New Method in Encryption

Enas Y.Abdullah
University of Kufa, Education College for Girls, Math. Dep.
Najaf, Iraq
Email: inasy.abdullah@uokufa.edu.iq

Abstract

Encryption in this paper includes the use of three values which they are the two shadows values of a base value, and the base value is attained from the three shadows values . Encryption based on two keys was proposed to increase the security of single encryption. We introduce a novel combination of asymmetric (two public –key) and symmetric (private-key). Public key and private key involves odd and even whole values (first shadow value , second shadow value and third shadow value) . shadows values are multiplied making a product value and the value of 1 is subtracted from the produce value, The base value is along with the chosen shadows values ,then we employ values to find public key to encrypt message and private key to decrypt the encrypted message , as well as introduce new ideal to conclude the private key from the public key in two method ,first method determine the values agreed on some of them between the sender and the recipient . Second raised prime number to different value.

Key words: Encryption, shadows value, public key, private key

1. Introduction :

Encryption is a method for a user to securely share data over an insecure network or storage site. Encryption is most used among transactions over insecure channels of communication ,such as the internet ,also used to protect data being transferred between devices such as automatic teller machines ,mobile telephones, and many more [3]. 4000 years ago ,the Egyptians used hieroglyphic symbols to confuse the reader and this is believed to be the first attempt at cryptography [9]. Several other civilization have also been found to have used cryptography technique.

Before the advent of public key cryptography , a widely held view was that for two users to communicate data confidentially they would need to a priori establish a mutually held secret key k [2].While this might be acceptable for some small or tightly knit organizations, such a solution was clearly infeasible for larger networks such as today internet consisting of billions of users.[1]

Every encryption method provides an encryption algorithm E and a decryption algorithm D. In classical encryption schemes, both algorithms depend on the same secret key k. This key k is used for both encryption and decryption . These encryption methods are therefore called symmetric . [3] Public –key encryption is a so - called one - way function with a trapdoor , anyone can easily encrypt a plaintext using the
the plaintext from the cipher text ,without knowing the secret key . Public – key encryption methods require more complex computations and are less efficient than classical symmetric method .Thus symmetric methods are used for the encryption of large amounts of data.

Diffie and Hellman [6,7] put forth a radically new idea in the concept of public key cryptography ,where iwo parties can securely communicate with each other without having an a prior mutual secret –radically challenging the conventional wisdom of the time.

In 1992 ,Bellovin and Merritt [5] proposed the Encrypted Key Exchange (EKE) family of key exchange protocols ,which allow people to use easy- to- remember (and therefore intrinsically weak) passwords without being threatened by dictionary attacks [4]

2.Notation :The following notation is used through this paper

S_a	first shadow	
S_b	second shadow	public key
S_c	third shadow	private key
M	Message	
e_1	encrypted	
e_2	encrypted	

d_1	decrypted
d_2	Decrypted

3.Shadow numbers

The suggested solution in this research uses any kind of positive or negative for each values and not necessarily being prime numbers, consequently making the encryption easy of use by simply randomly generating the three shadow values Therefore using the created three shadows values to derive a base value. And finally using two of the shadow value with the base value as the public encryption key, and the other shadow value with the base value as private encryption key .

In expression to use the shadow system ,a three shadows values are necessary and they may be any positive or negative each value and even ,odd and prime numbers After the three chosen values are multiplied ,a product is derived and twice the value of 2 is subtracted from the product ,a first base value is obtained .

The first and second shadow values may be each value that is greater than 1 and are may be even ,odd and prime number.The thrid shadow value may be any positive and negitive each value that is greater than 2,and are may be even ,odd and prime number .One the first shadow value and twice the second shadow value are multiplied by the thrid shadow value ,a product value is obtained. After reproduction value is obtained and the vlue of 1 is deducted from the product value , a first base value is

The base value may be the gained first base value or any other value that it can be divided with and creting a positive quotient value and zero for the remainder .In case the first base value is divisible by any other value,then the divisor value that is used in the division of the first base value and the quotient value of the division ,are also basees values.

4.First example

Public key and private key is used in the encryption and decryption ,we had three case introduce in each case diversify into a number public key and private key.

1.Case one(Three even shadow values)

Let s choose three shadow positive and negative even values $S_a = -6, S_b = 4, S_c = -10$. Assume that in this case we have two public key (S_a, S_b) and one private key .Now we find base value through applying the following equation:

$$B = (S_a . S_b . S_c) - 1 \qquad (1)$$

$$B = (-6.4.-10) - 1 \qquad (2)$$

$$B = 239 \qquad (3)$$

Therefore message to encrypt be $M = 238$

To obtain on the encryption through applying the following equations:

$$e_1 = (M.S_a)\ mod\ B \rightarrow\ e_1 = (238.-6) mod\ 239\ =\ 6 \qquad (4)$$

$$e_2 = (e_1.S_b)\ mod\ B\ \rightarrow\ e_2 = (6.4) mod\ 239\ = 24 \qquad (5)$$

Finally depended on above results, we find decryption from following equations:

$$d = (e_2.S_c)\ mod\ B \rightarrow\ e_1 = (24.-10) mod\ 239\ =\ 238 \qquad (6)$$

2.Case two (Three odd shadow values)

Let choose three shadow positive and negative odd values $S_a = -2, S_b = -3, S_c = 5$. Assume that in this case we have one public key (S_a) and two private key .Now we find base value through applying the equation (1):

$$B = (-2.-3.5) - 1 \ \rightarrow B = 29 \qquad (7)$$

Therefore message to encrypt be $M = 28$

To obtain on the encryption through applying the following equations:

$$e_1 = (M.S_a) \ mod \ B \rightarrow \ e_1 = (28.-2) mod \ 29 \ = 2 \qquad (8)$$

Finally depended on above results, we find decryption from following equations:

$$d_1 = (e_1.S_b) \ mod \ B \rightarrow \ d_1 = (27.-3) mod \ 29 \ = \ 23 \qquad (9)$$

$$d_2 = (d_1.S_c) \ mod \ B \rightarrow \ d_2 = (23.5) mod \ 29 \ = \ 28 \qquad (10)$$

3. Case three (Three shadow values be odd and even)

In this case shadow value consist of positive ,negative ,odd and even values,

where public key be $S_a = 2, S_b = -11$, and private key be $S_c = -61$, through

applying the equation(1) base value is $B = 1341$,conclusion message to encrypt be

$M = 1340$ and applying the equations (4) and (5) it found encryption be $e_1 = 1339$

$e_2 = 22$,depended on above results decryption be $d = 1340$.

4.Second example (Exponentiation+ addition)

The solution is separated into two parts ,first part is based on add the base value to the three shadows values . Then we raise three shadows values and base value to any value ,assume that 2 ,shadow value and base value show that in following table

Table (1) :show that three shadow value and base value after raised

N.	Base value	Shadow values	Raised to value 2
1	71	77	$S_{ar} = 5929$
2	71	75	$S_{br} = 5625$
3	71	74	$S_{cr} = 5476$
4	71		B_r =5041

Public key is the raised first shadow value and the raised base value ,to find new public key one ,we take the modulus between the first shadow and the base value

5929 mod 5041= 888

The new Public key is : $S_{ar} = 888$ and B_r =5041

Public key two is the raised second shadow and the raised base value ,to find new public key ,we take the modulus between the second shadow and the base value

5625 mod 5041= 584

The new Public key is: $S_{br} = 584$ and B_r =5041

Private key is the raised third shadow value $S_{cr} = 5476$ and the original base value $B = 71$,to find new private key ,we take the modulus between the third shadow and original base value .

547 mod 71 = 9

The new private key is: :S_{cr}= 9 and B =71.

The part second in this solution is depended on multiply the base value 71 by any value of shadow value it is chosen 6 ,the result 426 . we will add 426 to each : the public key one, public key two and raised base, as it is shown in the following table

Table (2) :show that three shadow value and base value after raised

N.	Public key + new value	Raised base value+ new value
1	$S_{ara} = 426 + 888 = 1314$	B_{ra}= 426+5041= 5467
2	S_{brb} = 426+ 584 =1010	

Now we may proceed and perform encryption and decryption with the new derived shadow s values and base value using similar equations

message to encrypt be $M = 70$

First public key is $S_{ara} = 1314$ and base value B_{ra}= 5467 .The encryption is performed with equation (11)

$$e = (M.S_{ara}) mod B_{ra} \rightarrow (1314 * 70) mod\ 5467 = 4508 \qquad (11)$$

Second public key is$S_{brb} = 1010$ and base value B_{ra}= 5467 .The encryption is performed with equation (12)

$e_1 = (e.S_{br}) mod\ B_r \ \rightarrow \ (4508 * 1010\ ) mod\ \ 5467 = 4536$ (12)

Private key is $S_{cr} = 9$ original base $B = 71$.The decryption is finished with equation (13):

$d = (e_1.S_{cr}) mod\ B_r \ \rightarrow \ (4536 * 9\ ) mod\ 71 = 70$ (13)

5. The methods of extraction the private key

It was introduced new methods can determined many of parameter such as private key second public key through it depended on message to encrypt and public key .

(The method of extraction the Second public keye_1 private key d)

This method is based on the prime number 2 raised to n where n = 3,4,5,…….

it chosen n start with 3 since it used three shadow value to evolution encryption

This method is distinguished from others that shadow value are equally when n=3

Through it is determined parameters following

first: it was evaluated two public key e_1 depended on message to encrypt M,

through following formula :

$$e_1 = \frac{M}{2} \qquad (14)$$

Second : determine three shadow value S_C depended on message to encrypt and two

public key through following formula:

$$S_C = \frac{M}{e_1} \qquad (15)$$

Third: determine private key d depended on two public key through following by the following formula:

$d = e_1 * 2$

Table (3) show that values two public key and private key

2^n	M	e	e_1	d
2^3	6	5	3	6
2^5	30	23	15	30
2^6	62	55	31	62
2^7	126	119	63	126
2^9	510	495	255	510
2^{13}	8190	8127	4095	8190

6.Conclusion :

In this paper ,introduce three shadow value where it chosen odd , even, positive and negative number ,encryption have been calculated using two public key consist of (first shadow value and second shadow value) while decryption have been calculated using one private key (three shadow value) ,although this method kept secret except she is required long time .So we made new method proposed conclusion private key depended on public key ,this method become more complexity and difficulty of encryption than previous method ,another new method we obtain second public key by knowing message to encrypt. Finally ,The research in this field is still in process and the efforts to find even more secure and optimized is still in the run

.

REFERENCES

[1] Craig Gentry " Practical identity –based encryption without random oracles In EUROCRYPT, pages 445-464,2006.

[2] Dan Boneh , Amit Sahai and Brent Waters " Function Encryption :Definition and Challenges ".AFOSR, pages 1-23,2006.

[3] Merkle R C, "Secrecy ,Authentication and Public Key Systems" UMI Research Press: pages 104 ,1982

[4] Robert Morris and Ken Thompson "Password security :A case history "Communications of the ACM ,pages 594-597,1979.

[5] Steven M. Bellovin and Michacl Merrit, "Encrypted key exchange : Password – based protocols secure against dictionary attacks" in Proceedings of the IEEE Symposium on Research in Security and Privacy ,pages 72-84,1992.

[6] Whitfield Diffie and Martin E. Hellman "Multiuser cryptographic techniques. In AFIPS National computer Conference ,pages 109-112,1976.

[7] Whitfield Diffie and Martin E. Hellman " New directions in cryptography" .IEEE Transactions on Information Theory, pages 644-654,1976.