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

“Hybrid Classical Methods”

A graduate research submitted to the Council of the Department of Mathematic College of Education for Pure Sciences, University of Babylon
It is part of the requirements for a Bachelor's degree in Mathematics

Prepared by

Alaa Manea Hadi Farhan

Supervised by

Prof. AMEER A . J . AL–SWIDI

2023 A.D **1444 A.H**

بسم الله الرحمن الرحيم

الله لا إله إلا هو الحي القيوم
لا تأخذه سنة ولا نوم
له ما في السماوات وما في الأرض
من ذا الذي يشفع عنده إلا بإذنه
يعلم ما بين أيديهم وما خلفهم
ولا يحيطون بشيء من علمه إلا بما شاء
وسع كرسيه السماوات والأرض
ولا يؤوده حفظهما وهو العلي العظيم

صدق الله العظيم

إهداء

قال تعالى: (قل اعملوا فسيرى الله عملكم ورسوله والمؤمنون)

صدق الله العلي العظيم

إلهي لا يطيب الليل الا بشكرك ولا يطيب النهار الا بطاعتك .....

ولا تطيب اللحظات الا بذكرك .. ولا تطيب الاخرة الا بعفوك ..

ولا تطيب الجنة الا برؤيتك

« الله جل جلالة»

الى من بلغ الرسـالة وادى الامانة ونصـح الامة .. الى نبي الرحمة ونور العالمين

« سيدنا محمد صلى الله عليه وسلم»

الى من كلله الله بالهيبة والوقار ..الى من علمني العطاء بدون انتظار ..الى من احمل اسمه بكل افتخار

« والدي العزيز»

الى ملاكي في الحياة ..الى معنى الحب والي معنى الحنان والتفاني ..الى بسمة الحياة وسر الوجود ..الي من كان دعائها سر نجاحي وحنانها بلسم جراحي

« امي الحبيبة»

الى منارة العلم والعلماء الصرح الشامخ ....جامعة بابل ..الى الذين حملوا اقدس رساله في الحياة الي الذين مهدوا لنا طريق العلم والمعرفة

« اساتذتنا الافاضل»

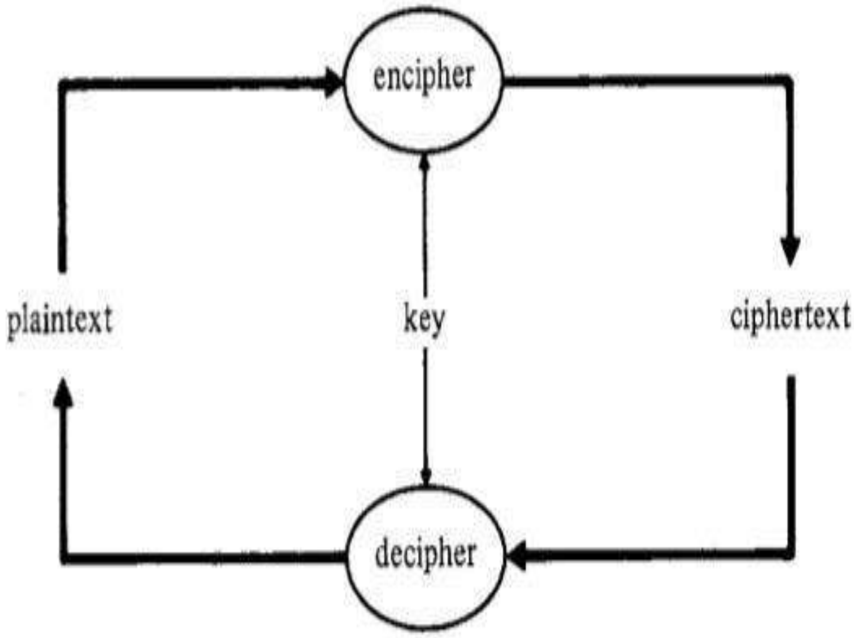
Abstract

In this research, we hybrid between the classical methods,in the first hybrid the vigener and variant Beaufort cipher and the second hybrid variant hybrid variant Beaufort and Hill cipher, and this give more complex to analysis and cracker’s from unknown person’s (Hacker’s).

Contents

1.1) Cryptography

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



(Figure 1.1)

1.2) Cryptanalysis

Cryptanalysis is the science and study of methods of breaking ciphers. A Cipher is breakable if it is possible to determine the plaintext or key from the Ciphertext, or to determine the key from plaintext-ciphertext pairs. There are three Basic methods of attack: ciphertext-only, known-plaintext, and chosen-plaintext. [1]

1) Under a ciphertext_only attack

A cryptanalyst must determine the key solely From intercepted ciphertext, though the method of encryption, the plaintext lan-guage, the subject matter of the ciphertext. [1]

2) Under aknown-plaintext attack

a cryptanalyst knows some plaintext-ciphertext pairs. As an example, suppose an enciphered message transmitted from A user's terminal to the computer is intercepted by a cryptanalyst who knows that The message begins with a standard header such as "LOGIN”. [1]

3) Under achosen-plaintext attack

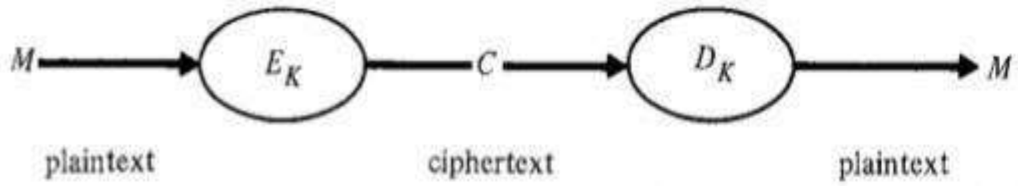
A cryptanalyst is able to acquire the cipher-text corresponding to selected plaintext. This is the most favorable case for the Cryptanalyst. A database system may be particularly vulnerable to this type of Attack if users can insert elements into the database, and then observe the changes In the stored ciphertext. [1]

1.3) Cryptographic systems

This section describes the general requirements of all cryptographic systems, the Specific properties of public-key encryption, and digital signatures[2]

- A cryptographic system (or cryptosystem for short) has five components:

1. A plaintext message space,"M"
2. A ciphertext message space, "C"
3. A key space, "K"
4. A family of enciphering transformations, E_k:m→c where K ∈K.
5. A family of deciphering transformations, D_k: C →m, where K ∈K.



(Figure 1.2)

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 trans-formation D_k is defined by a deciphering algorithm D and a key K. For a given K, D_k is the inverse of EK; that is, $D_k(E_k(M)) = M$ 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

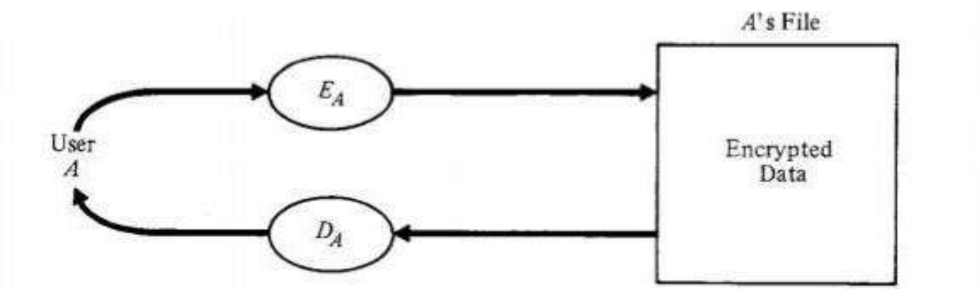
Is called the enciphering key, and the set of parameters describing D_k Kthe decipher-ing key. (Figure 1.2) illustrates the enciphering and deciphering of data.

Cryptosystems must satisfy three general requirements:

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 only on the secrecy of the keys and Not on the secrecy of the algorithms E or D.

❖ *In symmetric or one_Key*

cryptosystems the enciphering 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 transfor—mations E_k and D_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 sepa—rated from authenticity, however, because making either E_k or D_k available ex—poses the other. Thus, all the requirements for both secrecy and authenticity must hold in one-key systems. [3]



(Figure 1.3)

❖ *Asymmetric or two— Key*

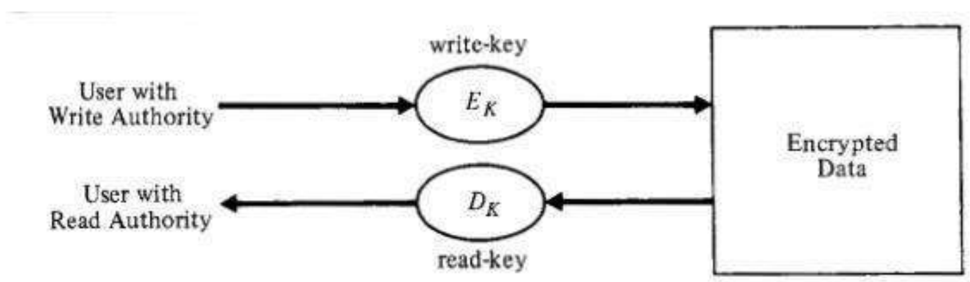
Cryptosystems the enciphering and deciphering keys differ in such a way that at least one key is computationally infeasible to Determine from the her. Thus, one of the transformations E_k or D_k can be re—vealed without

endangering the other.Secrecy and authenticity are provided by protecting the separate transforma—tions—D_k for secrecy, E_k for authenticity. (Figure 1.4) 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 authority 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. If E_k cannot be determined from D_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, while E_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). [3]



(Figure 1.4)

1.4) 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]

1.5) Congruences and Modular Arithmetic

Given integers a, b, and $n \neq 0$, a, is congruent to b modulo n, written?

$a \equiv_n b$

If and only if

$a-b=kn$

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

$n \mid (a - b)$.

For example, $17 \equiv_5 7$, because $(17 - 7) = 2 * 5$.

If $a \equiv b$, then b is called a residue of a modulo n (conversely, a is a residue of b modulo n). A set of n integers $\{r_1 \dots, r_n\}$ is called a complete set of residues modulo n if, for every integer a, there is exactly one r_i in the set such that $a \equiv_n r_i$

For any modulus n, the set of integers $\{0, 1 \dots, n - 1\}$ forms a complete set of residues modulo n. [4]

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 $a \equiv_n r$,

But not conversely. Furthermore,

$a \equiv_n b$ if and only if a mod n = b mod n;

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

1.6) Computing Inverses

Unlike ordinary integer arithmetic, modular arithmetic sometimes permits the Computation of multiplicative inverses; that is, given 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 mood 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.[4]

1.6.1)Theorem

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

ax mood n = 1.[5]

Prof:

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.

1.7) Chinese Remainder Theorem

Let d_1, …, d_t be pairwise relatively prime, and let n = d_1d_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]

1.8) Vigenere and Variant Beaufort Cipher

Apopular form of periodic substitution cipher based on shifted alphabets is the:

1.8.1) Vigenere Cipher

This cipher has been falsely attrib–uted to the 16th century french cryptologist Blaise de vigenere. The key K is specified by a sequence of letters:

K = k_1 ……K_d ,

Where $K_i(i=1,........,d)$ gives the amount of shift in the ith alphabet; that is,

$$F_i(a) =)a + k_i) \bmod n . [7]$$

1.9) Example:

The encipherment of the word RENAISSANCE under the key BAND is shown 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 .

1.8.2) Variant Beaufort Cipher

Uses the substitution. $f_i(a) = (a - k_i) \bmod n$.

Because

$)a - k_i) \bmod n\ (a +)n - k_i) \bmod n$

The variant Beaufort cipher is equivalent to a vigenere 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. [7]

1.10) Hill Cipher

The hill cipher performs a linear tranformation on d plaintext charac– ters to get d ciphertext characters. Suppose d=2,and let M= $m_1\, m_2$. M is enciphered as. $C= E_k(M)= C_1\, C_2$, where

$$C_1 =(K_{1\,1}\, m_1 + k_{1\,2}\, m_2) \bmod n$$

$$C_2 =(k_{2\,1}\, m_1 + k_{2\,2}\, m_2) \bmod n$$

Expressing M and C as the column vectors M =($m_{1\,,}m_2$) and C =(c_1 , c_2) ,

This can be written as

$$C =E_k(M) =KM \bmod n ,$$

Where K is the matrix of coefficients:

$$\begin{matrix} K_{1\,1} & k_{1\,2} \\ K_{2\,1} & K_{2\,2} \end{matrix}$$

That is,

$$\begin{matrix} C_1 \\ C_2 \end{matrix} = \begin{matrix} K_{1\,1} & K_{1\,2} \\ K_{2\,1} & K_{2\,2} \end{matrix} \quad \begin{matrix} m_1 \\ m_2 \end{matrix} \quad \bmod n$$

Deciphering is done using the inverse matrix k^{-1}:

$D_K(c) = k^{-1} C \bmod n$

$= K^{-1} kM \bmod n.$
$= M$

Where $K K^{-1} \bmod n = I$, and I is the 2×2 identity matrix. [2]

1.11) Example

Hello ,$K = 3$, $k^{-1} = 9$, $N = 26$

$C_1 = (P_1 K) \bmod 26 \rightarrow C_1 = (7\times3) \bmod 26 = 21$

$C_2 = (p_2 k) \bmod 26 \rightarrow C_2 = (4\times3) \bmod 26 = 12$

$C_3 = (p_3 k) \bmod 26 \rightarrow C_3 = (11\times3) \bmod 26 = 7$

$C_4 = (p_4 k) \bmod 26 \rightarrow C_4 = (11\times3) \bmod 26 = 7$

$C_5 = (p_5 k) \bmod 26 \rightarrow C_5 = (14\times3) \bmod 26 = 16$

VMHHQ

$P_1 = (c_1 k^{-1}) \bmod 26 \rightarrow (21\times9) \bmod 26 = 7$

$P_2 = (c_2 k^{-1}) \bmod 26 \rightarrow (12\times9) \bmod 26 = 4$

$P_3 = (c_3 k^{-1}) \bmod 26 \rightarrow (7\times9) \bmod 26 = 11$

$P_4 = (c_4 k^{-1}) \bmod 26 \rightarrow (7\times9) \bmod 26 = 11$

$P_5 = (c_5 k^{-1}) \bmod 26 \rightarrow (16\times9(\bmod 26 = 14$

Hello

Chapter two

Introduction

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

2.1) Hybrid between vigener and variant Beaufort

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

2.2) Example

Let the plaintext ($P = H \equiv 7$) with the key ($k = 3$)

Sollution

To encipher

C_1=(p+k) mod 26

= (7+3)mod 26

=10

C_2=(p-k)mod 26

= (10-3)mod 26

=7

To decipher

P_1=(c+k)mod 26

= (7+3)mod 26

=10

P_2=(c-k)mod 26

= (10-3)mod 26

=7

2.3) Example

let the plaintext (P = L ≡11) with the key (k = 17)

Sollution

To encipher

C=(11+17)mod 26

=28mod 26

=2

C=(2-17)mod 26

=15mod 26

= 11

To decipher

$P=(11+17) \bmod 26$

$=28 \bmod 26$

$=2$

$P=(2-17) \bmod 26$

$=15 \bmod 26$

$=11$

2.4) Example

Let the plaintexts ($P = G \equiv 6$,$P = O \equiv 14$) with key's ($k = 4$,$k = 5$)

Sollution

To encipher

$C_1= (6+4) \bmod 26$

$=10 \bmod 26$

$=10$

$c_1=(10-4) \bmod 26$

$=6 \bmod 26$

$=6$

$C_2=(14+5) \bmod 26$

$=19 \bmod 26$

$=19$

C_2=(19-5)mod 26

=14mod 26

=14

To decipher

P_1=(6+4)mod 26

=10mod 26

=10

P_1=(10-4)mod 26

=6mod 26

=6

P_2=(14+5)mod 26

=19mod 26

=19

P_2=(19-5)mod 26

=14mod 26

=14

2.5) Hybrid between variant Beaufort and Hill cipher

In this method we encipher by varent Beaufort method after that encipher by Hill cipher and decipher by Hill cipher method after that decipher by varent Beaufort.

2.6) Example

Let the plaintext ($P = W \equiv 22$) with key's ($k = 10, k = 3$)

Sollution

To encipher

C=(p-k)mod 26

=(22-10)mod 26

=12mod 26

=12

C=pkmod 26

=(12×3)mod 26

=36mod 26

=10

To decipher

The $k^{-1} = k^{\varphi(n)-1} \bmod 26 \Rightarrow K^{-1} = 3^{\varphi(26)-1} \bmod 26 \Rightarrow k^{-1} = 3^{12-1} \bmod 26 \Rightarrow k^{-1} = 3^{11} \bmod 26 \Rightarrow k^{-1} = 9$

P=Ck^{-1} mod 26

=(10×9)mod 26

=90mod 26

=12

$P=(c+k) \bmod 26$

$=(12+10) \bmod 26$

$=22 \bmod 26$

$=22$

2.7) Example

let the plaintexts ($P = A \equiv 0$,$P = L \equiv 11$ and $P = I \equiv 8$) with key's ($k = 18$, $k = 3$)

Sollution

To encipher

$C_1=(p_1-k) \bmod 26$

$=(0-18) \bmod 26$

$=8 \bmod 26$

$=8$

$C_1= p_1 k \bmod 26$

$=(8\times3) \bmod 26$

$=24 \bmod 26$

$=24$

$C_2=(p_2-k) \bmod 26$

$=(11-18) \bmod 26$

$=19 \bmod 26$

$=19$

$C_2 = p_2 k \bmod 26$

$= (19 \times 3) \bmod 26$

$= 57 \bmod 26$

$= 5$

$c_3 = (p_3 - k) \bmod 26$

$= (8-18) \bmod 26$

$= 16 \bmod 26$

$= 16$

$c_3 = p_3 k \bmod 26$

$= (16 \times 3) \bmod 26$

$= 48 \bmod 26$

$= 22$

To decipher

The $k^{-1} = k^{\varphi(n)-1} \bmod n \Rightarrow K^{-1} = 3^{\varphi(26)-1} \bmod 26 \Rightarrow k^{-1} = 3^{12-1} \bmod 26 \Rightarrow k^{-1} = 3^{11} \bmod 26 \Rightarrow k^{-1} = 9$

$P_1 = c_1 k^{-1} \bmod 26$

$= (24 \times 9) \bmod 26$

$= 216 \bmod 26$

$= 8$

$P_1=(c_1+k)\bmod 26$

$=(8+18)\bmod 26$

$=26\bmod 26$

$=0$

$P_2=c_2\, k^{-1}\bmod 26$

$=(5\times9)\bmod 26$

$=19\bmod 26$

$=19$

$P_2= (c_2+k)\bmod 26$

$=(19+18)\bmod 26$

$=37\bmod 26$

$=11$

$P_3=c_3\, k^{-1}\bmod 26$

$=(22\times9)\bmod 26$

$=198\bmod 26$

$=16$

$p_3=(c_3+k)\bmod 26$

$=(16+18)\bmod 26$

$=34\bmod 26$

$=8$

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 " in troduction 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.