Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 1, March 2016 , p.p(20-28)
ISSN 1992 – 0849

A Developed Discrete Fourier Transform based Cryptosystem

Ashty M. Aaref

College of Technology / Software Engineering Dept., Kirkuk , Iraq

ashty_06@yahoo.com

Received date: 23 / 4 / 2015 **Accepted date: 14 / 9 / 2015**

ABSTRACT

This paper provides a developed cryptosystem for data encryption based on using the Discrete Fourier Transform (DFT). The encryption side using the DFT method for performing the main security development that is considered as the main encryption process in the developed cryptosystem. The primary ciphered plaintext data must be prepared as a block of (N) data, and entered to the DFT part. The decryption side uses as an inverse DFT method, to get back the primary ciphered plaintext from the received cipher text. The proposed method applied to classical encryption method, and can be applied to a stream cipher method. The validity of the developed encryption process is illustrated through many numerical examples.

Keywords: *DFT, Stream Cipher, Monoalphabetic Cipher System, Frequency Analysis.*

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 1, March 2016 , p.p(20-28)
ISSN 1992 – 0849

نظام تشفير مطور معتمد على محول فوريه المتقطع

ئاشتي مهدي عارف

الكلية التقنية كركوك / قسم هندسة البرمجيات / كركوك ، العراق

ashty_06@yahoo.com

تاريخ استلام البحث: ١٤ / ١٢ / ٢٠١٤ تاريخ قبول البحث: ١٤ / ٩ / ٢٠١٥

الملخص

يعرض البحث نظام تشفير مقترح لأمنية البيانات معتمدا على استخدام (محور فوريه المتقطع DFT). في جانب المشفر يكون استخدام طريقة ال DFT مع الطريقة الاساسية المستخدمة (مع ذلك النظام المعني) لإنجاز عملية التشفير للبيانات المدخلة، حيث يجب تهيئة البيانات (المراد تشفيرها) على هيئة مقاطع مكونة من N من القيم ، وتدخل هذه القيم الى المعالج DFT . وبالطرف المقابل (حل الشفرة) يتم استخدام المعكوس لهذا المعالج ، وهو الـ IDFT لاسترجاع البيانات الاصلية. تطبق الطريقة المقترحة في هذا البحث على طرائق التشفير التقليدية، وكذلك يمكن تطبيقها مع نظام التشفير الانسيابي. وقد تم ايضاح قابلية تطبيق الطريقة المقترحة من خلال عدد من الامثلة.

الكلمات الدالة: الـ DFT ، تشفير انسيابي، نظام تشفير وحيد الهجائية، تحليل التردد.

1. INTRODUCTION

The cipher system provides confidential information in such a way that it's meaning is unintelligible to unauthorized person. The historical development of cryptography can be divided into a number of stages. First stage is the handwritten systems such as a simple letter substitution that could be implemented using pencil and paper or simple mechanical machines. The second stage dates from the beginning of the twentieth century (the time the telegraph became truly established) the late 1950s. These systems normally used complex mechanical and electro-mechanical machines [1].

Diffie and Helman in 1976 [2] proposed a system for distributing the secret key to be used in conventional cryptosystem over public (insecure) communication channel. The disguised information about the key is sent over an insecure channel in such a way that only the authorized partner can deduce the key [1]. The process of applying a key to transfer back from the cipher text to the plain text is known as deciphering. The block diagram of cryptosystem is shown in Fig. (1).

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 1, March 2016 , p.p(20-28)
ISSN 1992 – 0849

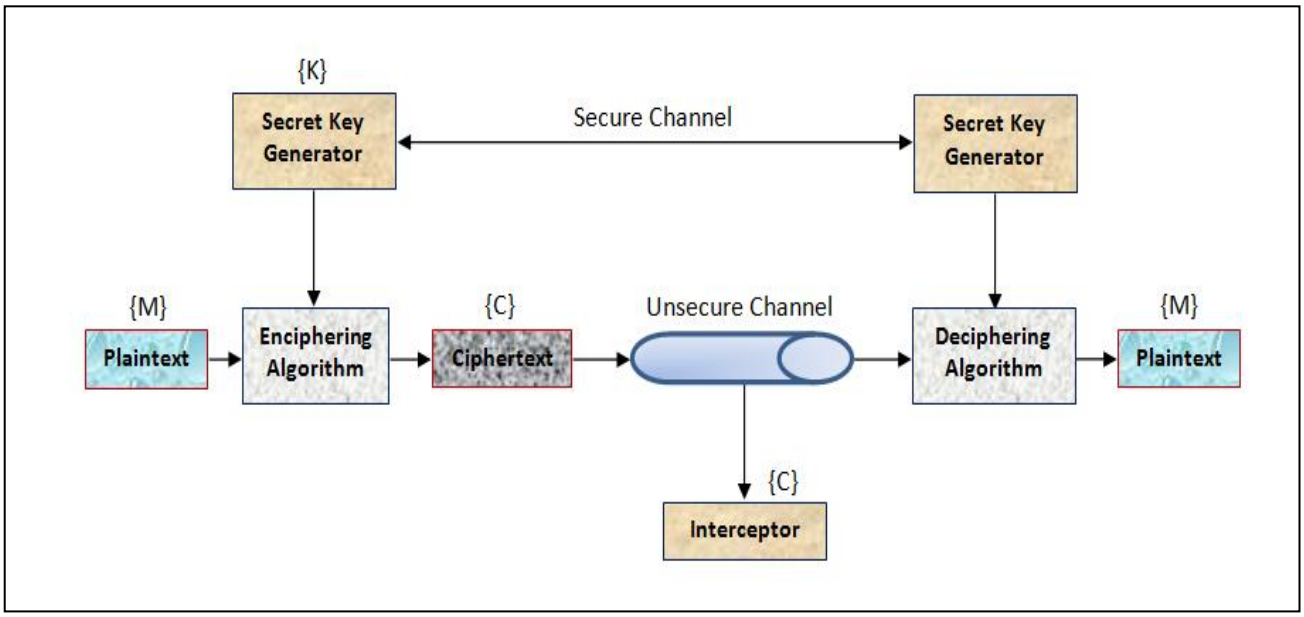

Fig. (1): The Block Diagram of crypto system

The set of all messages is called the "Message Space" and is denoted by {M}. The set {C} of all cryptograms is called "Cryptogram Space" and the set of all keys is denoted by {K}. In any practical situation M, C and K will be finite sets [3]. One crucial requirement of cipher system is that knowledge of the cryptogram, key and algorithm must enable the recipient to determine the message uniquely. Thus if c = t(m), then (m) must be uniquely determined by c and t. In other words, (t) must be reversible and (m) must be the image of c under t^{-1}. In [6], it was given a generalization of the DFT. If (s) be a periodic sequence whose elements lie in a finite field. It presented an algorithm which calculates the minimal polynomial of (s), assuming that a period of (s) is known [4].

The main objective of this paper is: " A proposing method for developed data enciphering and deciphering using the DFT with some well-known cipher systems and evaluating the new developed cryptosystem".

Section two introduces the DFT and its main properties. Section three provides the use of DFT in Cryptography, i.e., discussion of the proposed procedure for using of the DFT based developed cipher systems. Section four provides evaluation of the developed system through a given mathematical example. Section five provides the conclusions and future works.

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 1, March 2016 , p.p(20-28)
ISSN 1992 – 0849

2. FOURIER TRANSFORM- MATHEMATICAL BACKGROUND

Consider a complex series x(k) with N samples of the form $x_0, x_1, x_2, \ldots\ldots\ldots\ldots, x_{N-1}$ where x is a complex number: $x_i = x_{real} + j\, x_{imag}$

The Fourier Transform (FT) of this series will be denoted X(k). It will have N samples. The Forward Transform is defined as:

$$X(n) = \frac{1}{N} \sum_{k=0}^{N-1} x(k)\, e^{-j k \pi n/N} \qquad \text{for } n = 0..N-1 \qquad ------(1)$$

While the Inverse Fourier Transform (IFT) will be defined as:

$$X(n) = \sum_{k=0}^{N-1} x(k)\, e^{j k 2\pi n/N} \qquad \text{for } n = 0..N-1 \qquad ------(2)$$

In general, the transform into the frequency domain will be a complex valued function, that is, with magnitude and phase.

$$\left.\begin{aligned} \text{Magnitude} &= \|X(n)\| = (x_{real} \times x_{real} + x_{imag} \times x_{imag})^{0.5} \\ \text{Phase} &= \tan^{-1}\left(\frac{x_{imag}}{x_{real}}\right) \end{aligned}\right\} \quad ------(3)$$

Notes:

1. The first sample X(0) of the transformed series is the DC component.

2. The DFT of a real series, i.e.: imaginary part of x(k) = 0, results in a symmetric series about the Nyquist frequency.

3. The negative frequency samples are also the inverse of the positive frequency samples.

3. A Proposed Developed Cryptosystem based on DFT

The paper provides a developed method for enciphering using the DFT with some monoalphabetic ciphers system. The proposed system is illustrated in Fig. (2).

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 1, March 2016 , p.p(20-28)
ISSN 1992 – 0849

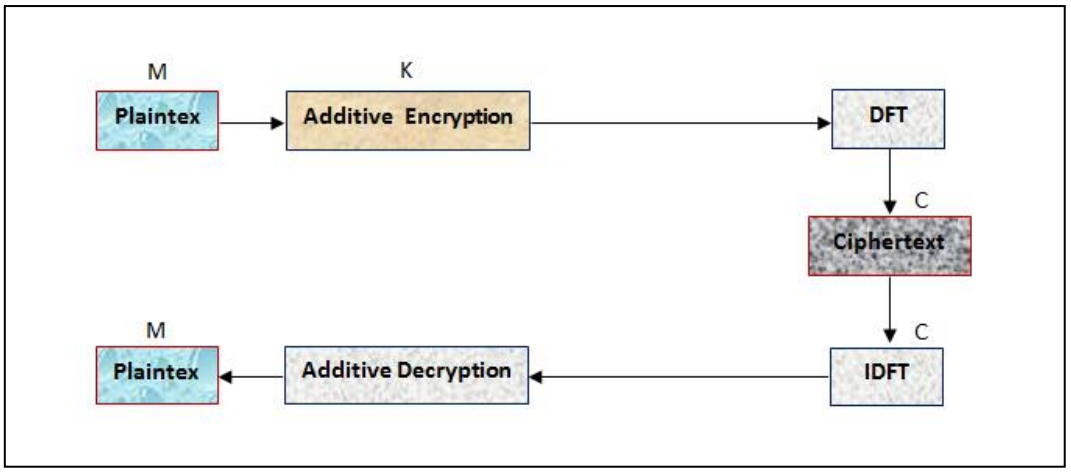

Fig. (2): The basic system by using the DFT with some ciphers system

The DFT with additive ciphers or multiplicative ciphers [5] is developed for producing new cipher system that consists of same substitution cipher system in connection with DFT. This means that the ciphered output of the classical substitution cryptosystem is passed to another mapping or transformation that is achieved by the DFT.

Example (1):

Encipher and decipher the message "Notation", using the proposed DFT based cipher system.

Solution:

- Using the additive cipher system with key k =3, we get the cipher text

[q r w d w l r q], or in numbers: [17,18,23,4,23,12,18,17]

- Using the DFT algorithm with N = 8, and the data [17, 18, 23, 4, 23, 12, 18, 17], the output of the DFT will be :

C(0) = 132, C(1) = 7.435033 - 5.024916E - 02 j, C(2) = - 0.999925 - 9.000002 j C(3) = - 19.43501 + 9.94976 j, C(4) = 30 + 1.941512E-05 j, C(5) = - 19.43506 - 9.949713 j, C(6) = - 1.000034 + 9.000002 j, C(7) = 7.434974 + 5.026633E - 02 j.

This data is transmitted in the channel (i.e. for each coefficient, two values will be transmitted):

(132, 0, 7.435033, -5.024916E-02, -0.999925, -9.000002, -19.43501, 9.94976, 30, 1.941512E-05, -19.43506, -9.949713, -1.000034, 9.000002, 7.434974, 5.026633E-02).

- The receiver use the IDFT algorithm with N = 8, this will result in:

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 1, March 2016 , p.p(20-28)
ISSN 1992 – 0849

X(0) = 16.99998 + 1.049833E-05 j, X(1) = 18 - 1.72175E-05 j, X(2) = 23 + 5.130169E-06 j, X(3) = 4.00001 - 5.879232E-07 j, X(4) = 23.00001 - 7.351455E-06 j, X(5) = 12+ 6.95597E-06 j,

X(6) = 18 - 9.065786E-07 j, X(7) = 16.99999 + 5.000801E-06 j.

- The receiver approximates the resulted data to integer values, and then the resulted numbers will be:

(17, 18, 23, 4, 23, 12, 18, 17)

- By using the inverse of additive cipher system with key (K= 3) the receiver gets the data

(14, 15, 20, 1, 20, 9, 15, 14), or the massage "Notation".

4. Evaluation of the Proposed Developed DFT based Cipher Systems

An example of evaluation the security of the proposed cipher system will be considered to illustrate the evaluation task.

4.1. The Proposed Monoalphebetic - DFT Cipher

Actually it is well known that this system has a limited security due to many factors, such as:

- The limited number of alphabet size which results in a limited number of the used keys.
- The statistical behavior of the used language in preparing the input data of the cryptosystem.

These factors cause the possibility of ease breaking of ciphered output. Hence any proposition to enhance the security must overcome these factors. The following example illustrates this concept.

Example (2):

Use the Monoalphabetic to encipher the plaintext given below: "since its not to easy to hand write or type write bold face letters we should write a vector either with an arrow over it".

Solution:

- Using additive cipher system with key = 3,

i.e., cipher text ≡ (Plaintext + key) (mod 26), or $c_i = m_i + k \pmod{26}$, then the resulting cipher text will be:

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 1, March 2016 , p.p(20-28)
ISSN 1992 – 0849

{vlqfhlwv, qrwhdvbw, rkdqgzul, whruwbsh, zulwhero, gidfhohw, whuvbrxv, krxogzul, whdyfwr, uhlwkhuz, lwkdqduu, rzruhulw}.

Each letter by the number of its position in the alphabet and instead of representing it by 26, we represent z by 0. Thus we have:

Letter:	a	b	c	d	e	f	g	h	i	j	k	l	m
Number:	1	2	3	4	5	6	7	8	9	10	11	12	13
Letter:	n	o	p	q	r	s	t	u	v	w	x	y	z
Number:	14	15	16	17	18	19	20	21	22	23	24	25	0

- We divide the ciphertext to blocks of letters, each block contains eight letters. Then convert each letter into its corresponding decimal value as shown below:

{the block (no.1): 22, 12, 17, 6, 8, 12, 23, 22; the block (no.2): 17, 18, 23, 8, 4, 22, 2, 23; the block (no.3): 18, 11, 4, 17, 7, 0, 21, 12; the block (no.4): 23, 8, 18, 21, 23, 2, 19, 8; the block (no.5): 0, 21, 12, 23, 8, 5, 18, 15; the block (no.6): 7, 9, 4, 6, 8, 15, 8, 23; the block (no.7): 23, 8, 21, 22, 2, 18, 24, 22; the block (no.8): 11, 18, 24, 15, 7, 0, 21, 12; the block (no.9): 23, 8, 4, 25, 8, 6, 23, 18; the block (no.10): 21, 8, 12, 23, 11, 8, 21, 0; the block (no.11): 12, 23, 11, 4, 17, 4, 21, 21; the block (no.12): 18, 0, 18, 25, 8, 21, 12, 23}.

- Applying the DFT algorithm to each block separately to calculate the corresponding coefficients as follows: For block (no.1):

$C_1(0) = 122$, $C_1(1) = 25.31371 + 17.3137\ j$, $C_1(2) = -10 + 4\ j$, $C_1(3) = 2.686308 + 5.313724\ j$, $C_1(4) = 18$, $C_1(5) = 2.686261 - 5.31368\ j$, $C_1(6) = -10 - 4\ j$, $C_1(7) = 25.31363 - 17.31372\ j$, note that the subscript 1 in the above C's represents the number of blocks, and so for the other blocks.

- Draw a histogram for the cipher letters before using the DFT and the coefficients resulting for the DFT, these graphs are shown in Fig. (3) and (4).

According to the coefficient histogram Fig. (4), it is difficult to recognize the statistics of the natural language, while in the ciphertext histogram Fig. (3), it is clear that it will be easy for cryptanalyst to find a way to break the ciphertext through the existence of the statistical behavior of the English language.

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 1, March 2016 , p.p(20-28)
ISSN 1992 – 0849

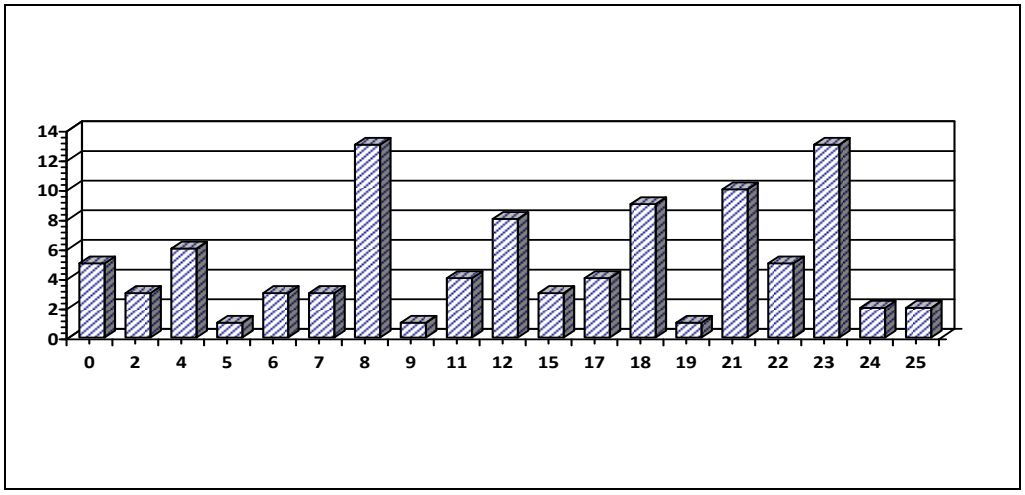

Fig. (3): The histogram of the coefficients of the cryptogram resulted before DFT

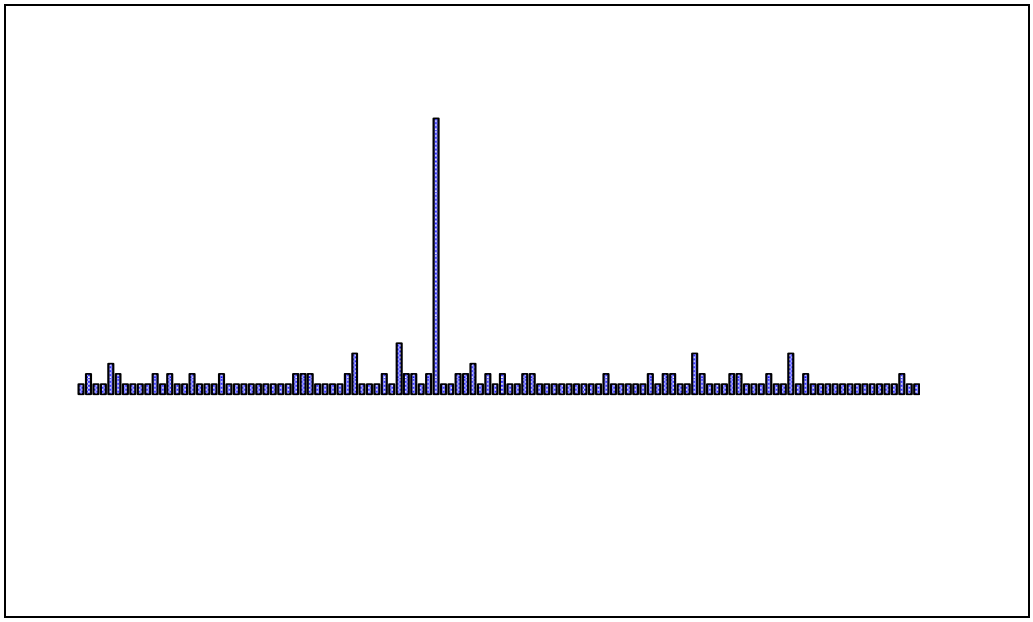

Fig. (4): The histogram of the coefficients of the cryptogram resulted after DFT

5. Conclusion and Future Work

The use of the DFT (in the developed cryptosystem) causes a failure of the frequency analysis of the statistical cryptanalysis, and the failure of the trying of all possible used enciphering keys. Hence the use of the DFT with the conventional cipher systems (monolaphabetic and polyalphabetic) will enhance the security of the resulted encryption messages. This will results in more complexity to the attack approaches (methods) used to cryptanalysis of these developed cryptosystems. For the future work, it will be suitable to try

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 1, March 2016 , p.p(20-28)
ISSN 1992 – 0849

the applying the same structure with different N size of the input data (4, 8, 16, 32, and 64) and compare the relative performance from the complexity point of view.

References

[1] D. W. Davies, and W.L. Price, "***Security for Computer Networks - An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer***", John Wiley and Sons, 1984.

[2] W. Trappe and L. C. Washington, "***Introduction to Cryptography with Coding Theory***", Prentice Hall, 2002.

[3] Th. Bier, and M. R. Wahiddin, "***Mathematical Aspects of Classical and Quantum Cryptography***", International Islamic University Malaysia, 2004.

[4] A. C. Cilbert, M. J. Strass, and J. A. Tiopp, "***A Tutorial on Fast Fourier Sampling***", IEEE Signal Processing Magazine, Vol. 57, March 2008.

[5] C. Carlet, "***Boolean Function for Cryptography and Error Correcting Codes***", University of Paris, INRIA, October 10, 2006.

[6] J. L. massey, "***Fundamentals of Information Theory, Coding and Cryptography***", Zurich, 1988.

AUTHOR

Ashty Mahdy Aaref : PhD at computer science department, university of technology, Baghdad, October 2009, in the field of "Improved backtracking ant systems". MSc at computer science department, university of technology, Baghdad, November 1999, in the field of "Improving & implementing a one-way hash function algorithm for multiple purposes". BSc at computer science department, university of technology, Baghdad, 1992. Interested fields: Digital Image Processing, Computer Networks, Search Techniques, Cipher Systems.