Testing the Randomness and Using the Digital Sequences of GF(5) in Cryptography

Lecturer Dr. Ayad Ghazi Naser Al-Shammari*

Abstract

In this paper, first, the Golomb's postulates of randomness are expanded to construct a good mathematical base, and then expand the binary standard randomness tests to be suitable to be applied on penta-sequences this mean the elements of the sequence belong to Galois Field GF(5). Second we will show usefulness of using penta-sequences in cryptography. The paper also includes some tables describe the tests results of the penta-sequences generated from some digital generators, like the Multiplicative Cyclic Group System (MCGS). The proposed cryptosystem using the GF(5)-sequences will compress or minimizing the ciphertext size comparing with the cryptosystems using GF(2)-sequences.

Keywords: Golomb's postulates, penta-sequences, GF(5), (MCGS).

*Ministry Of Education

1. Introduction

In general, any sequence generated from any generator considered a statistical experiment, for this reason the randomness tests called **statistical random tests**. Since they are statistical experiments then the proof of that the sequence is random is called **probabilistic** proof, that means when the generated sequence is random in high ratio for all experiments, then we can judge that the sequence is random, and vice versa. The randomness judgment done by two conditions [1]:

1. The length of the tested sequence must be as high as possible.
2. The number of repeating the experiment must be as high as possible.

Now, we will introduce some relevant basic concepts.

Cryptography is the study of principles and techniques by which information can be concealed in ciphertexts and later revealed by legitimates users employing the secret key, but in which it is either impossible or computationally infeasible for an unauthorized person to do so. **Cryptanalysis** is the science (and art) of recovering information from ciphertexts without knowledge of the key. Both terms are subordinate to the more general term **Cryptology**. The cryptography concerned in **Encryption** and **Decryption** processes [2].

In **stream ciphers**, the message units are bits, and the key is usual produced by a **random bit generator**. The plaintext is encrypted on a bit-by-bit basis.

The key is fed into random bit generator to create a long sequence of binary signals. This “key-stream” k is then mixed with plaintext m, usually by a bit wise XOR (Exclusive-OR modulo 2 addition) to produce the ciphertext stream, using the same random bit generator and seed. Stream ciphers are generally faster than block ciphers in hardware, and have less complex hardware circuitry. They are also more appropriate, and in some cases mandatory (e.g., in some telecommunications applications), when buffering is limited or when characters must be individually processed as they are received [3].

Universal tests were presented by Schrift and Shamir in 1993 [4] for verifying the assumed properties of a pseudorandom generator whose output sequences were not necessarily uniformly distributed.

Gustafson et al. in 1994 [5] describe a computer package which implements various statistical tests for assessing the strength of a pseudorandom bit generator.

In 1996, Gustafson [6] considered alternative statistics for the runs test and the autocorrelation test. Gustafson, Dawson, and Golić [7] proposed a new repetition test

which measures the number of repetitions of l-bit blocks. The test requires a count of the number of patterns repeated, but does not require the frequency of each pattern.

2. Using Penta-Sequences in Cryptography

It's important to show that how the penta-sequences can be useful in cryptography when used as encryption (decryption) key specially in stream cipher systems?

As an example let's take the following plaintext (length=222 letters) as a sample:

> The art and science of keeping messages secure is Cryptography, which is used as a tool to protect national secrets and strategies, and it is practiced by cryptographers. Cryptography is the study of mathematical techniques related to aspects of information security.

This plaintext encrypted by using binary key, the resultant ciphertext (length=1110 bits) is:

> 0111101101110010001110001110001001100011001010111000011
> 0111010010001011111011011100100101011010000011101111000
> 1000101110011101110010100100111111010001110001100011000
> 1100000101010001111011100 11….

In digits with base 5, the situation is different, table (1) describes the English letters coding in digits with base 5.

Table (1) The English letters coding in digits with base 5.

Letter	Code	Letter	Code	Letter	Code	Letter	Code	Letter	Code
A	00	**F**	10	**K**	20	**P**	30	**U**	40
B	01	**G**	11	**L**	21	**Q/Z**	31	**V**	41
C	02	**H**	12	**M**	22	**R**	32	**W**	42
D	03	**I**	13	**N**	23	**S**	33	**X**	43
E	04	**J**	14	**O**	24	**T**	34	**Y**	44

The above plaintext encrypted using table (1) the resultant ciphertext (length=444 digits) is:

12103304211112431001320301412412020310334413434441401 04
12314413301120334013022000233012033140434111423410010 44
14431100234123333124200244123202234332102112244424130 13
44202024101441324243133032020001042114110422432402442 22
11334302422033200111202330100244130331402244114410100 43
04200321003402120132221331430204113023341040010202 22….

Notice that the compression average of ciphertext of digits with base 5 to the ciphertext with binary key is 2/5=0.4.

3. Golomb′s Concept of Randomness [3]

Definition (1): Let S be a periodic sequence of period N. Golomb′s randomness postulates are the following:

R1: In the cycle S^N of S, the number of 1′s differs from the number of 0′s by at most 1.

R2: In the cycle S^N at least half the runs have length 1, at least one-fourth have length 2, at least one-eighth have length 3, etc., as long as the number of runs so indicated exceeds 1. Moreover, for each of these lengths, there are (almost) equally many gaps and blocks.

R3: The autocorrelation function C(t) is two-valued. That is for some integer K:

$$N.C(t)=\sum_{i=0}^{N-1}(2s_i-1)\cdot(2s_{i+t}-1)=\begin{cases}N & ,t=0\\ K & ,0\le t\le N-1\end{cases}$$

Definition (2): A binary sequence which satisfies Golomb′s randomness postulates is called a pseudo-noise sequence or a pn-sequence.

Pseudo-noise sequences arise in practice as output sequences of maximum-length linear feedback shift registers.

4. Expansion of the Golomb's Postulates

We showed before that the Golomb's postulates are applied on binary sequences. In this section we try to expand these postulates in order to be suitable to be applied on penta-sequences. We can define the penta-sequence which is satisfied the new expanded postulates, as **Pseudo Random Penta-Sequence** (PRPS).

Let S be a sequence has m distinct digits (0,1,2,3,4) with period P. Let i_j be the digit j of S, s.t. $0 \le i_j \le 4$, j=0,1,…,. In the next subsections we will introduce the new penta-digital postulates.

4.1 Penta-Digital Frequency Postulate

Its obvious that if the frequency N_i of each distinct digit i is approximate to other frequencies, then the digital sequence is satisfies this postulate, so must be:

$N_0 \approx N_1 \approx N_2 \approx N_3 \approx N_4$

Statistically, N_i represents the observed number occurrence of digit i, $0 \le i \le 4$.

The expected number of occurrence is:

$$E^*_F = \frac{P}{5} \quad \ldots(1)$$

Then, $N_i \approx E^*_F$, $\forall i \in \{0,1,2,3,4\}$

Where P is the period of the sequence.

4.2 Penta-Digital Run Postulate

The penta-digital run here can be defined as the number of similar digits which are lie between two different digits. Now we can depend on mathematical deduction to deduce the two new conditions of run postulates:

the number (R_{ij}) of kind i runs with length j is approximately equal to 1/5 of the number of runs of length j-1; $R_{ij} \approx (1/5) R_{ij-1}$, where $2 \le j \le M_i$, M_i denotes the length of maximum run of kind i. The all kinds of runs of length j are approximate to each other, s.t. $R_{0j} \approx R_{1j} \approx R_{2j} \approx R_{3j} \approx R_{4j}$, where $1 \le j \le M_i$, its obvious that:

$$\sum_{j=1}^{M_i} j.R_{ij} = N_i, 0 \le i \le 4 \quad \ldots(2)$$

$R_{ij} \approx E_{Rj}, \forall i \in \{0,1,2,3,4\}$, where E_{Rj} is the expected number of the runs with length j which can be calculated from the next theorem.

Theorem (1): Let S be a sequence satisfies the run postulate, then the expected number of runs with length j is $E_{Rj}=\frac{16P}{5^{j+2}}$, $1\le j\le M$, where $M=\max(M_0,M_1,M_2,M_3,M_4)$.

Proof

From equation (2), and $N_i\approx E^*_F$, then

$$E^*_F=\frac{P}{5}=E_{R1}+2E_{R2}+\ldots+M.E_{RM}=\sum_{j=1}^{M} j\cdot E_{Rj} \qquad \ldots(3)$$

And since $R_{i2}=\frac{R_{i1}}{5}$ then $E_{R2}=\frac{E_{R1}}{5}$, since S satisfies the runs postulate, so in general,

$$E_{Rj}=\frac{E_{R1}}{5^{j-1}},\ 2\le j\le M \qquad \ldots(4)$$

substitute equation (3) in equation (4), we get:

$$\frac{P}{5}=\sum_{j=1}^{M}\frac{j\cdot E_{R1}}{5^{j-1}}=5E_{R1}\sum_{j=1}^{M}\frac{j}{5^j} \qquad \ldots(5)$$

By using the ratio test:

as $M\to\infty$ then $S'=\lim_{j\to\infty}\sum_{j=1}^{M}\frac{j}{5^j}=\sum_{j=1}^{\infty}\frac{j}{5^j}$ is convergence series.

$$\rho=\lim_{j\to\infty}\frac{u_{j+1}}{u_j}=\lim_{j\to+\infty}\frac{j+1}{5^{j+1}}\cdot\frac{5^j}{j}=\frac{1}{5}\lim_{j\to+\infty}\frac{j+1}{j}=\frac{1}{5}$$

So that $\rho<1$.

For S′ we have,

$s_1=\frac{1}{5}$

$s_2=\frac{1}{5}+\frac{2}{5^2}$, so

$$s_M=\frac{1}{5}+\frac{2}{5^2}+\ldots+\frac{M}{5^M} \qquad \ldots(6)$$

$$\frac{1}{5}s_M=\frac{1}{5^2}+\frac{2}{5^3}+\ldots+\frac{M}{5^{M+1}} \qquad \ldots(7)$$

Subtract equation (7) from (6)

$$s_M - \frac{1}{5}s_M = \frac{1}{5} + \frac{1}{5^2} + \ldots + \frac{1}{5^M} - \frac{M}{5^{M+1}}$$

$$\frac{4}{5}s_M = \sum_{k=1}^{M}\frac{1}{5^k} - \frac{M}{5^{M+1}} = \frac{1}{5}\left(\sum_{k=1}^{M}\frac{1}{5^{k-1}} - \frac{M}{5^M}\right), \text{ then}$$

$$s_M = \frac{1}{4}\left(\sum_{k=1}^{n}\frac{1}{5^{k-1}} - \frac{M}{5^M}\right)$$

let $n \to \infty$, the series

$$S' = \lim_{M\to\infty} s_M = \frac{1}{4}\left(\sum_{k=1}^{\infty}\frac{1}{5^{k-1}} - \lim_{M\to\infty}\frac{M}{5^M}\right) \qquad \ldots(8)$$

Notice that $\lim_{M\to\infty}\frac{M}{5^M} = \lim_{M\to\infty} M.\ \lim_{M\to\infty}\frac{1}{5^M} = \lim_{M\to\infty} M.0 = 0$

Since the series is $\sum_{k=1}^{\infty}\frac{1}{5^{k-1}}$ geometric series [8] with a=1 and r=$\frac{1}{5}$, and

since |r|=$\frac{1}{5}$<1, then the series is convergence series and the sum:

$$S = \sum_{k=1}^{\infty}\frac{1}{5^{k-1}} = \frac{a}{1-r} = \frac{1}{1-1/5} = \frac{5}{4} \qquad \ldots(9)$$

substitute equation (9) in equation (8)

$$S' = \frac{1}{4}.\frac{5}{4} = \frac{5}{16} \qquad \ldots(10)$$

Substitute equation (10) in equation (5) we get:

$$\frac{P}{5} = 5.E_{R1}.\ \frac{5}{16}$$

$$\therefore E_{R1} = \frac{16P}{5^3} = \frac{16P}{5^{1+3}}$$

In general, and by using the mathematical induction, we have

$E_{Rj} = \frac{16P}{5^{j+2}}$, where $1 \le j \le M$ ■

Theorem (2): The expected number of total number E^*_R of runs of any kind i, where $0 \le i \le 4$ is $E^*_R = \frac{4P}{25}$.

Proof

$$E^*_R = \frac{16P}{5^3} + \frac{16P}{5^4} + \ldots + \frac{16P}{5^{M+2}} = \frac{16P}{5^3} \sum_{j=1}^{M} \frac{1}{5^{j-1}} \quad \ldots(11)$$

The series $\sum_{j=1}^{M} \frac{1}{5^{j-1}}$ is geometric convergence series as $M \to \infty$, then

$$\sum_{j=1}^{\infty} \frac{1}{5^{j-1}} = \frac{5}{4} \quad \ldots(12)$$

Using equation (12) in (11), we get:

$$E^*_R = \frac{16P}{5^3} \cdot \frac{5}{4} = \frac{4P}{25} \quad \blacksquare$$

By using theorem (2) we can estimate the expected number E^*_{SR} of sum of E^*_R of sum of all runs by:

$$E^*_{SR} = \sum_{i=0}^{m-1} E^*_R = 5. \frac{2P}{25} = \frac{2P}{5}$$

Notice that $E^*_{SR} = P - \frac{P}{5} = P - E^*_F$

4.3 Penta-Digital Auto Correlation Postulate

As mentioned before, that this postulate found to specify that if the tested penta-digital sequence has a repetition with itself. Let $N_0(\tau)$ denotes the number of similar digits in S after shifting it by τ, let $N_1(\tau)$ denotes the number of distinct tri-digits in S after shifting it by τ, where $1 \le \tau \le P-1$, s.t.

$N_0(\tau) = \#\{s_i = s_{i+\tau} : \forall 1 \le i \le P\}$

$N_1(\tau) = \#\{s_i \ne s_{i+\tau} : \forall 1 \le i \le P\}$,

s.t. $1 \le \tau \le P-1$.

Where $N_0(\tau) + N_1(\tau) = P - \tau$.

The probability of similarity of one digit from n digits is 1/m, then the expected number of similarity is $E^*_0=\frac{P-\tau}{5}$, and expected number of difference is:

$E^*_1=\frac{4(P-\tau)}{5}=(P-\tau)-E^*_0$.

5. Evolving the Penta-Digital Randomness Test

In this section we will reformulate the three main testing laws to be suitable to apply on digital sequence. We called the new digital randomness tests by the **Main Penta-Digital Standard Randomness Tests** (MPDSRT).

Let S be the digital sequence, which want to be tested, with length L has the element(s) i, ranged $0\le i\le 4$.

5.1 Penta-Digital Frequency Test

Let N_i represents the observed number of occurrence of digit i, where $0\le i\le 4$, and the expected number of occurrence of digit i is $E^*_F=\frac{L}{5}$, then

$$T_F=\sum_{i=0}^{4}\frac{(N_i-E^*_F)^2}{E^*_F}=\sum_{i=0}^{2}\frac{(N_i-L/5)^2}{L/5} \qquad \ldots(13)$$

With freedom degree $\upsilon=4$.

The following Lemma (1) gives more simple formula for T_F of frequency test using formula (13).

Lemma (1): For frequency test of penta-digital sequence S, $T=\frac{5}{L}\sum_{i=0}^{4}N_i^2-L$.

Proof:

$$T=\sum_{i=0}^{4}\frac{(N_i-L/5)^2}{L/5}=\frac{5}{L}(\sum_{i=0}^{4}N_i^2-2\frac{L}{5}\sum_{i=0}^{4}N_i+\sum_{i=0}^{4}\frac{L^2}{5^2})=\frac{5}{L}\sum_{i=0}^{4}N_i^2-2L+L$$

$$\therefore T=\frac{5}{L}\cdot\sum_{i=0}^{4}N_i^2-L \qquad \ldots(14)$$

■

5.2 Penta-Digital Run Test

Let R_{ij} represents the observed number of runs of kind i with length j, and let E_{Rj} be the expected number of runs of any kind with length j, then

$$T_{Ri}=\sum_{j=1}^{M_i}\frac{(R_{ij}-E_{Rj})^2}{E_{Rj}}=\sum_{j=1}^{M_i}\frac{(R_{ij}-\frac{16L}{5^{j+2}})^2}{\frac{16L}{5^{j+2}}},\ 0\le i\le 4 \qquad \ldots(15)$$

With freedom degree $\upsilon_i=M_i-1$.

A formula (15) can be reformulated in another face:

$$T_{Ri}=\frac{25}{16L}\cdot\sum_{j=1}^{M_i}5^j\cdot R_{ij}^2-2\sum_{j=1}^{M_i}R_{ij}+\frac{4L}{25} \qquad \ldots(16)$$

5.3 Penta-Digital Auto correlation Test

Let $N_0(\tau)$ and $N_1(\tau)$ represent the number of similar and distinct tri-digits of the sequence S respectively, after shifting it by τ, then the expected number of similarity and difference respectively are:

$E_0(\tau)=\frac{L-\tau}{5}$ and $E_1(\tau)=\frac{4(L-\tau)}{5}$, the following lemma proofs that chi square of auto correlation test for the digital sequence S is:

$$T_A(\tau)=\frac{(5N_0(\tau)-(L-\tau))^2}{4(L-\tau)} \qquad \ldots(17)$$

With freedom degree $\upsilon=1$.

Lemma (2): The Chi square of auto correlation test for the penta-digital sequence S shifted by τ is:

$$T_A(\tau)=\frac{(5N_0(\tau)-(L-\tau))^2}{4(L-\tau)}.$$

Proof: for simplicity, take $L'=L-\tau$, $N_0=N_0(\tau)$ and $N_1=N_1(\tau)$.

$$T_A(\tau)=\sum_{i=0}^{1}\frac{(N_i(\tau)-E_i(\tau))^2}{E_i(\tau)}=\frac{(N_0-\frac{L'}{5})^2}{\frac{L'}{5}}+\frac{(N_1-\frac{4L'}{5})^2}{\frac{4L'}{5}}$$

$$=\frac{4(N_0-\frac{L'}{5})^2+(N_1-\frac{4L'}{5})^2}{\frac{4L'}{5}}=\frac{4(N_0-\frac{L'}{5})^2+(L'-N_0-\frac{4L'}{5})^2}{\frac{4L'}{5}}$$

$$=\frac{4(N_0-\frac{L'}{5})^2+(\frac{L'}{5}-N_0)^2}{\frac{4L'}{5}}=\frac{5(N_0-\frac{L'}{5})^2}{\frac{4L'}{5}}=\frac{25(N_0-\frac{L'}{5})^2}{4L'} \quad \ldots(18)$$

$$\therefore T_A(\tau)=\frac{(5N_0(\tau)-(L-\tau))^2}{4(L-\tau)} \quad \ldots(19)$$

■

Remark (1): In the Lemmas (1) and (2), note that we have no need to calculate the expected value of any sample in the three tests, so we don't need equations (13) and (15) any more.

6. Implementation of MPDSRT on Penta-Digital Sequences

In this section we will show how we can applied the MPDSRT on arbitrarily penta-sequence with 50 digits length, using the new statistic digital laws. Let the sequence S consists of the following digits:

S="01441034200023244020123432021332444433210321223432'.

1. **Penta-Frequency test**: table (2) shows the frequency values N_i:

Table (2) frequencies of digits (0..4).

i	0	1	2	3	4
N_i	9	6	13	11	11

By using formula (14) we get:

$$T_F=\frac{5}{50}(81+36+169+121+121)-50=2.80$$

This value compared with T_0=9.52 where υ=4. The sequence S passed this test.

2. **Run test**: table (3) shows the run values R_{ij}.

Table (3) frequencies of runs (R_{ij}).

J \ I		Runs (R_{ij})				
		0	**1**	**2**	**3**	**4**
Length	**1**	6	6	11	7	3
	2	0	0	1	2	2
	3	1	0	0	0	0
	4	0	0	0	0	1

M_0=3, M_1=3, M_2=2, M_3=4, M_4=2, and M=3, by using formula (16) we get:

T^*_{R0}= 0.03125(5(36)+5^2(0)+5^3(1))-2(6+0+1)+8= 3.51845

This value compared with T_0=5.99 at υ_0=2.

Using the same formula, we obtain:

T^*_{R1}=1.61220 compared with T_1=3.84 at υ_1=1,

T^*_{R2}=3.67470 compared with T_2=3.84 at υ_2=1,

T^*_{R3}=0.76845 compared with T_3=3.84 at υ_3=1,

T^*_{R4}=20.0497 compared with T_4=7.84 at υ_4=3,

Since $T^*_{Ri} \leq T_{Ri}$ for i=0,1,2,3, but for i=4 is $T^*_{Ri} \geq T_{Ri}$ then the penta-sequence S considered failed in this test.

3. **Auto correlation test**: first, let us shift the sequence S by one shift (τ=1), then

0	1	4	4	1	0	3	4	2	0	0	0	2	3	2	4	4	0	2	0	1	2	3	4	3	2	0	2	1	3	…
	0	1	4	4	1	0	3	4	2	0	0	0	2	3	2	4	4	0	2	0	1	2	3	4	3	2	0	2	1	…

We found that there are 10 similar digits (shaded cells), so $n_0(1)=10$, and by using formula (17), then $T^*_A(1)=\frac{(5(10)-49)^2}{4(49)}=0.005$

So we can find the other $n_0(\tau)$'s by table (4).

Table (4) auto correlation test $n_0(\tau)$.

τ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$N_0(\tau)$	10	9	4	10	6	9	12	7	8	6	9	7	10	6	7
$T_A(\tau)$	0.01	0.05	3.81	0.09	1.25	1.11	0.02	1.9	0.22	0.0	0.52	0.3	0.03	1.36	0.18
τ	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$N_0(\tau)$	7	12	6	9	3	3	2	6	8	1	4	3	2	7	7
$T_A(\tau)$	0.12	0.03	6.13	0.01	1.88	1.7	1.5	2.68	0.15	2.25	3.76	0.1	0.56	1.4	2.8

Notice that $0.0\leq T^*_A(\tau)\leq 6.13$, for $1\leq\tau\leq 30$, compare all values of $T^*_A(\tau)$ with $T_A(\tau)=3.84$, where $\upsilon=1$, notice that $T^*_A(\tau)\leq T_A(\tau)\ \forall\tau$ except for $\tau=18$ s.t $T^*_A(\tau)=46.13\geq T_A(\tau)$, which is ignored. So S passes the test.

7. Testing the Penta-Digital Sequences Generated from MCGS

The sequences generated from MCG system mentioned in [9] is being tested for binary randomness test (m=2) only. In this paper we can test these sequences by using the MPDSRT.

Now we will test the penta-digital sequences with length L=5000. The penta-sequence is generated from linear MCGS (CF is XOR function) have the initial keys described in table (5).

Table (5) the parameters of MCGS.

N	q_i	α_{1i}	α_{2i}	k_i	m
2	101	2	8	1	5
	997	7	855	1	

Table (6) shows the randomness test results of the penta-digital sequence mentioned above by using MPDSRT.

Table (6) MPDSRT results of MCGS output with L=5000 for m=5.

Test	T^* Value	υ	Pass Value T_0	Decision
Freq.	2.294	4	9.52	pass
Run	1.40	3	7.84	pass
	3.49	4	9.52	
	5.73	4	9.52	
	6.62	3	7.84	
	10.99	4	9.52	
A.C.	No# of fail value $0.0 \le T(\tau) \le 9.465$ 0.07% for 500 shift	1	3.84	pass

8. Conclusions and Future Works

This work concludes the following aspects:

1. In penta-digital auto correlation test, we can applied another method to estimate $T(\tau)$, the new method applied by adding (mod 5) for the shifted sequence by τ with the origin penta-sequence S, we get a new penta-sequence S′ with length L-τ and the expected mean of occurrence of digit i is $E^*_F = \frac{L-\tau}{5}$, then applying the penta-digital frequency test using the following equation:

$$T(\tau) = \sum_{i=0}^{4} \frac{(N_i(\tau) - \frac{L-\tau}{5})^2}{\frac{L-\tau}{5}} = \frac{5}{L-\tau} \sum_{i=0}^{4} N_i^2(\tau) - (L-\tau)$$

   Where $N_i(\tau)$ is the frequency of the digit i in the sequence S′.
2. We have to expand more randomness tests, like serial, Poker,…etc. to be applied on penta-digital tests, in order to estimate the real randomness of the sequence.
3. It is importuned to show that the ciphertext of digit with base 5 is costless in size (in backup and transmitting time) then ciphertext with binary digits
4. The penta-sequence is more complicated in cryptanalysis than the binary sequence, e.g. the cipher bit 1 results from (1+0) and (0+1) while the cipher digit 1 in penta-sequence results from (0+1),(1+0), (3+3), (4+2) and (2+4).

References

[1]. Schneier, B., "**Applied Cryptography: Protocols, Algorithms, and Source Code in C**", John Wiley & Sons, New York, 2nd edition, 1996.

[2]. Motwani, R. and Raghavan, P., "**Randomized Algorithms**", Cambridge University Press, 1995.

[3]. Menezes, A. P. van Oorschot, P. and Vanstone, S., "**Handbook of Applied Cryptography",** CRC Press, 1996.

[4]. Schrift, A.W. and Shamir, A., "**Universal Tests for Nonuniform Distributions**", Journal of Cryptology, vol. 6,p. 119–133, (1993).

[5]. Gustafson, H., Dawson, E., Nielsen, L. and Caelli, W.,"**A Computer Package for Measuring the Strength of Encryption Algorithms**", Computers & Security, 13 (1994).

[6]. Gustafson, H., "**Statistical Analysis of Symmetric Ciphers**", Ph. D thesis, Queensland University of Technology, 1996.

[7]. Gustafson, H., Dawson, E., and Golić, J., "**Randomness Measures Related to Subset Occurrence**", Cryptography: Policy and Algorithms, International Conference, Brisbane, Queensland, Australia, July 1995 (LNCS 1029), p.132–143, (1996).

[8]. Gilbert, W. J. "**Modern Algebra with Applications**", Wiley-Interscince, March 2002.

[9]. Al-Azawi, F. H., "**Use the Multiplicative Cyclic Group to Generate Pseudo Random Digital Sequences**", Journal of Al-Rafidain University College for Sciences, Vol.20, p.122-135, (2006).

اختبار عشوائية متتابعات الحقل الرقمية GF(5) واستخدامها في مجال علم التشفير

م .د. أياد غازي ناصر الشمري *

مستخلص

في هذا البحث تم توسيع بديهيات Golomb للعشوائية لإنشاء قاعدة رياضية جيدة، ومن ثم تم توسيع الاختبارات الثنائية العشوائية وتحويرها لتلائم اختبار المتتابعات الخماسية التي تنتمي للحقل كالوا GF(5). في هذا البحث تم عرض فائدة المتتابعات الخماسية في حقل التشفير. تضمن عرض نتائج الاختبارات للمتتابعات الرقمية الخماسية المولدة من بعض المولدات الرقمية مثل مولد الزمرة الضربية الدوارة (MCGS).

نظام التشفير المقترح باستخدام متتابعات الحقل GF(5) سوف يضغط أو يقلل من حجم النص المشفر بالمقارنة مع أنظمة التشفير التي تعتمد على متتابعات الحقل GF(2).

الكلمات المفتاحية : بديهيات Golomb،مولد الزمرة الضربية الدوارة، متتابعات الحقل **GF(2).**

* وزارة التربية / المديرية العامة للتعليم المهني