Odd-Even Based Cryptography

Keerthi Kamal Adusumilli, *Member, IAENG*

***Abstract*— every character is represented as a number, which is either odd or even; they are to be encrypted differently. This paper describes how such an odd-even based encryption is applied, and how this approach makes a Cryptanalyst's job much tougher.**

Index Terms— **complexity, cryptography, number theory, substitution**

I. Introduction

This paper presents an approach of odd-even based cryptography which implies encryption to be applied must be different for the odd and even numbers present in the plain text. This paper describes one such application of Mono alphabetic substitution. In Mono alphabetic substitution, a character in the plain text is always changed to the same character in the cipher text regardless of its position in the text. In this approach the encryption is simply adding the key to the plain text number to get the cipher text number while decryption is subtracting the key from the cipher text number to get the plain text, normally a crypt-analyst can easily find out key but in this odd-even approach a combination of two numbers is used for encryption.

II. Application

In this method two different even numbers are chosen say *k1* and *k2* and the number representing the character is tested for evenness if it is an even *k1* is added to the number and if it is not even then definitely its an odd number and *k2* is added to it.

Odd numbers when added with an even number results in an odd number, in the same way an even number added with even number results in an even number.

On the decrypting side each number is tested for evenness if it is even *k1* is subtracted otherwise *k2* is subtracted.

The Shared key is a pair of numbers (*k1, k2*).

The Sender uses the following algorithm to encrypt the message:

If P mod 2 =0

Then $C = P + k1$

Else $C = P + k2$

In this algorithm, P is the plain text, which is represented as a number; C is the number that represents the cipher text. The two numbers *k1* and *k2* are components of the shared key. Plain text P is added to the *k1* if P is an even number else P is added to the *k2*. The mod term indicates that the remainder obtained by dividing the P with 2 is used for judging evenness.

The receiver uses the following algorithm to decrypt the message:

If C mod 2 =0

Then $P = C - k1$

Else $P = C - k2$

In this algorithm P and C are the same as before. The two numbers are components of the same shared key.

Imagine that the shared key is the pair (4, 12). The sender needs to send the character F. This character can be represented as number 6(F is the sixth character in the alphabet). The encryption algorithm calculates 6 mod 2 as 0 so C=6+4=10. This number is sent to the receiver as the cipher text. The receiver uses the decryption algorithm to

Keerthi Kamal Adusumilli is a 3rd year Integrated Post Graduate Student at ABV-Indian Institute of Information Technology & Management, Gwalior, India 474010(phone: +91-9893317446; fax: +91-751-2460313; e-mail:akkamal@gmail.com).

calculates 10 mod 2 as 0 so P=10-4=6(the original number). The number 6 is then interpreted as F.

If the sender needs to send the character M with the same shared key. This character can be represented as number 13(M is the thirteenth character in the alphabet). The encryption algorithm calculates 13 mod 2 as 1 so C=13+12=25. This number is sent to the receiver as the cipher text. The receiver uses the decryption algorithm to calculates 25 mod 2 as 1 so P=25-12=13(the original number). The number 13 is then interpreted as M.

III. BACKGROUND

In the given approach the odd & even numbers representing the plain text are treated differently. The two numbers should be chosen such that the range of encrypted odd numbers and the range of encrypted even numbers do not overlap.

We know that sum of two even numbers is an even number and sum of an even number and an odd number is an odd number making use of this axioms the two numbers chosen need to be either odd or even.

If two odd numbers are chosen the odd and even numbers representing the plain text gets converted to even and odd numbers respectively so decrypting algorithm becomes little bit tricky, not suitable for hard ware encryption. If even numbers are chosen, the odd and even numbers representing the plain text remains as such. i.e.: when the plain text is added with even numbers, odd remains odd and even remains even so the decrypting algorithm is just reverse.

IV. SECURITY ISSUES

There is nothing common in between the two numbers other than both the numbers are even and if one number is known to the adversary he cannot deduce the other number.

For an adversary to apply the brute force approach, he needs to know of the possible combinations of the two numbers. By taking the C long integer (on 64-bit machines) as 64 bits, so each number is 64 bits long and for trying if we fix one number the other number can have 2^63 (an even number will have its LSB 0) possibilities but the first number can be any one of 2^63 possibilities there by the number of possible alternatives becomes

$$2^{63} * 2^{63} = 2^{126}$$

Trying possible alternatives is not worthy.

If text analysis is to be done all the odd numbers and even numbers in the cipher text are categorized into two groups i.e., odd and even. In this approach the whole character range is to be considered, for every combination in one group we have to check all the combinations in the other group so further increasing the possibilities to a greater extent.

V. COMPARISION TO SUBSTITUTION

Substitution and this odd-even based cryptographic application have common conceptions like symmetric key and the decryption algorithms are the reverse of the encryption algorithms.

In our odd-even based cryptographic application there are two encryptions that do not occur cascaded but occur on the basis of evenness of numbers in the same way if we have 2 encryptions (multiple encryption) using substitution method the resulted cipher is equivalent to single substitution with another number i.e., if $key1$ is 2 and $key2$ is 4 then the resultant cipher can also be obtained by having a single encryption with key3 as 6 which is $key1 + key2$.

VI. CONCLUSION

Though the cipher text can be broken, this odd-even based cryptography differentiates the encryption scheme to be applied based on the evenness of numbers. Future work includes

applying the same approach for contemporary encryption methods by carefully choosing the keys so as the cipher text spaces do not overlap.

ACKNOWLEDGMENT

Keerthi kamal Adusumilli thanks his professor G.K.Sharma and his mentor Prashant Singh.

.

REFERENCES

[1] Forouzan, Behrouz A, “Data Communications and Networking”, third edition, Tata McGraw-Hill Edition 2004, ISBN: 0-07-058408-7.

[2] Schneier Bruce,”Applied Cryptography” second Edition:protocols,algorithms and source code in C, John Wiley& Sons, ISBN: 9971-51-348-X.

[3] Song Y Yan,”Number Theory for Computing” Springer, 10 June 2002, ISBN: 35430725, P 1-12.

[4] Andrew S.Tanenbaum,”Computer Networks”, Fourth edition,Pearson Education,2003,ISBN:81-7808-785-5.