who is trying to read their message is Eve.

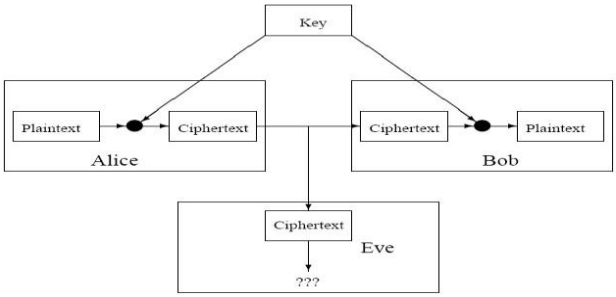

Figure 2: The Setup

The terms in the figure have the following meanings:

1) Plaintext: Knowing the plaintext is equivalent to knowing the original message. The original message has to be translated into some standard form to be encrypted.
2) Cipher text: The message which is transmitted after translation is the cipher text. Alice and Bob assume that the message which Eve will get will be the translated message called as the cipher text.
3) Key: Key varies from transmission to transmission whether it is symmetric key transmission or asymmetric key transmission. Both Alice and Bob must have the information about the key, in order to perform encryption and decryption.
4) Encryption: The process of applying substitutions and transformations on the plaintext.
5) Transposition: The 1 order of the letters in the plaintext is arranged in some systematic way. The key is permutation applied to the positions.
6) Substitution: Individual letters are replaced by different letters in a systematic way. The key is the sequence of applied permutations.
7) Decryption: The process of getting back the original text from the cipher text available by using the same secret key.
8) Symmetric Key Algorithms: The same key is used for both encryption and decryption.
9) Asymmetric or Public Key Systems: When two different keys called as public key and private key or secret key are used for encryption and decryption respectively. We are provided with the initial weights in the knapsack.

- Weights :(2, 3,5, 6, 8, 7, 9)

IV. PUBLIC KEY CRYPTOGRAPHY

Public key cryptography is a system in which there are two keys, one is secret key and another is public key. One key is used for encrypting the plain text, and other decrypts the cipher text. Both the keys cannot perform the same function. One of the key is public and the other is kept as private. Public Key Cryptography is also called as 'Asymmetric Key Cryptography'. The algorithms which are used for Public Key Cryptography are based on mathematical relationships. The algorithms are based on the concept of Digital Signatures of the message which uses the private key and the signature is the verified by using the public key.

Manuscript received December, 2013

Komal Sachdeva, Assistant Professor, Department of Computer Science and Engineering Manav Rachna College of Engineering, Faridabad, India.

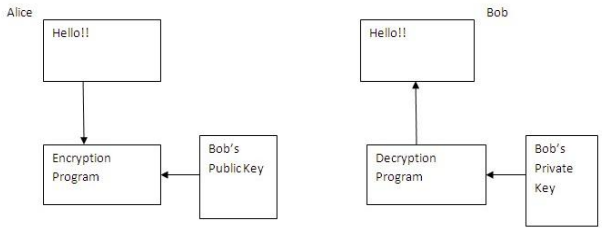

Figure 3

Alice and Bob Communication using Public Key System

Here, the message is encrypted by using the Bob's Public Key when the Alice initialized the process of communication. When the Bob wants to read the message, Bob uses its own Private Key to decrypt the message.

Public Key Cryptography was invented by Whitfield Diffie and Martin Hellman in 1976. So, it is also called as Diffie-Hellman Encryption.

V. MERKLE HELLMAN KNAPSACK CRYPTOSYSTEM:

Merkle Hellman Knapsack Cryptosystem, invented by 'Ralph Merkle' and 'Martin Hellman' in 1978 is one of the earliest Public Key Cryptosystem.

This cryptosystem is based on the "Subset Sum Problem', which is a special case of the knapsack problem and is defined as follows:

Problem

Given a set of numbers S, and a number m, to find a subset of S, which sums to m.

The problem is called as the NP-complete problem. The problem will be solved easily by a simple algorithm like Greedy Algorithm if the each element of the knapsack is greater than the sum of all the numbers before it. Also, called as the super increasing numbers.

E Mathematical Knapsack Problem:

Suppose we are given a set of n weights w0, w1, ... wn-1 and their sum 'Sum' is it possible to find ai {0, 1}, so that

Sum = a0w0+a1w1+ ..... + an-1wn-1

Let us see the problem with the help of an example where

 Problem: To find the weights that sums to Sum=18

Answer: 9+6+3=18

If 'Greedy Algorithm' technique is tried here, according to which, at each stage, if the largest element is put into the knapsack, the results obtained are as follows:

18= 9+8+1,

Which does not give us the solution?

The solution to the problem was given when taken into account the Super Increasing sequence for the weights in the knapsack.

Let us take an example:

W= (1, 3, 7, 15, 31, 63, 127, 255), The sum of the weights is:

∑W= 502

A number is chosen in such a way which is greater than the sum, and call it q, so,

q= 557

Again, a number is chosen from the range defined [1, q) in such a way which is coprime to q is r, such that,

r=323, and is coprime to q Our purpose is to find out the private key here, and this consists of q, w, and r.

The public key, β is calculated multiplying each element of the knapsack by 'r mod q', so the sequence will be:

1*323 mod 557= 323
3*323 mod 557= 412
7*323 mod 557= 33
15*323 mod 557= 389
31*323 mod 557= 544
63*323 mod 557= 297
127*323 mod 557= 360
255*323 mod 557= 486

β= (323, 412, 33, 389, 544, 297, 30, 486)

This sequence makes up the public key.

The Encryption Process:

Suppose 'Alice' wants to encrypt the original message called as the Plaintext. Say the initial message to be encrypted is in the binary form as;

01100101

To encrypt the message, each and every bit of the original message is multiplied by respective number in β. So, if,

a= 01100101, then,

0*323
1*412
1*33
0*389
0*544
1*297
0*30
1*486(412+33+297+486), this sums to be equivalent to 1228

'Alice' sends this to the recipient 'Bob'.

The Decryption Process:

At the receiver end, to decrypt the message,'Bob' multiplies 128 by r-1 mod q.

= Inverse Of (323 mod 557) = 169 1228* 169 mod 557 = 368

Then, the Greedy Algorithm is applied, so that we obtain,:

328 = 255+73=255+63+10= 255+63+7+3,

So that the bit string obtained now is the same as the original text taken into account. i.e.: 01100101

VI. CONCLUSION

The Keys values for Public Key Cryptography based upon the weights in the knapsack is calculated and then by using the Key values the message is first encrypted. The original message is then decrypted by repeating the process in the reverse order.

REFERENCES

1. L.M. Adleman. On breaking the iterated Merkle-Hellman Public Key Cryptosystem, pp. 303-308 in Advances in Cryptology: Proceedings of Crypto 82, D.Chaum, R.L.Rivest and, A.T. Sherman, eds, Plenum Press, 1983
2. "Network Security Essentials", Applications and Standards - Third Edition, -William Stallings.
3. "Security in Computing" Fourth Edition - Charles P. Pfleeger, Shari Lawrence Pfleeger
4. http://en.wikipedia.org/wiki/Merkle%E2%80%93Hellman_knapsack_cryptosystem
5. http://userpages.umbc.edu/~rcampbel/NumbThy/Class/BasicNumbThy.html
6. "Advance Cryptography Algorithm For Improving Data Security ", Volume 2, Issue 1, January 2012, ISSN: 2277 128 X, International Journal of Advanced Research in Computer Science and Software Engineering. - Vishwa Gupta, Gajendra Singh, Ravindra Gupta.
7. "Frame Based Symmetric Key Cryptography",Volume 02, Issue: 04, Pages 762-769(2011), Int. J. Advanced Networking and Applications.- Uttam Kr. Mondal, Satyendra Nath Mandal, J. PalChoudhart, J.K.Mandal