منظومة تقنية لتأمين أمن تبادل المعلومات

د. م أحمد خضور[1]

الملخص

يدور البحث حول إيجاد تقنية مغايرة لما هو معروف على صعيد أمن المعلومات، بقصد حماية المعلومات، وزيادة مستوى الأمن، وعدم السماح لأي شخص غير مخول بالوصول إليها من اختراقها عند انتقالها من مكان إلى آخر. وقد تم التوصل إلى منظومة تقنية تعمل على رفع سوية درجة أمن المعلومات، ويمكن من خلالها أيضاً تطبيق أي من الخوارزميات المعروفة ذات الطابع البرمجي. تعتمد المنظومة المقترحة على بعض الإجراءات التقنية، وعلى مبدأ التشفير بأكثر من شكل وعلى مراحل عدّة يصعب من خلالها النفاذ إلى المعلومات المتبادلة عبر الشبكة التي تعتمد مثل هذه المنظومة. تتكون المنظومة من قسمين منفصلين عن بعضهما بعضاً، الأول من طرف المرسل، والثاني من طرف المستقبل، عمل كل منهما يكمل عمل الطرف الآخر.

الكلمات المفتاحية: مولد الأرقام شبه العشوائية، الترميز، التشفير، الكراكرز، الرماز ASCII

[1] أستاذ مساعد في قسم الهندسة الطبية– كلية الهندسة الميكانيكية والكهربائية – جامعة دمشق

A technique system for information protection and security

Dr. Ahmad Khadour[(1)]

Abstract

This search aims to finding a different technique to what is known on the common information security systems, with the aim of the protection of information and increase the level of security and not allowing any unauthorized person to access or hack when it travels between two parties apart. We achived atechnical system that upgrades the degree of information security, in which we can also apply any of the well-known software algorithms. The proposed system relies on several technical procedures and on the principle of encryption over more than one form with several stages which make it hard to access information exchanged over the network-based on system such as this. The system consists of two parts separated from each other first at the sender and the second part at the receiver, Each part complements the work of the other part.

Key words: Pseudo-Random Number Generator, Encoding, Encryption, Crackers, ASCII code

[(1)]Assistant Professor in the Biomedical Engineering Department, Electrical and Mechanical Engineering Faculty, Damascus University.

المقدمة:

إن تطوّر وسائل التواصل، وانفتاح العالم على بعضه، واعتماده على إرسال شتى أنواع البيانات خلال الشبكات، أدى إلى إحداث خطر على تسرّب البيانات المتبادلة، ووصولها إلى الأشخاص غير المخولين، بحيث أصبحت الحاجة ملحّة للحفاظ على أمن المعلومات. يعّرف أمن المعلومات باختصار، بأنه السيطرة التامة على المعلومات، من حيث تحديد من سيستلم هذه البيانات، وتحديد صلاحيّات الوصول إليها، واستخدام مجموعة من التقنيّات من أجل ضمان عدم اختراقها [1]، [3].

أصبحت شبكة الإنترنت تشكل أهم المخاطر على أمن المعلومات لوجود مجموعة كبيرة من نقاط الضعف التي تمكّن أشخاصاً غير مخوّلين من الوصول إلى البيانات المتبادلة عبر الشبكة، ومنها الأخطاء البرمجيّة التي يقوم بها المبرمجون في أثناء بناء الشبكات، أو تصميم التطبيقات، كما أنّ هناك العديد من المبرمجين الذين يقومون بتصميم برامج مخصّصة لاختراق الأنظمة، والبحث عن نقاط ضعفها[4].

يعمل هذا البحث على حماية المعلومات من الاختراق، والاستعمال غير المصرّح به، باستعمال طرائق يمكن من خلالها تأمين المعلومات عند نقلها من طرف إلى آخر من كلّ الأخطار ولاسيّما الاختراق والوصول بشكل غير شرعي إلى لمعلومات المنقولة [4]،[2] .

يعّرف الاختراق بأنّه عمليات غير شرعية تتم عن طريق فتحات موجودة في النظام يستطيع المخترق من خلالها الدخول إلى جهاز الضحية لإتمام غرض معين يسعى إليه. والمخترق هو كل شخص يقوم بعملية الاختراق والدخول إلى الأجهزة بطرق وأساليب مختلفة تمكنه من السيطرة على الجهاز والعبث بما فيه من معلومات هامة وخاصة. يوجد مخترقون يستخدمون مهارتهم العالية في الحاسوب للهجوم على الأجهزة لإثبات قدراتهم، ويطلق عليهم اسم الهاكرز Hackers. ويوجد مخترقون تكون نيتهم سيئة، وهم الأشخاص الذين ينتهكون نظام الأمن في الجهاز من أجل سرقة بيانات معينة أو تدميرها والتسبب بمشاكل خطيرة على أجهزة الحاسوب والشبكات ويسمى هذا النوع من المخترقين بالكراكرز Crackers، ويكونون عادة من المبرمجين الذين يعتمدون الوسائل البرمجية في هجماتهم على أجهزة الآخرين [5]،[2] .

من أهم الطرائق المعمول بها حالياً للمحافظة على أمن المعلومات وعدم اختراقها، نذكر:

– طرائق الحماية الماديّة: وتتمثل بالمحافظة على جهاز الحاسوب في مكان آمن، ووضع كلمة سرّ يصعب التنبّؤ بها، وتغييرها دورياً .

– استخدام الجدار الناري (Firewall): الذي يمثل تطبيقاً، يوضع عند الخادم.

– التشفير: ويُسْتَخْدَمُ فيه خوارزميات متعددة، تختلف درجة التعقيدات في هذا التشفير من خوارزمية إلى أخرى [5]، [4].

– مراقبة البيانات (Packet Sniffers) : يوجد العديد من التطبيقات التي تمّكن معرفة حركة البيانات الخارجة، والداخلة إلى الشبكة، وبتحليلها يمكن التوصل للاختراقات التي تحدث للشبكة، ومعرفة مكان الاختراق[4] .

التشفير والترميز:

بما أن موضوع التشفير يعّد من أهم الطرق المستخدمة حالياً لحماية المعلومات، نشير إلى أن التشفير"encryption" يمثل عملية تحويل، أو "بعثرة"، البيانات إلى هيئةٍ غير قابلة للفهم، وذلك لإرسالها عبر وسطٍ ناقل معين إلى جهة محددة، بحيث لا يمكن لأي جهة أخرى تفسير هذه البيانات المبهمة واستخلاص

البيانات المفهومة منها، على أن تؤمن هذه العملية أعلى درجة أمانٍ ممكنة [6].

يقابل كل عملية تشفير، عملية فك التشفير (decryption)، في الطرف المستقبل، والتي لا يمكن أن تتم إلا بمعرفة المفتاح (key) الذي اعتُمِد خلال إنشاء خوارزمية التشفير.

أما الترميز (encoding) فيمثل عملية تحويل المعلومات من هيئة معينة إلى هيئة أخرى وفق نظامٍ محدد، فالبرامج المكتوبة بلغات البرمجة المختلفة، وأطقم الحروف المختلفة للغات، كاللاتينية والعربية الممثلة بشيفرات ASCII وASMO وغيرها، المستخدمة في أنظمة التشغيل المختلفة، هي بعض أنواع الترميز. وتحتاج الملفات والهيئات المختلفة إلى برامج تحول هذه الهيئة المرمزة إلى نظام مفهوم، أي "فك ترميزها". ويمكن بمقارنة عملية الترميز مع التشفير، أن نُعدَّ التشفير أحد أنواع الترميز، المرتبط بموضوع السرية.

فالترميز لا يُعنَى كثيراً بموضوع السرية أو الأمان، أمَّا التشفير، فهو عملية "ترميز" معقدة وسرية، تتبع خوارزميات معينة لطمس هوية البيانات، ومنع كل من لا يمتلك المفتاح، من تفسيرها، والإفادة منها [4]،[1].

تطورت عمليات التشفير، ودخلت فيها مفاهيم جديدة، أصبحت جزءاً منها، كمفهوم تدقيق الشرعية(authentication)، المتمثل بعمليات إلكترونية، مثل التوقيع الرقمي.

تتألف عملية التشفير من العناصر الآتية:

1- المعلومات التي ستجرى لها عملية تشفير، وقد تكون رسالة نصية، أو إشارات كهربائية مشفرة وغيرها.

2- خوارزمية التشفير لتحويل المعلومات إلى بياناتٍ مبهمة، وخوارزمية فك التشفير التي تعيد هذه البيانات إلى حالتها الأصلية.

والخوارزميات بشكل عام هي عبارة عن دوال رياضية محددة، يزداد عامل الأمان الذي توفره، بازدياد تعقيدها.

3- المفتاح، وهو سلسلة أو أكثر من الرموز تتسلمها الخوارزميات المتبعة، وتطبقها على البيانات لتشفيرها [2]،[1] .

تتبع أنظمة التشفير بحسب المفاتيح المستخدمة أسلوبين مختلفين للتشفير، هما:

أولاً: تشفير المفتاح السري (secret-key) SKE (encryption)، ويستخدم هذا النظام المفتاح ذاته في عمليتي التشفير وفك التشفير. ويعتمد هذا النوع على اتفاق الطرفين المرسل والمستقبل للمعلومات المشفرة، على مفتاح سري واحد. ويعرف هذا النوع من التشفير بالتشفير المتناظر (symmetric cryptography). مثل نظام Data Encryption Standard

ثانياً: نظام المفتاح العام (public-key) PKE (encryption)، ويستخدم زوجاً من المفاتيح: أحدهما يدعى المفتاح العام Public key، ويُعْلَنُ عنه للجهات جميعها التي تتبادل المعلومات، وهو المفتاح المستخدم لتشفير البيانات، والآخر المفتاح الخاص Private key، وهو المستخدم لفك التشفير، ويبقى هذا المفتاح سراً عند الجهة المستقبلة، فتزول بذلك، ضرورة تبادل المرسل والمستقبل المفتاح، الذي قد يتعرض للكشف خلال عملية التبادل. بالطبع تحدد قوة نظام التشفير بناءً على الخوارزمية المتبعة وطول المفتاح المستخدم، ويزداد عامل الأمان كلما زاد طول المفتاح. ويعدُّ نظام RSA ونظام Digital Signature Algorithm، أشهر الأنظمة التي تعتمد على هذا التشفير [5].

تقنيات التشفير:

من أشهر التقنيات المعمول بها حالياً، نذكر:

- تقنية مقاييس تشفير البيانات DES (Data Encryption Standard)، إذْ يُرَكَبُ هذا النظام بشكلٍ عتادي، عكس كثيرٍ من أنظمة التشفير التي تعتمد على أنظمة برمجية. ويعدُّ غير قابل للاختراق، بسبب الخوارزمية التي يتبعها.

- نظام مقاييس التشفير المتطورة AES (Advanced Encryption Standard) إذْ تقرر نهاية عام 1998 أن يستبدل بنظام DES للتشفير نظام AES، الذي يعتمد على تقنية تشفير الكتل (block cipher) ،

- نظام أو تقنية الخصوصية الجيدة PGP

(Pretty Good Privacy)، ويعتمد هذا النظام على طريقة المفتاح العام (PKE)، ويضم عدداً من الأنظمة الضمنية التي يختص كل منها بوظائف محددة، ويؤمن بذلك سرعةً عاليةً في إنجاز عمليات التشفير، تزيد كثيراً على التي كانت متبعة قبله [1].

- نظام RSA القياسي: وهو يعتمد على طريقة المفتاح العام. ويعدُّ التعامل مع نظام RSA أسهل من نظام DES، مع أنَّه أقل سرعةً وأقل أماناً. ومن أساسيات هذا النظام، احتواؤه على توقيع رقمي (digital signature) يميز المرسل.

- تشفير المنحنى الإهليجي ECC (Elliptic Curve Cryptography)

ويعّد تطبيق هذه الخوارزميات أسهل وأكثر فعالية من كثير من الأنظمة الأخرى المتبعة. ويعتبر من أنسب أنظمة التشفير التي يمكن استخدامها في الاتصالات المتحركة، وذات العتاد صغير الحجم، كأنظمة الهواتف النقالة.

يضاف للعديد من لتقنيات التشفير بروتوكولات التشفير ومن أكثر هذه البروتوكولات انتشاراً:

- بروتوكول التحويلات الإلكترونية الآمنة Secure) Electronic Transaction) ويدعم هذا البروتوكول SET نظامي DES وRSA، ويضم عدداً من البروتوكولات الضمنية الأخرى.

- بروتوكول طبقة المقابس الآمنة Secure) SSL Sockets Layer) الذي لا يرتبط مع التطبيقات التي يعمل عليها. ويسمح هذا الأسلوب لبروتوكولات أخرى مثل (HTTP) و(FTP) و(Telnet)، أن تعمل في طبقةٍ خاصةٍ بها بشكلٍ شفاف، بحيث لا تتعارض معه. ويستخدم البروتوكول عدداً من الخوارزميات المختلفة في مراحله المختلفة.

- البروتوكول الآمن لامتدادات بريد إنترنت متعدد الأغراض S/MIME (Secure/ Multipurpose Internet Mail Extensions) وهو البروتوكول المسؤول عن التواقيع الرقمية، وعمليات التشفير في رسائل إنترنت التي تتبع هيئة MIME. وتسمح هذه الهيئة لرسائل البريد الإلكتروني أن تتضمن نصوص محسنة وصور وفيديو [4].

الدراسات المرجعية:

لا يتضمن البحث فقرة واضحة المعالم عن الدراسات المرجعية، كما هو مفترض ومعتاد، لأنَّه ينطلق بالأساس من أفكار مقتبسة من تصفح بعض المواقع والمقالات العلمية من الانترنيت، ومطالعة بعض المراجع عن أمن المعلومات والدارات المتكاملة وغيرها من المراجع التي قد يطول تعدادها، وترجمة بعض هذه الأفكار بمنظومة تجريبية تقوم على تشفير المعلومات المراد إرسالها من طرف إلى آخر بأسلوب مغاير لما هو معروف. بالطبع بحوث ودراسات أمن المعلومات احتلت مساحة واسعة من بين أبحاث تقنية المعلومات المختلفة، ولا يتسع المجال هنا للدخول بتفاصيل التقانات والخوارزميات المستخدمة، علماً

أن معظم الخوارزميات المعتمدة لتأمين حماية المعلومات وأمنها ذات طابع برمجي يمكن اختراقها بدرجات متفاوتة [4], [5].

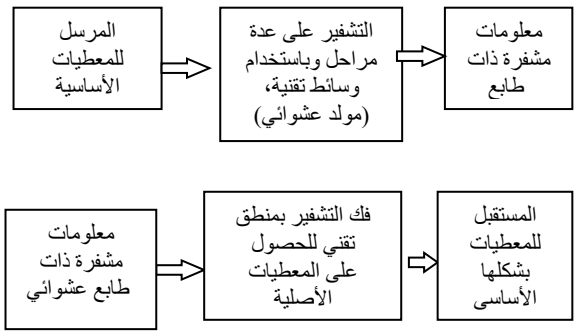
لم يتم في هذا البحث اقتباس أي شيء محدّد من المقالات والمراجع العلمية حتى تتم الإشارة له، بل يمثل أفكار تم العمل على تطويرها كمنظومة تقنية يمكن تضمينها أي نوع من الخوارزميات المهمة والمعروفة على صعيد أمن المعلومات (مثل خوارزمية RSA المشهورة)، فضلاً عن إجراءات تقنية إضافية للتشفير تستخدم قبل تطبيق أي خوازمية وبعدها يتم اعتمادها، بحيث يصعب اختراق المنظومة الهجينة بوجود إجراءات تقنية وبرمجية بوجود تقنيات تشفير وفك تشفير في كل منها على حدة.

المقترح Proposal:

مع أنَّه لا يمكن التأكيد بوجود نظام أمن مطلق الحماية، إلَّا أنَّه يوجد بعض الخوارزميات ذات الطابع البرمجي المعمول بها والتي يصعب اختراقها مثل خوارزميات RSA و OTP وغيرها[3]. سيعتمد بهذا البحث مبدأ الترميز بشكل مغاير والتشفير من خلال تطوير منظومة تعمل على تشفير البيانات تقنياً على مراحل عدّة وبأشكال مختلفة، تجعل من الصعوبة لأي شخص غير مخول بالوصول إلى المعلومات خلال نقلها من طرف إلى آخر. هَدَفَ البحث إلى تأمين أمن تبادل المعلومات بإضافة اجراءات تقنية (إضافة لبعض الاجراءات البرمجية) يصعب التنبؤ بمخرجاتها، تحدّ من قدرات المخترقين المحترفين المعروفين بالكراكرز على أي اختراق للمنظومة المقترحة.

يتمثل المخطط العام للبحث بالشكل1، الذي يتكون من قسمين أساسيين، بحيث يظهر القسم الأول (العلوي من الشكل) الإجراءات التقنية المعتمدة من طرف المرسل، والقسم الثاني (السفلي) الإجراءات المعتمدة من طرف المستقبل يضاف لذلك تقنيات التشفير وفك التشفير المستخدمة في كل منهما على حدة.

تم الانطلاق في تصميم المنظومة التقنية، من أن الأحرف جميعها باللغة الانكليزية بشكليها الكبير والصغير، والأرقام العربية والرموز المتداولة في كتابة النصوص والعلاقات الرياضية توجد في كود (رماز) ASCII بين القيمتين 20H و 7EH واعتماد ترميز جديد وفق ما هو مبيّن بالجدول1، يتمثل بإلغاء التراكيب المقابلة لبعض الوظائف وأوامر التحكم بالتراكيب من "0000 000" حتى "1111 001" جميعها واعتماد ترميز جديد يتمثل باستخدام أرقام عشرية للرموز والأرقام والأحرف، ابتداء من أول رمز SP في جدول الـ ASCII بالرقم 1 حتى الإشارة ~ بالرقم 95 بالترتيب والتسلسل نفسه الواردة فيه، وهذا هو الشكل الأول المعتمد في التشفير. تخزن القيمة الثنائية المقابلة لكل رمز من ASCII يراد إرساله من موضع لآخر بمسجل من نوع



الشكل (1) التركيبة التقنية لمنظومة تأمين أمن تبادل المعلومات لدى كل من المرسل والمستقبل.

SISO (Serial in Serial out) مكون من سبع قلابات بطول كود ASCII بالترتيب:

$D_6D_5D_4D_3D_2D_1D_0$،

الجدول (1) القسم الأساسي من جدول ASCII المعتمد بالمنظومة التقنية

	$b_7b_6b_5b_4$ ، $b_7 = 0$					
$b_3b_2b_1b_0$	010	011	100	101	110	111
0000	1- SP	17- 0	33- @	49- P	65- '	81- p
0001	2- !	18- 1	34- A	50- Q	66- a	82- q
0010	3- "	19- 2	35- B	51- R	67- b	83- r
0011	4- #	20- 3	36- C	52- S	68- c	84- s
0100	5- $	21- 4	37- D	53- T	69- d	85- t
0101	6- %	22- 5	38- E	54- U	70- e	86- u
0110	7- &	23- 6	39- F	55- V	71- f	87- v
0111	8- '	24- 7	40- G	56- W	72- g	88- w
1000	9- (	25- 8	41- H	57- X	73- h	89- x
1001	10-)	26- 9	42- I	58- Y	74- i	90- y
1010	11- *	27- :	43- J	59- Z	75- j	91- z
1011	12- +	28- ;	44- K	60- [	76- k	92- {
1100	13- ,	29- <	45- L	61- \	77- l	93- |
1101	14- -	30- >	46- M	62-]	78- m	94- }
1110	15- .	31- =	47- N	63- ^	79- n	95- ~
1111	16- /	32- ?	48- O	64- _	80- o	

تم بالخطوة الثانية من تصميم المنظومة، إعادة ترميز كود ASCII بإعادة ترتيب المعطيات ليصبح الجدول المعتمد للرموز والأرقام والأحرف وفق الجدول (2) .

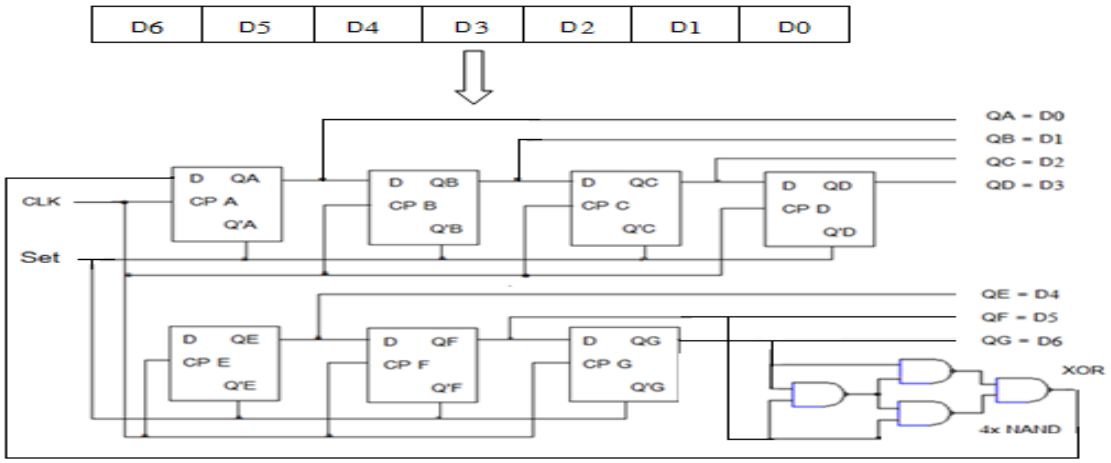
الجدول (2) الترميز العشري للرموز الأساسية بجدول الـ ASCII

الرمز بالـ ASCII	الكود المقابل	$D_6D_5D_4$ $D_3D_2D_1D_0$	الترميز العشري	$Q_GQ_FQ_E$ $Q_DQ_CQ_BQ_A$
SP	20H	010 0000	1D	000 0001
!	21H	010 0001	2D	000 0010
"	22H	010 0010	3D	000 0011
#	23H	010 0011	4D	000 0100
$	24H	010 0100	5D	000 0101
…	…	……..	…	…….
x	78H	111 1000	89D	101 1001
y	79H	111 1001	90D	101 1010
z	7AH	111 1010	91D	101 1011
{	7BH	111 1011	92D	101 1100
|	7CH	111 1100	93D	101 1101
}	7DH	111 1101	94D	101 1110
~	7EH	111 1110	95D	101 1111

يلي ذلك في الخطوة الثالثة، تصميم مولد عشوائي للأعداد، يضم جميع التراكيب من "0000 010" حتى "1110 111" ولكن بشفرات جديدة مقابلة لها من "000 0001 حتى "111 101".

يتكون المولد العشوائي للأعداد فضلاً عن السجل (أو المسجل Register) الذي يحتفظ بشيفرة الرمز المراد إرساله إلى سجل آخر نوع SIPO (Serial in Parallel out) وشبكة منطقية خاصة تعمل على استنباط المدخل التسلسلي للسجل من القلابات المكونة له، بحيث كل قيمة مدخلة للسجل يتولد من أجلها قيمة عشوائية ثنائية جديدة. يمكن تغير التشفير بتغير مخارج القلابات التي تعتمد كمدخل للشبكة المنطقية التي تغذي مدخل السجل الأساسي. جرى في التصميم المعتمد أخذ مخارج آخر قلابين في السجل Q_GQ_F لتشكيل مدخل السجل الأساسي. وباعتماد قلابات مثل القلاب D مثلاً يكون المخطط المنطقي لمولد القيم العشوائية وفق ما هو مبين بالشكل2، الذي يظهر مخارج القلابات المكونة للسجل للتعامل معها في مرحلة لاحقة كمداخل لسجل ثالث يعتمد بالطرف الثاني لفك التشفير[6].

يظهر الشكل2، المنطق الإضافي البسيط المستخدم لتوليد المدخل التسلسلي للسجل وهو يكافئ بوابة XOR (منفذة باستخدام أربع بوابات NAND) يعمل مع كل نبضة ساعية



الشكل(2) مولد لقيم ثنائية بشكل عشوائي

على المقارنة بين خرجي آخر قلابين بالسجل لإدخال "0 " (في حال تماثل الخرجين) أو "1" على مدخل السجل، بحيث المعطيات الأصلية المراد إرسالها D6….D0 أصبحت تقابل بالمولد العشوائي المخارج QA…. QG، ويتم كإجراء تقني إضافي بالمرحلة التالية قلب ترتيب مكونات السجل عند التشفير لجعله بالترتيب المبين أدناه:

	MSB						LSB
معطيات الدخل	D0	D1	D2	D3	D4	D5	D6
المعطيات العشوائية المقابلة على الخرج	QA	QB	QC	QD	QE	QF	QG

بحيث الـ LSB يصبح مقابل الـ D6 (QG) وبيت الـ MSB يقابل D0 (QA). وبالانطلاق من القيمة $D_6D_5D_4D_3D_2D_1D_0$ = 111 1111 بجعل Set = 1 للمقابلات كلّها المستخدمة بالسجل (قلابات بمداخل مباشرة)، يصبح جدول الحالات للسجل بالترميز الجديد المعتمد، وفق ما هو مبين بالجدول (3)، حيث

يمكن من سجل مكون من 7 bits تشكيل 128 توافقية (تركيبة) مختلفة.

الجدول(3) القيم العشوائية المتولدة من مولد الأعداد العشوائية

تسلسل التنقلات	الرمز بدخل المولد	القيمة العشوائية المتولدة ثنائيا
0	start	1111 111
1	^	0111 111
2	=	0011 111
3	.	0001 111
4	&	0000 111
5	"	0000 011
6	SP	0000 001
7	_	1000 000
8	?	0100 000
9	/	0010 000
10	'	0001 000
11	#	0000 100
12	!	0000 010
...	.....	.....
121	t	1010 101
122	Don't	1101 010
123	Don't	1110 101
124	Don't	1111 010
125	Don't	1111 101
126	Don't	1111 110

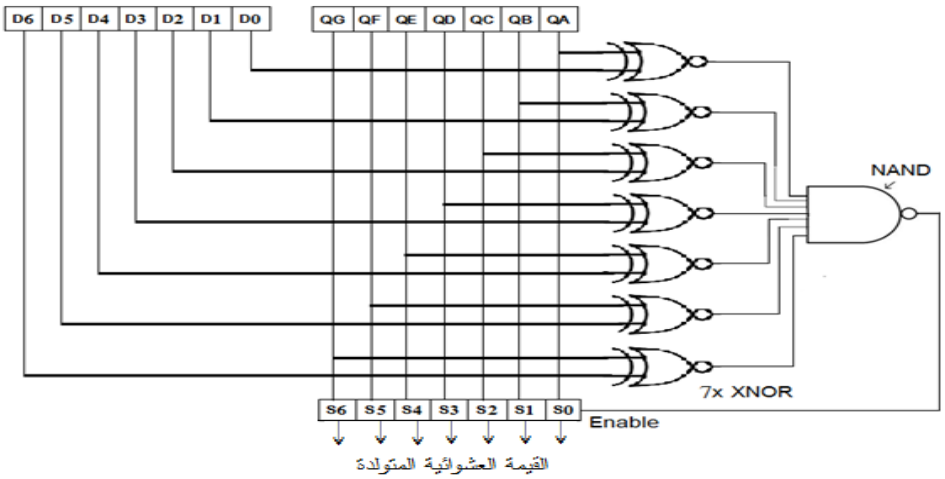
وبما أن أعلى رقم عشري مستخدم بالتصميم هو $(101\ 1111)_2 = (95)_{10}$ فإن كافة التراكيب التي تقابل أعداد عشرية أكبر من $(95)_{10}$ تهمل وتعامل كحالة عدم تعين (Don't care) وهي كافة التراكيب التي فيها D6D5 = 11.

يتضح من الجدول3 أن المقارنة بين أعلى بتين بالسجل، أي $D_5 \oplus D_6 = 1 \oplus 1 = 0$ ابتداء من القيمة 1111 111 التي يتولد عنها التركيبة (011 1111) ينقل الناتج منها إلى مدخل السجل (QA الذي يقابل D0) وتزاح بقية البيانات نحو اليمين مع قدوم النبضة الساعية التالية لينتج الكود المقابل للرمز "^" المقابل للرقم 63 وفق الترميز المعتمد. يفترض أن يظهر بالجدول 128 توافقية (من 0 وحتى 127). وقد ظهر فقط 127 تركيبة، وهي التراكيب الممكنة جميعها لـ 7 bits عدا التركيب "000 0000". التي لا يمكن توليدها بالمولد المعتمد، إذْ إن وجود مثل هذه التركيبة بالمولد لا يؤدي إلى أي تركيبة أخرى، ومن ثُمَّ المولد المشار إليه أعلاه مولد تام للأعداد العشوائية، بل يمكن تسمية مثل هذا المولد، بمولد الأعداد شبه العشوائية Pseudo-Random Number Generator. يمكن من الجدول (3)، تحديد كافة التراتيب والرموز التي سيتم التعامل معها من جدول الـ ASCII وعددها 95 تركيبة. أي أن هذا المولد يولد مع كل نبضة ساعية قيمة عشوائية بالاسم والترتيب $S_6S_5S_4S_3S_2S_1S_0$ للتميز وهي القيمة العشوائية المتولدة والمرسلة، أما التراكيب التي يمكن اعتبارها كحالة عدم تعين d يمكن تحديدها من الجدول (3) أيضاً وعددها 32 تركيبة إضافة إلى تركيبة الصفر (المجموع 33 تركيبة بما فيها التركيبة العائدة للأمر Del بالتركيبة 111 1111)، وهي كافة التراكيب التي يكون فيها S_6S_5 = 11.

يقسم التصميم إلى جزأين يختلف كل منهما عن الآخر بحسب موقعه إن كان من طرف المرسل أم من طرف المستقبل والجزءين هما:

الأول– من طرف المرسل:

يخصص سجل أول بطول 7 bit لتخزين الترميز المقابل للرمز المراد إرساله بالترتيب $D_6D_5\ldots D_0$ ويقارن هذا الترميز تقنياً مع خرج المولد بالترتيب المقابل $Q_GQ_E\ldots.Q_A$ والمتواجد بسجل ثاني، باستخدام مقارن بسيط مكون من بوابات XNOR وبوابة NAND بسبع مداخل وفق ما هو مبين بالشكل3. عند تساوي القيمتين، يتم اعتماد الرقم العشوائي المتولد بالتسمية والترتيب $S_6S_5S_4S_3S_2S_1S_0$ في سجل ثالث، بحيث إن Q_A يقابل S_0 وQ_G يقابل S_6 ويرسل هذا الترميز الجديد إلى المستقبل. يلي ذلك استخدام الخوارزمية البرمجية (مثل RSA التي تطبق على الترميز الجديد).



الشكل(3) دارة توليد واعتماد القيمة العشوائية المتولدة لأي رمز من قبل المرسل

الثاني– من طرف المستقبل:

بعد وصول الكود المشفر تقنياً من المرسل إلى الطرف الثاني وفك التشفير الداخلي، تبدأ عملية تشكيل التوابع المنطقية التي تعيد

الكود العشوائي الذي تم استقباله إلى أصله $D_6D_5D_4D_3D_2D_1D_0$. وللوصول إلى توابع التحويل المناسبة، نشكل جدول للحقيقة فيه الدخل هو الترميز العشوائي القادم من طرف المرسل والخرج هي المعطيات الأساسية (ألأصلية) لطرف المستقبل. يظهر الجدول4 القيمة الأصلية المفترض الحصول عليها مقابل كل شفرة عشوائية مولدة من طرف المرسل.

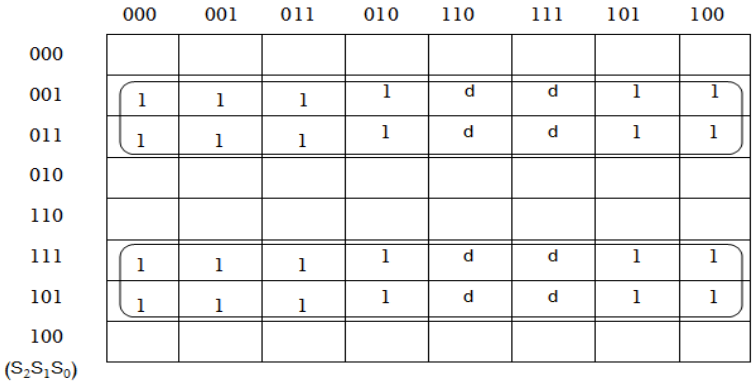
الجدول (4) القيمة الأصلية المقابلة لكل قيمة مشفرة

الترتيب العشري	Inputs S_6 S_5 S_4 S_3 S_2 S_1 S_0	Outputs D_6 D_5 D_4 D_3 D_2 D_1 D_0	الترتيب المتولد
64	1 0 0 0 0 0 0	0 0 0 0 0 0 1	1
65	1 0 0 0 0 0 1	0 0 0 0 0 1 0	2
1	0 0 0 0 0 0 1	0 0 0 0 0 1 1	3
2	0 0 0 0 0 1 0	0 0 0 0 1 0 0	4
66	1 0 0 0 0 1 0	0 0 0 0 1 0 1	5
67	1 0 0 0 0 1 1	0 0 0 0 1 1 0	6
110	1 1 0 1 1 1 0	1 0 1 1 1 0 1	93
111	1 1 0 1 1 1 1	1 0 1 1 1 1 0	94
47	0 1 0 1 1 1 1	1 0 1 1 1 1 1	95

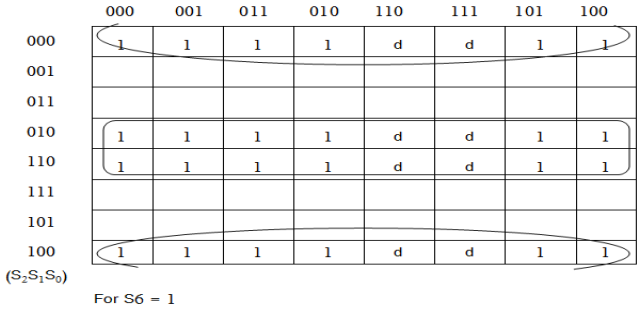
بمعنى أنه للحصول على الرقم "1" الذي يرمز في جدول الـ ASCII للمسافة Space بالترميز $D_6D_5D_4D_3D_2D_1D_0$ = 000 0001 يجب أن يكون الترميز العشوائي المستقبل من الشكل $S_6S_5S_4S_3S_2S_1S_0$ = 100 0000، الذي يمكن منه تحديد التوابع من D0 وحتى D6 بدلالة المداخل S0…S6 وذلك بتمثيل التوابع السبعة بمخططات K-map كل على حدة.

المخطط المقابل لكل تابع يتكون من 2^7 = 128 خلية. فمثلاً من أجل تابع الخرج D0 تمثل المداخل S6…S0 من أجل كل خلية يكون فيها D0 = 1 ومن أجل القيم التي هي أكبر من 95 نمثل في الجدول حالة عدم التعين d ليتم استخدامها بحسب الحلقة التي تضم الواحدات المتجاورة، بحيث يمكن احتساب d = 1 في حال امكانية تشكيل حلقة وجعلها أكبر ما يمكن. وبعكس ذلك تحسب d = 0. برسم الحلقات المناسبة وبكتابة المقابل لكل حلقة يكون

التابع: D0(S6,S5,S4,S3,S2,S1,S0)



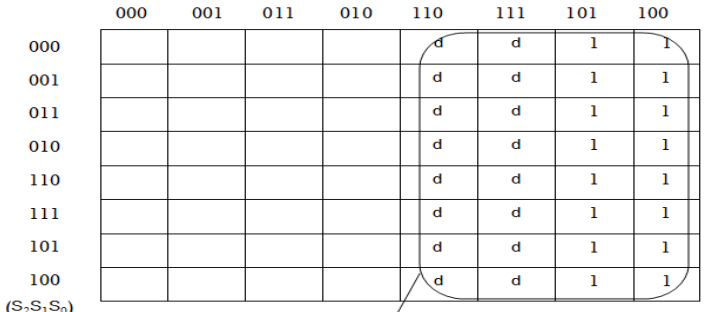
For S6 = 0



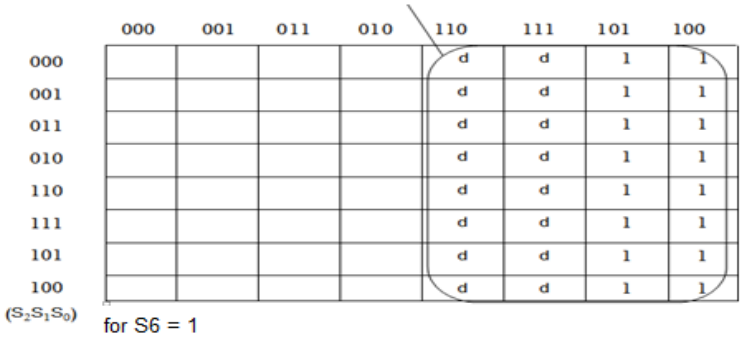
For S6 = 1

$$D0 = S'6S'2S0 + S'6S2S0 + S6S1S'0 + S6S'1S'0$$

التابع: D6(S6,S5,S4,S3,S2,S1,S0)



For S6 = 0



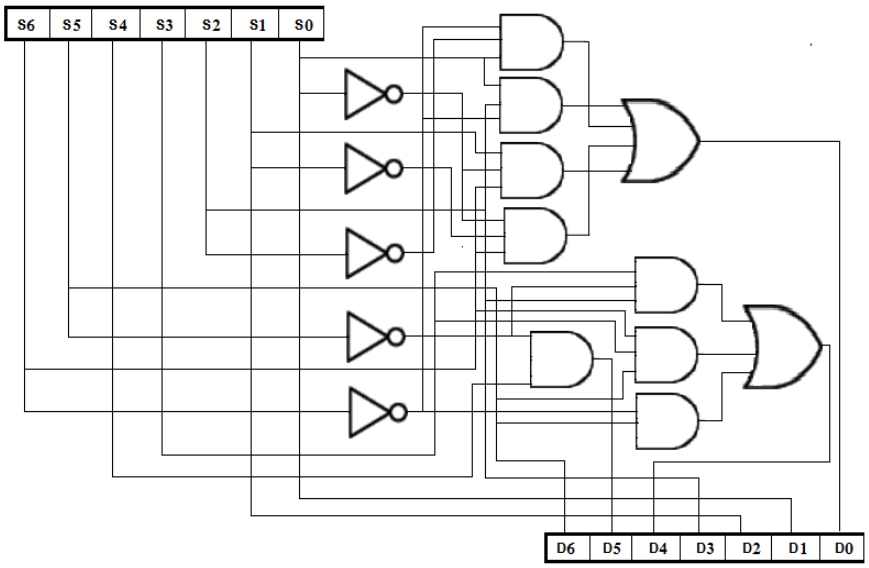
for S6 = 1

$$D6 = S5$$

اكْتُفِيَ بتمثيل التابعين D0 وD6، وبأسلوب مماثل يمكننا أن نمثل بقية التوابع، فنحصل على التوابع الآتية:

$$D1 = S0$$
$$D2 = S1$$
$$D3 = S2$$
$$D4 = S'5S3 + S'6S5S2 + S6S5S3$$
$$D5 = S'5S4$$

ويمكن رسم الشبكة المقابلة لمجمل التوابع السبعة بوجود مسجل الدخل الذي يحتوي على الرمز المشفر ومسجل الخرج الذي يحوي على الشكل الأصلي المقابل للرمز المشفر وفق المخطط المبين بالشكل (4)، الذي يضم مجموعة من البوابات المنطقية المقابلة للتوابع التي تم التوصل اليها، لتشكيل مجمل المنظومة التقنية. يمكن ضمن المنظومة التقنية بين المرسل والمستقبل استخدام أي خوارزمية برمجية أخرى لتأمن درجة الأمان المناسبة لتبادل المعلومات بين طرفين متباعدين.



الشكل(4) دارة فك التشفير لدى المستقبل وإعادة كل رمز للشكل الذي أرسل منه

طريقة عمل أو استخدام المنظومة

تتكون المنظومة التقنية التي تم تطويرها لتأمين أمن المعلومات من جزءين أحدهما من طرف المرسل والثاني من طرف المستقبل، إذْ يمكن وضع الجزء الأول بأي شبكة حاسوبية كما يوضع المواديم عند الطرف الأول (المرسل) والجزء الثاني عند الطرف الثاني (المستقبل). بعد الترميز والتشفير التقني في المرحل الأولى من إرسال أي رسالة من طرف المرسل تبدأ عملية التشفير الثانية لأي رمز مشفر بإنتاج المفاتيح (العام والخاص) لتشفير أي رسالة يراد ارسالها من طرف لآخر وفق الآتي:

1- نختار عددين أوليين عشوائيين كبيرين مختلفين p و q.

2- نحسب n = p.q حيث n يستخدم كمعامل لكلا المفتاحين العام والخاص.

3- نحسب الدالة Ø(n) = (p-1)(q-1) التي تعطي عدد الأعداد الأولية بين 2 و n والتي هي أولية مع n، بحيث إن القاسم المشترك الأكبر (greater common division) GCD(n, i) = 1 من أجل $2 \le i \le n$.

4- نختار عدد صحيح e بشكل عشوائي (كأس عمومي)، إذْ $2 \le e \le Ø(n)$ و GCD(Ø(n), e) = 1، (e و Ø(n) أوليين فيما بينهما).

5- نوجد قيمة المفتاح الخصوصي d (كأس خصوصي)، بحيث يحقق العلاقة الآتية:

ويحسب d.e = 1 (mod(Ø(n))

باستخدام خوارزمية اقليدس الموسعة. وبعد الحصول على المفتاح العام (n_A, e_A) والمفتاح الخاص السري (n_A, d_A) للطرف الأول (المرسل)، والمفتاح العام

(n_B, e_B) والمفتاح الخاص السري (n_B, d_B) للطرف الثاني (المستقبل)، تبدأ عملية التشفير للرسالة m من قبل المرسل بالعلاقة: $c = m^{eB} mod(n_B)$.

يمكن فك التشفير من قبل المستقبل باستخدام المفتاح الخاص(n_B, d_B) وفق العلاقة: $m=c^{dB} mod\ (n_B)$، إذْ يتم الحصول على الرمز بالشكل الذي شفر به تقنياً من قبل المرسل، ليتم بعد ذلك ارجاع هذا التشفير إلى شكله الأصلي تقنياً أيضاً باستخدام دارات فك التشفير لدى المستقبل.

النتائج ومناقشتها:

تتمثل أهم نتيجة تم التوصل إليها من خلال هذا البحث، بتصميم منظومة تقنية قابلة للتنفيذ، بكلفة مادية بسيطة مقابل تأمن درجة عالية لأمن المعلومات التي يتم تبادلها باستخدام مثل هذه المنظومة. شُفِّرَتْ بالمنظومة المقترحة البيانات على أكثر من مرحلة وبأكثر من شكل، إحداها توليد أرقام عشوائية بشكل يصعب فيه على أي شخص اختراق المعلومات عبر المنظومة. ويمكن ملاحظة درجة الأمن التي تؤمنها المنظومة من سياق العرض الوارد أعلاه، إذْ يصعب اختراق المنظومة، لأنَّ الاختراق يتطلب الوصول إلى الجزءين الرئيسين للمنظومة المتباعدين عن بعضهما بعضاً، كما أن الوسائل البرمجية المتبعة في هجمات المتطفلين على أنظمة الآخرين لم تعد تجدي نفعاً بوجود الإجراءات التقنية المتبعة والأشكال المتعددة للتشفير، إذ إن اكتشاف أي إجراء من قبل الـ Hackers وحتى الـ Crackers يليه إجراء ثاني وثالث يصعب التوصل إليه إلا بالتوصل للمنظومة بكاملها، وهذا غير ممكن لدى جهات عامة أو خاصة تحرص على أمن معلوماتها. ولمقارنة نتائج هذا البحث مع غيرها من النتائج التي تم التوصل إليها على صعيد أمن المعلومات، لم يتسنى معرفة منهجية مماثلة لتأمين أمن المعلومات للمقارنة معها والحكم على درجة الآمن التي تؤمنها هذه المنظومة مقارنة مع غيرها، وهذا كان السبب في صعوبة عملية النمذجة والمحاكاة للنتيجة بوسائط برمجية (مثل الماتلاب) لمثل هذه الحالة. لكن من طرف آخر تعتبر التقنية المستخدمة في البحث أقرب ما تكون لتقنية مقاييس تشفير البيانات DES التي تعتبر من التقنيات غير قابلة للاختراق، نظراً لتركيب المنظومة بشكل اعتادي Hardware. الطريقة الوحيدة لاختراق المنظومة هو الوصول إلى المنظومة نفسها بجزأيها (من طرف المرسل والمستقبل)، وتجريب كافة الاحتمالات الممكنة للمفتاح المستخدم بالخوارزمية المستخدمة بالمنظومة، علماً أن أطوال المفاتيح المستخدمة في عمليات التشفير تراوح ما بين 40 إلى 2048 bits، مع العلم أن المفتاح لا يُعتَبر ذو عامل أمان مرتفع، حسب التقنيات الموجودة الآن، إلا إذا كان طوله يساوي أو يزيد على 128 bits، وتحسب الاحتمالات الممكنة في هذه الحالة من العلاقة "2 طول المفتاح" حيث إن طول المفتاح يساوي عدد البتات التي يتكون منها ومن ثُمَّ هذا له عدد كبير من الاحتمالات يصعب تصورها.

REFERENCES

[1] David Basin, Patrick Schller, Michael Schlapfer, Applied Information Security, Springer, 2011

[2] Jason Andress, THE BSSICS OF INFORMATION SECURITY, Second Edition, Elsevier Inc., 2014

[3] William Stallings, Lawrie Brown, Computer Security: Principles and Practice,3th Edition, Pearson Education Limited, 2015

[4] Variety Internet Websites about information and computer security

[5] Orr Dunkelman, Liam Keliher, 22nd International Conference, Selected Areas in Cryptography, SAC 2015 Canada.

[6] Ljupco Kocarev, Shiguo Lian, Chaos-Based Cryptography, 2011, Springer.

[7] الدكتور أحمد خضور، الدارات المنطقية، من منشورات جامعة دمشق، 2016

Received	**2017/02/07**	**إيداع البحث**
Accepted for Publ.	**2018/01/15**	**قبول البحث للنشر**