International Journal of Current Research in Science and Technology
Volume 2, Issue 1 (2016), 51–54. (Special Issue)
ISSN: 2394-5745
Available Online: http://ijcrst.in/

International Journal of Current Research in Science and Technology

Improvement of Merkle-Hellman Scheme using RSA Problem

Seminar Paper*

Swati Verma[1]

1 Department of Mathematics, Government V.Y.T. Autonomous PG.College, Durg(C.G.), India.

Abstract: The public key cryptosystem proposed by Merkle and Hellman in 1978 is based on “Knapsack Problem”. In this paper, we demonstrate a polynomial message which have been encrypted through the Merkle-Hellman encryption scheme by using RSA problem. This scheme is more efficient because only proposed receiver is decode the message.

MSC: 94A60, 94B40 68p30.

Keywords: Knapsack problem, super increasing vector, subset sum problem.

1. Introduction

The opinion, of the superincreasing subset problem was coined by Merkle-Hellman in 1978. Ralph Merkle and Martin Hellman used the subset problem to create a cryptosystem to encrypt data. A super-increasing knapsack vector s is created and the super-increasing property is hidden by creating a second vector M by modular multiplication and permutation. The vector M is the public key of the cryptosystem and s is used to decrypt the message. In 1976, Diffie and Hellman [3] introduced the idea of public key cryptography, in which two different key are used: one for encryption, and one for decryption. Each user keeps his decryption key secret, while making the encryption key public, so it can be used by everyone wishing to send message to him. The Merkle Hellman system is based on the subset sum problem. The subset sum problem is a special case of the knapsack problem. The subset sum problem is hard, its decision problem was shown to be NP-complete by Karp [5]. It will be shown that the related search problem of actually finding a solution, even when a solution is known to exist, is at least as hard as any NP complete problem. The subset sum problem is to find a subset of a given set of positive integers $z_1, \ldots, z_n$, such that the elements in the subset sum up to some given integer s.

The knapsack problem is an NP complete problem [5] in combinatorial optimization. The knapsack problem selects the most useful items from a number of items given that the knapsack has a certain capacity. Knapsack problems are widely used to model solutions, industrial problems such as public-key cryptography. The $0-1$ knapsack problem states that if there is a knapsack with a given capacity and a certain number of items that need to be put in the knapsack.The knapsack problem selects the items that can be put in the knapsack so that the value of all items is maximized and the weight does

* *Proceedings : UGC Sponsored National Seminar on `Value and Importance of Mathematical Physics` held on 05.12.2015, organized by Department of Mathematics and Physics, Government Rajeev Lochan College, Rajim, Gariaband (Chhattisgarh), India.*

not increase the total capacity of the knapsack. This can be denoted as

$$Maximize \sum_{i=0}^{n} k_i x_i \tag{1}$$

$$Subject\ to \sum_{i=0}^{n} w_i x_i \leq W \tag{2}$$

$$x_i = \begin{cases} 1,\ if\ the\ item\ is\ included\ in\ the\ knapsack \\ 0, if\ the\ item\ is\ not\ included\ in\ the\ knapsack \end{cases} \tag{3}$$

where, k is the value associated with each item i. w is the weight associated with each item i. W is the maximum capacity of the knapsack. n is the number of items. Ralph Merkle and Martin Hellman used the subset problem to create a cryptosystem to encrypt data. A super-increasing knapsack vector s is created and the super-increasing property is hidden by creating a second vector M by modular multiplication and permutation. The vector M is the public key of the cryptosystem and s is used to decrypt the message [2].

2. Encrypting Messages

The proposed cryptosystem performs encryption in two steps. First the polynomials are converted to their binary equivalent. These polynomials message are encrypted through the Merkle-Hellman encryption scheme whose main idea is to create a subset problem which can be solved easily and then to hide the super-increasing nature by modular multiplication and permutation. Secondly, these encrypted polynomial message are further encrypted though the use of RSA concepts. We choose two prime numbers p and q and calculate n as the product of these two prime numbers, euler's function $ø(n)$ as the result of $(p-1)*(q-1)$. We choose another number e which is relatively prime to the other two prime numbers which we had earlier chosen and gcd $(e$,ø(n)) =1. Using these details we find out the value of d such that d≡ e^{-1} (mod $ø(n)$). This (e, n) acts as the private key and the pair (d, n) acts as the public key. Thus the formula to encrypt the message using discrete logarithmics is C = M^e mod n.

3. Mathematical Explanation

Step 1: The first step is to choose key of length 7 bits. These are used to perform the first encryption process.

Step 2: The second step is to convert the polynomial of the message into binary. The binary sequence is represented by the variable y.

Step 3: Choose a superincreasing sequence of number of positive integers. A superincreasing sequence is one where every number is greater than the sum of all preceding numbers $s = (s_1, s_2, s_3, ...s_n)$.

Step 4: The forth step is to choose a random integer (z) such that

$$z > \sum_{i=0}^{n} s_i \tag{4}$$

and a random integer r, such that $gcd(z, r) = 1$ where r and z are coprime.The sequence s and the numbers z and r be the private key of the cryptosystem. All the elements $s_1, s_2, s_3, ...s_n$ of the sequence s are multiplied with the number r and the modulus of the multiple is taken by dividing with the number z. Now calculate the sequence $k = (k_1, k_2............k_n)$, where

$$k_i = r * s_i\ mod\ z \tag{5}$$

The public key is k and private key is (r,z,s).

Step 5: The message is encrypted by multiplying all the elements of sequence k_i with the corresponding elements of sequence y_i, where y_i is the i-th bit of the message and $y_i \in \{0, 1\}$. The numbers are then added to create the encrypted message M_i forms the cipher text of the cryptosystem. Therefore,

$$M_i = \sum_{i=0}^{n} k_i * y_i \tag{6}$$

3.1. Example

Encrypting the message $X^6 + X^5 + X^2 + X + 1$.

Step 1: The first step is to convert the polynomial in binary equivalent $x^6 + x^5 + x^4 = 1\ 1\ 0\ 0\ 1\ 1\ 1$

Step 2: The second step is to choose a super-increasing sequence s is created $s =$ (3, 5, 15, 25, 54, 110, 225). This problem is easy because s is a super-increasing sequence.

Step 3: The binary sequence is $y = (y_1, y_2, y_3.....y_n)$, choose a number z that is greater than the sum of all superincreasing sequence then $z = 439$ and choose a number r that is in the range $[1, z)$ where $r = 10$. The private key consists of z, s and r.To calculate a public key, generate the sequence k by multiplying each element in s by r mod z; $k =$ (30, 50, 150, 250, 101, 222, 55) because

k_1 = 3* 10 mod 439 = 30

k_2 = 5 * 10 mod 439 = 50

k_3 = 15 * 10 mod 439 = 150

k_4 = 25* 10 mod 439 =250

k_5 = 54 * 10 mod 439 = 101

k_6 = 110 * 10 mod 439 = 222

k_7 = 225 * 10 mod 439 = 55

where the sequence k is a public key.

Step 4: The message is encrypted by multiplying all the elements of sequence k with the corresponding elements of sequence y and adding the resulting sum. Therefore, the encrypted message is

$$M = \sum_{i=0}^{n} k_i * y_i \tag{7}$$

Encrypting the message $x^6 + x^5 + x^4$. Its binary equivalent is 1 1 0 0 1 1 1, where $k =$ (30, 50, 150, 250, 101, 222, 55) and y =(1 1 0 0 1 1 1). Then, M = 30+ 50 + 101 + 222 + 55 = 458.

Step 5: This is encrypted using RSA concepts. Here the prime numbers chosen are 53 and 31. The value of e is chosen as 7. Therefore d becomes 223. The value of n is the product of the two relatively prime integers. Thus here n = 1643. Thus the message is encrypted according to the formula, C = M^e mod n. Where, (e, n) be private keys. Thus the encrypted code for the first character becomes $C_g = 458^7$ mod 1643 = 344.

4. Decrypting Messages

During the decryption process, the blocks of encrypted code are separated. On these blocks decryption is performed using the RSA concepts. The formula used is

$$M = C^d mod\ n \tag{8}$$

The values of the prime numbers, e, d and n are same as that used during encryption. The output of it is decrypted using Merkle-Hellman Knapsack cryptosystem decryption process.

4.1. Mathematical Explanation

To decrypt the message M, the recipient of the message would have to find the bitstream which satisfies the Equation [1]

$$M = \sum_{i=0}^{n} k_i * y_i \tag{9}$$

The first step is to calculate the modular multiplicative inverse of 'r' in r mod z [3].This is calculated using the Extended Euclidean algorithm. This is denoted by r^{-1}. The second step is to multiply each element of the encrypted message (M) with r^{-1} mod z . Since r was chosen such that gcd(r,z)=1. The largest number in the set which is smaller than the resulting number is subtracted from the number. This continues untill the number is reduced to zero [4].

4.2. Example

Step 1: Decrypting the message: C= 0344

Step 2: Decrypting encrypted code. Perform the decryption process on C=0344 using the concepts of RSA. Thus, the prime numbers chosen were 53 and 31. The value of e was chosen as 7. Therefore d becomes 223. The value of n is the product of the two relatively prime integers.Thus here n = 1643. Thus the message is encrypted according to the formula, M= C^dmod n. Thus M = 344^{223} mod 1643 =458.

Step 3: The modular inverse of 10 in 10 mod 439 is calculated using the extended Euclidean algorithms and was found out to be 44.

Step 4: The encrypted message M is 458 and s = (3, 5, 15, 25, 54, 110, 225). Again, $458 * 44$ mod $439 = 397$. Now decompose 15 by selecting the largest element in s which is less than or equal to 15. Then selecting the next largest element less than or equal to the difference, until the difference is 0. 397-225 = 172; 172-110 = 62; 8-5= 3; 3-3=0. Thus, the binary sequence becomes 1 1 0 0 1 1 1. The polynomial equivalent to this binary sequence is $x^6 + x^5 + x^2 + x + 1$.

5. Conclusion

This paper explain how to encrypt and decrypt data by the working of Merkle Hellman Knapsack cryptosystem through the use of RSA concepts. The whole cryptosystem was demonstrated by encrypted a polynomial "$X^6 + x^5 + x^4$" and then decrypting it. The decrypted polynomial message matched the original polynomial message.

References

[1] M.Hellman and R.Merkle, *Hiding information and signatures in trapdoor knapsacks*, IEEE Trans. Inform. Theory, 24(1978), 525-530.

[2] A.Menezes, P.Vanoorschot and S.Vanstone, *Handbook of Applied Cryptography*, CRC Press, (1996).

[3] W.Diffie and M.Hellman, *New directions in cryptography*, IEEE Trans. Inform. Theory, 22(1976), 644-654.

[4] Ashish Agarwal, *Encrypting Message using the Merkle Hellman Knapsack Cryptosystem*, International Journal of Computer Science and Network Security, 11(2011), 12-14.

[5] Richard M.Karp, *Reducibility among combinatorial problems in Complexity of Computer Computations*, Raymond E. Miller and James W. Thatcher (eds.) Plenum Press, NY, (1972).