Ministry of Higher Education and
Scientific Research
University of Babylon / College of
Education for Pure Sciences
Department of Mathematics

Hybrid Public key Method

This research is submitted to the University of Babylon / College of Education for Morphological Sciences, Department of Mathematics as part of the requirements for obtaining a bachelor's degree in mathematics

By

Naba Raad Kathem

Supervisor

Prof. Ameer A.J. Al-Swidi

بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

فَتَعَالَى اللَّهُ الْمَلِكُ الْحَقُّ ۗ وَلَا تَعْجَلْ بِالْقُرْآنِ مِن قَبْلِ أَن يُقْضَىٰ إِلَيْكَ
وَحْيُهُ ۖ وَقُل رَّبِّ زِدْنِي عِلْمًا

صدق الله العلي العظيم

سورة طه ايه ١١٤

الإهداء

الى من أحمل أسمه بكل أفتخار....والدي

إلى من كان دعاؤها سرنجاحي وحنانها بلسم جراحي......أمي

إلى من كان حاضرا في كل مكان

المهدي صاحب العصر والزمان عجل الله فرجه الشريف وسهل مخرجه

الشكر والتقدير

بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ الحمد الله رب العالمين الذي وفقنا وأعاننا على إنهاء هذا البحث والخروج به بهذه الصورة المتكامل فبالامس القريب بدئنا مسيرتنا التعليمية ونحن نتحسس الطريق برحبه وإرتباك فرئينا المسيرة العلمية هدفا ساميا وحبا وغايه تستحق السير لاجلها وإن بحثنا يحمل في طياته طموح شباب يحلمون أن تكون أمتهم العربيه شامخة بين الامم وإنطلاقا من مبدأ من لايشكر الناس لايشكر الخالق فإننا نتوجه بالشكر للأستاذ (أمير السويدي) التي رافقتنا في مسيرتنا لإنجازهذا البحث وكانت لها بصمات واضحة من خلال توجيهاتها والدعم الاكاديمي كما و نشكر عائلاتنا التي صبرت وتحملت معنا ورفدتنا بالكثير من الدعم على جميع الاصعده ونشكر الاصدقاء والاحباب وكل من قدم لنا الدعم المادي والمعنوي

Abstract

In this research, we hybrid between the some methods of ciphers, in the first between vigenere and pohlig-Hellman second between Beaufort and pohlig-Hellman and the last between vigenere and Rivest-shamir adleman which give more complexity from the analysis and clacker's from the unknoon person's (Hacker's)

Contents

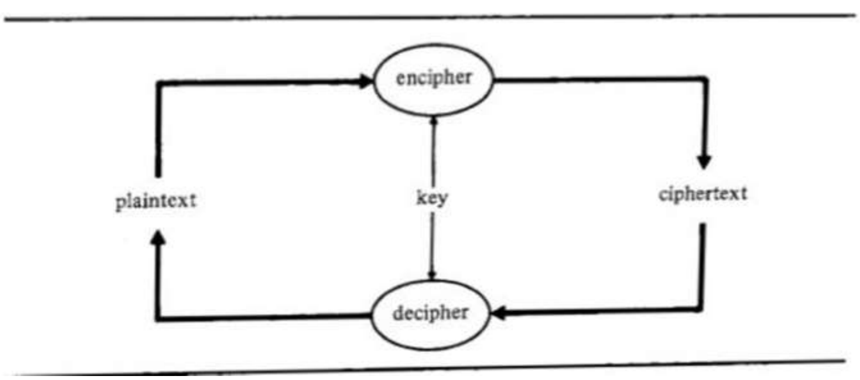
Subject	**The page**
Chapter one	**1**

1.1 CRYPTOGRAPHY	2
1.2 Cryptanalysis	2
1.3 CRYPTOGRAPHIC SYSTEM	3-6
1.4 Public-Key Systems	6
1.5 NUMBER THEORY	7
1.6 Congruences and Modular Aritemtic	7-8
1.7 Computing Inverses	8-9
1.7.1 Theorem	9
1.7.2 Theorem	9
1.7.3 Example	10
1.8 Theorem Chinese Remainder theorem	10
1.9 Vigenere and variant beaufort	10
1.9.1 Vigenere	10-11
1.9.2 Variant Beaufort	11
1.10 Pohlig Heilman scheme	11-12
1.11 Hivest-shamir-Adleman (RSA) scheme	12-13
Chapter tow	**14**
Introduction	15
2.1 hybrid between vigenere and Polig-Hellman algorithem	15
2.2 hybrid between Beaufort and Pohlig-Hellman algorithem	16
2.3 hybrid between vigenere and Hivest-shamir Adleman(RSA) algorithem	17
2.4 hybrid between Beaufort and Hivest-shamir(RSA) algorithem	18
References	19

Chapter one

1.1CRYPTOGRAPHY

Cryptography is the science and study of secret writing. Acipher is a secret meth-od of writing, whereby plaintext(or cleartext) is transformed into ciphertext(sometimes called a cryptogram). The process of transforming a plaintext into ciphertext is called encipherment or encryption; the reverse process of transforming ciphertext into plaintext is called ddeciphement or decryption. Both encipherment and decipherment are controlled by a cryptographic key or keys [1]



(Figure 1.1)

1.2 cryptanalysis

is the science and study of methods of breaking ciphers. A cipher is breakable if it is possible to determine the plaitext or key from the ciphertext, or to determine the key from pplaitext-cipher text pairs.[1]

1.3 CRYPTOGRAPHIC SYSTEMS

This section describes the general requirements of all cryptographic systems, the specific properties of public-key encryption, and digital sighatures. A cryptographic system (or cryptosystems for short) has five components:

1. A plaintext message space,m.
2. A ciphertext message space, $\mathcal{C}$.
3. A key space,k.
4. A family of enciphering transformations, $E_k: m \rightarrow \mathcal{C}$ $where\ k \in$ K
5. A family of deciphering transformation, $D_k: \mathcal{C} \rightarrow m$ Where k $\in K$

Each enciphering transformation $E_k\ is\ defined$

By an enciphering algorithm E, which is common to every transformation in the family, and a key K, which distinguishes it from the other transformations. Similarly, each deciphering transformation $D_k$is defined by a deciphering algorithm D and a key K. For a given k,

$$D_k\ is\ the\ invers\ of\ E_k: than\ is, D_k\left(E_k(M)\right) = M$$

For every plaintext message M, In a given cryptographic system, the transformations $E_k and\ D_k$ are described by parameters derived from k(or directly by k). the set of parameters describing E_k

is called the enciphering key, and the set of prametrts describing D_k $the\ deciphering\ key$.

illustrates the enciphering and deciphering of data.

Cryptos systems must satisfy three general require ments:

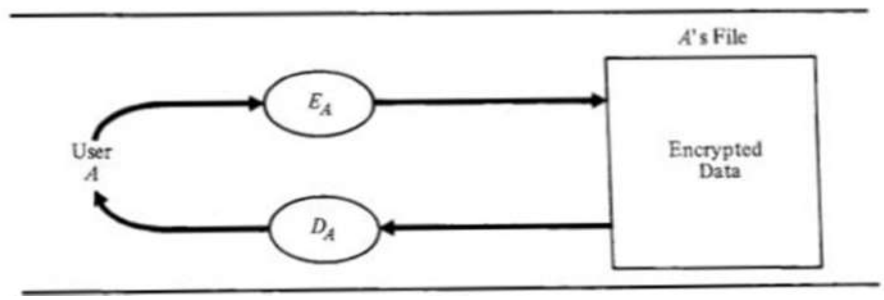
1.the enciphering and deciphering transformations must be efficient for all keys.

2.the system must be easy to use.

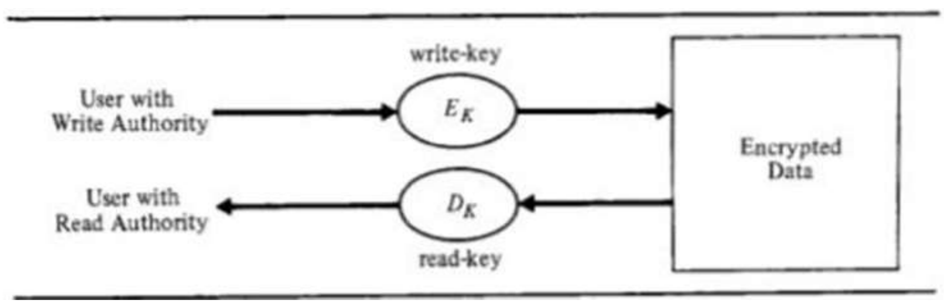
3.the security of the system should depend and the secrecy of the keys and not on the secrecy of the algorithems E or D.

In symmetric or one-key cryptosystems the encipherings and Deciphering keys are the same (or easily determined from each other) Because we have assumed the general method of encryption is known, this means the transformationE_k andD_k are also easily derived from each other.thus,if both E_k and D_k

Are protected, both secrecy and authenticity are achieved. Secrecy cannot be seps mations & and D are also easily De available a derived from each other. Thus, if both E, and D poses the other. Thus, all the requirements for both secrecy and authenticity rated from authenticity, however, because making either Ex or hold in one-key systems



(Figure 1.2)



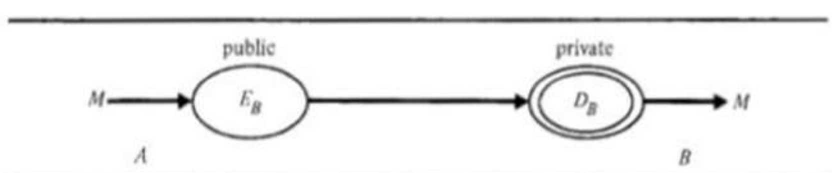
(Figure 1.3)

In asymmetric or two-key cryptosystems the enciphering and deciphering. Keys differ in such a way that at least one key is computationally infeasible to Determine from the other. Thus, one of the transformations E_k or D_k can be re-Vealed without endangering the other.Secrecy and authenticity are provided by protecting the separate transforma-Tions—D_k for secrecy, E_k for authenticity. illustrates how this principle Can be applied to databases, where some users have read-write authority to the Database, while other users have read authority only. Users with read-write au-thority are given both D_k and E_k so they can decipher data stored in the database Or encipher new data to update the database. IfE_k cannot be determined fromD_k Users with read-only authority can be given $D_k$so they can decipher the data but Cannot update it. Thus D_k is like a read-key, whileE_k is like a write-key (more Precisely, the deciphering key describing D_k is the read-key, and the enciphering Key describing E K the write-key). [2]

1.4 Public-Key Systems

The concept of two-key cryptosystems was introduced by Diffie and Hellman in 1976 . They proposed a new method of encryption called public-key en- cryption, wherein each user has both a public and private key, and two users can communicate knowing only each other's public keys

In a public-key system, each user A has a public enciphering transformation E_A which may be registered with a public directory, and a private deciphering transformation D_A which is known only to that user. The private transformation D_A is described by a private key, and the public transformation E_A, by a public key (Figure 1.4)



Derived from the private key by a one-way transformation. It must be computa- tionally infeasible to determine D_A, from E_A, (or even to find a transformation equivalent to D_A,).[3]

1.5 NUMBER THEORY

This section summarizes the concepts of number theory needed to understand the cryptographic techniques described in Chapters 2 and 3. Because we are primarily interested in the properties of modular arithmetic rather than congruences in gen- eral, we shall review the basic theorems of number theory in terms of modular arithmetic, emphasizing their computational aspects. We shall give proofs of these

Fascinating theorems for the benefit of readers unfamiliar with them.[4]

1.6 Congruences and Modular Arithmetic

Given integers a, b, and n≠0, a, is congruent to b modulo n, written A

$a \equiv_n b$

If and only if

$a - b = kn$

for some integer k; that is n divides (a – b), written

n| (a – b).

For example, 17≡ 7, because (17–7) = 2*5.

If $a \equiv_n b$, then b is called a residue of a modulo n (conversely, a is a residue of b modulo n). A set of n integers $\{r_1 \ldots.., r_n\}$is called a complete set of residues modulo n if, for every integer a, there is exactly one r in the set such that a =,, For any modulus n, the set of integers {0, 1,…,n-}) forms a complete set of Residues modulo n. We shall write

a mod n

To denote the residue r of a modulo n in the range [0. n-1]. For example, 7 mod 3 = 1. Clearly,

a mod n=r implies a≡ r

but not conversely. Furthermore,

a ≡ b if and only if a mod n = b mod n;

Thus, congruent integers have the same residue in the in the range[0,n–1].[5]

1.7 Computing Inverses

Unlike ordinary integer arithmetic, modular arithmetic sometimes permits the Computation of multiplicative inverses; that is, gives an integer a in the range [0,n–1].

it may be possible to find a unique integer x in the range [0,n–1] such that

ax mod n=1.

For example, 3 and 7 are multiplicative inverses mod 10 because 21 mod 10=1. It Is this capability to compute inverses that makes modular arithmetic so appealing In cryptographic applications.

We will now show that given a [0,n– 1], a has a unique inverse mod n When a and n are relatively prime; that is when gcd(a,n)= 1, where "gcd" Denotes the greatest common divisor.[6]

1.7.1 Theorem

If gcd (a, n) = 1, then there exists an integer x, 0 < x < n, such that ax mod n = 1.

Proof:

Because the set $\{ai \; mod \; n\}_{i=0.....n-1}$ is a permutation of {0, 1. …. n–1}, x=i, where ai mod n = 1, is a solution. [7]

1.7.2 Theorem

For n= pq and p, q prime,

Ø(n) = Ø(p)Ø(q) = (p −1)(q–1).

Proof:

Consider the complete set of residues modulo n:{0, 1,…, pq-1}. All of these residues are relatively prime to n except for the p- 1 elements{q, 2q,…,(p-1)q}, the q- 1 elements {p. 2p…(q-1)p}, and 0.

Therefore,

Ø(n) = pq– [(p-1) + (q – 1) + 1] = pq -p -q+1

=(p-1) (q-1). [5]

1.7.3 Example

Let a=3 and n=7. Then

X = 3^5 mod 7. Which we saw earlier is 5. This checks, because 3*5 mod 7= 1.

1.8 Theorem Chinese Remainder Theorem:

Let d_1 …, d_t , be pairwise relatively prime, and let n= $d_1 d_2$,…d_t. Then the System of equations

(x mod d_i) = x_i (i= 1,….,t)

has a common solution x in the range [0,n– 1].[6]

1.9 Vigenère and variant Beaufort

1.9.1 Vigenère

Vigenère and Beaufort Ciphers

A popular form of periodic substitution cipher based on shifted alphabets is the Vigenere cipher. As noted by Kahn this cipher has been falsely attrib- uted to the 16th Century French cryptologist Blaise de Vigenère. The key K is Specified by a sequence of letters:

K= $k_1 \dots k_d$,

Where k_i (i = 1,...,d) gives the amount of shift in the ith alphabet; that is, $f_i(a) = (a + k_i) mod\ n$.

Example:

The encipherment of the word RENAISSANCE under the key BAND is show next:

M =RENA ISSA NCE

K. =BAND BAND BAN

E_k (M)=SEAD JSFD OCR

In this example, the first letter of each four-letter group is shifted (mod 26) by 1, the second by 0, the third by 13, and the fourth by 3.[2]

1.9.2 variant Beaufort

The Variant Beaufort cipher uses the substitution

f_i=(a–k_i) $mod\ n$.

Because

(a–k_i) mod n= (a + (n-k_i)) mod n,

The Variant Beaufort cipher is equivalent to a Vigenère cipher with key character (n–k_i).

The variant Beaufort cipher is also the inverse of the Vigenere cipher; thus if one is used to encipher. The other is used to decipher. [4]

1.10 Pohlig Heilman Scheme

In the pohlig- Heilman scheme, the modulus is choses to be a trags prime p The enciphering and deciphering functions are thus given by

C=$M^e mod\ p$

M=$c^d mod\ p$

Wher all arithmetic is done in the Gsion field GF(p)

Bocease p is.prime.Ø(p)=p–1 which is trivially derived from p thusThe scheme can only be used for conventional cocryption, where e and d are both kept secret .[3]

Example

Let p =11, whence Ø(p)=p–1= 10. Choose and d=7 compute e=inv(7,10)=3 Suppose M=5 Then M is enciphered as

C=M^e mod p = 5^3 mod 11=4

Similarly, c is deciphered as:

M=$C^d mod\ p = 4^7\ mod\ 11 = 5.$

1.11 Hivest- Shamir- Adleman (RSA) Scheme

In the RSA scheme, the modulus n is the product of two large primes p and q.

n=pq

Thus

Ø(n) =(p–1)(q–1)

(see theorem 1.3 in section 1.6.2) the enciphering and deciphering functions are given by Eq. (2.2)and (2.3).Rivest, shamir and Adleman recommend picking a relatively prime to Ø(n) in the interval [max (p, q) +1,n–1] (any prime in the interval will do);e I'd computed using Eq. (2.5).If inv(d, Ø(n)) such that e<log 2 $n\ then\ a\ new\ value\ of\ d\ should\ be\ picked\ to$nceypt ed message undergoes some wrap-around(reduction modulo n).[7]

Example:

Let p=5 and q=7whence n=pq=35 and Ø(n) =(5–1)(7–1)=24 pick d=11. Then e=inv(11,24)=11(in fact, e and d will always be the same for p=5 and q=7—see exercises at end of chapter). Suppose M=2 Then

C=$M^e mod\ n = 2^{11} mod\ 35 = 2048\ mod\ 35 = 18,$

and

$$C^d mod\ n = 18^{11} mod\ 35 = 2 = M.$$

Chapter tow

Introduction

In this chapter, we hybrid between the public key algorithem, and classical clyptaglaphy

2.1 hybrid between vigenere and pohlig–Hellman algorithem.

In this method we encipher by vigenere method after that encipher by pohlig and decipher by pohlig method after that decipher by vigenere.

Example: Let the plaintext (M≡F≡5) with the keys (k=4,p=11and e=3)

To Encipher

$C_1 = p + k \; mod\; 26$

$C_1 = 5 + 4 mod\; 26 = 9$

$C_2 = p^e \; mod\; p$

$C_2 = 9^3 mod\; 11 = 3$

To Decipher

Comput d=$e^{\varphi(\varphi(p))-1}\; mod \varphi(p)$

d=$3^{\varphi(\varphi(11)-1}\; mod \varphi(11) = 7$

$M_1 = c_2^d \; mod\; p$

$M_1 = 3^7 mod\; 11 = 9$

$M_2 = M_1 - k\; mod\; 26 \rightarrow M_2 = 9 - 4\; mod\; 26 = 5$

2.2 hybrid between Beaufort and pohlig–Hellman algorithem

In this method we encipher by Beaufort method after that encipher by pohlig and decipher by pohlig method after that decipher by Beaufort.

Example:Let the plaintext (M≡F≡5) with the keys (k=4,p=11 and e=3)

To Encipher

$C_1 = p - k \; mod \; 26$

$C_1 = 5 - 4 \; mod \; 26 = 1$

$C_2 = p^e \; mod \; p$

$C_2 = 1^3 \; mod \; 11 = 1$

To Decipher

Comput d= $e^{\varphi(\varphi(p))-1} \; mod \; \varphi(p)$

d= $3^{\varphi(\varphi(p))-1} \; mod \; \varphi(p) = 7$

$M_1 = c_2^d \; mod \; p$

$M_1 = 1^7 mod \; 11 = 1$

$M_2 = M_1 + k \; mod \; 26$

$M_2 = 1 + 4 mod \; 26 = 5$

2.3 hybrid between vigenere and Hivest-shamir-Adleman(RSA) algorithem

In this method we encipher by vigenere method after that encipher by Hivest-shamir-Adleman(RSA) and decipher by Hivest-shamir-Adleman(RSA) method after that decipher vigenere.

Example: Let the plaintext (M≡F≡5) with the keys (k=4,p=5,q=7

n=35 and e=11)

To Encipher

$C_1 = p + k \; mod \; 26$

$C_1 = 5 + 4mod \; 26 = 9$

$C_2 = p^e \; mod \; n$

$C_2 = 9^{11} \; mod \; 35 = 4$

To Decipher

Comput d= $e^{\varphi(\varphi(n))-1} \; mod \; \varphi(n)$

d= $11^{\varphi(\varphi(35))-1} \; mod \; \varphi(35) = 11$

$M_1 = c_2^d \; mod \; n$

$M_1 = 4^{11} \; mod \; 35 = 9$

$M_2 = M_1 - k \; mod \; 26$

$M_2 = 9 - 4 \ mod \ 26 = 5$

2.4 hybrid between Beaufort and Hivest-shamir-Adleman (RSA) algorithem

In this method we encipher by Beaufort method after that encipher by Hivest-shamir-Adleman(RSA) and decipher by Hivest-shamir-Adleman(RSA) method after that decipher Beaufort .

Example: Let the plaintext (M≡F≡5) with the keys (k=4,p=5,q=7

n=35 and e=11)

To Encipher

$C_1 = p - k \ mod \ 26$

$C_1 = 5 - 4 \ mod \ 26 = 1$

$C_2 = p^e \ mod \ n$

$C_2 = 1^{11} \ mod \ 35 = 1$

To Decipher

Comput d= $e^{\varphi(\varphi(n))-1} \ mod \ \varphi(n)$

d= $11^{\varphi(\varphi(35))-1} \ mod \ \varphi(35) = 11$

$M_1 = c_2^d \ mod \ n$

$M_1 = 1^{11} \ mod \ 35 = 1$

$M_2 = M_1 + k \ mod \ 26$

$$M_2 = 1 + 4\ mod\ 26 = 5$$

References

1-Alfred J-menezes paul C.van Oorschot and scott A.vanstone ″Hand book of Applied cryptography″ CRC press, 1996.

2-Bruce″ application cryptography″ second edition published by john wiley and sonsinc, 1996.

3-Dorothy E″ cryptography and data security″ by addison wesley publishing company 1982.

4-David M.B″ Elementeray number theory″ second edition Wcb published 1989.

5-Hans delfs and helmut knebl″ introduction to cryptography″ germany 2002.

6-J.van zur gathen ″classical cryptography bonn – Aachen intemational center tech nology version-july 14, 2008.

7-Jennifer S. and Josef p ″cryptography an introduction to computer security″ by prentic hall of a stralia pty-lid P-35-88, 1982.