Development Hyper Algorithm for Encryption Arabic Text using Mors Code

Najla Dabagh **Melad jader saeed** **Subhi Hamadi**

meladjader@uomosul.edu.iq *subhi53@alnoor.edu.iq*

College of Computer Science and Mathematics, University of Mosul, Iraq

Received on: 18/12/2006 **Accepted on: 05/03/2007**

ABSTRACT

Morse code is considered as one of the codes that are used to transfer information among long distant areas.

The research concentrates on Morse code applications, transmissions to overcome weakpoints, a necessary mixture between coding and cryptography to get benefits from the properties of each one of them to increase the secrecy of morse code transmission.

Anew algorithm was put in use for encryption and decryption which passes through multistage process, each stage has special properties that make the transmission more confident and safer than the stage before.

In addition to the ability of using password as a key, which is at the same time passed through the same encryption processes which make it hard to break.

This work is applied on integrated programming environoment which is (MATHCAD).

Keywords: Codes, Morse Code, Binary Code, Complement, Fixed length code, Cipher system

تطوير خوارزمية هجينة لتشفير النصوص العربية باستخدام شفرة مورس

صبحي حمادي حمدون **نجلاء بديع الدباغ** **ميلاد جادر سعيد**

كلية علوم الحاسبات والرياضيات

جامعة الموصل

تاريخ الاستلام: 18/12/ 2006 *تاريخ القبول: 5/3/2007*

الملخص

رمز مورس من الرموز المستخدمة في عمليات إرسال المعلومات بين المناطق البعيدة. تم التركيز في هذا البحث على دراسة هذا الرمز والتعرف على الوسائل والطرائق الأكثر استخداماً لإرساله. ومن ثم تم تحديد نقاط الضعف الموجودة في طريقة استخدام وإرسال هذا الرمز.تم تجاوز نقاط الضعف بربط الترميز مع التشفير للاستفادة من خصائص كل منهما لزيادة سرية الرسالة المنقولة ، ولهذا تم استحداث خوارزمية جديدة للتشفير وفك الشفرة عبر مراحل متعددة ولكل مرحلة مميزات تجعلها أكثر سرية وأمانا من المراحل التي تسبقها، فضلاً عن استخدام كلمة المرور كمفتاح والتي بدورها أيضا خضعت لعدد من مراحل الترميز. طبق هذا العمل باستخدام بيئة برمجية متكاملة وهي الـ MATHCAD.

الكلمات المفتاحية: الرموز, رمز مورس, الترميز الثنائي, المتمم, ترميز ثابت الطول, نظام التشفير

1.المقدمة

الرموز هي مجموعة من القوانين التحويلية التي تحدد العلاقة بين عناصر المعلومات الأصلية وعناصر المعلومات المرمزة أو العلاقة بين أبجديتين مختلفتين، وتكون العلاقة (واحد الى واحد), ويحدث هذا لتمثيل المعلومات بطريقة أخرى مع المحافظة على الترتيب الأصلي[10,9] وباستخدام برامج الحاسوب تصبح مهمة بناء أنظمة الترميز عملية سهلة.

أما بالنسبة إلى الشفرات فهي سلسلة من القوانين لتحويل المعلومات الواضحة إلى معلومات غير مفهومة (تبدو غير ذات معنى)، من الممكن القيام بعمليات التشفير وفك الشفرة يدوياً وبصورة سريعة بالنسبة إلى الرسائل القصيرة. وباستخدام الحاسب فلا يشكل طول النص الصريح أي إشكال. من الناحية المثالية, لايمكن للأشخاص غير المخولين اعتراض الرسائل المشفرة. في حالة اعتراض هذه الرسائل فمن الممكن لخبير محترف أن يكسر الشفرة [1].

هنالك اختلافات جوهرية بين لفظة رمز ولفظة شفرة، والتي يمكن إيجازها [10,9,7,4,2]:

1. الترميز يستبدل الأحرف أو الكلمات أو العبارة بمجموعة من الرموز أو الأرقام أو الأحرف، بينما التشفير يعيد ترتيب أو تعويض الأحرف بأخرى.

2. الترميز هو سلسلة عمليات دفعية مثل جهاز إرسال مورس(التلغراف)، بينما التشفير هو عملية خطية لكل حرف أو قد يكون لحرفين أو أكثر.

3. أنظمة الترميز في عملها لا تغير المعنى، بينما أنظمة التشفير في عملها تغير المعنى إذ تحول من كلمة (ATTACK) التي لها معنى واضح إلى كلمة مبهمة المعنى(FRGPL).
4. أنظمة التشفير أكثر ملاءمة من أنظمة الترميز، لعدم احتياجها إلى كتاب الرموز.
5. عملية تحويل النص المقروء إلى بيانات مرمزة لا تحتاج أن تكون سرية بالمقارنة مع البيانات المشفرة.

يعتبر رمز مورس من الرموز العالمية للإرسال وأكثرها فهماً وانتشاراً في العالم، اكتشفها في عام 1838م من قبل الأمريكي صاموئيل مورس (1791−1872)، الذي ابتكرها كطريقة جديدة لإرسال الرسائل بسرعة لمسافات طويلة ومازالت مستخدمة لحد الآن، ومما يجدر ذكره إن مصدر رمز مورس هي الأبجدية التي تتكون من 26 حرفاً من الأحرف الرومانية الكبيرة وتُرمْز هذه إلى وجه أخر الذي هو عبارة عن صيغة ثنائية تتكون من النقاط(dots) والخطوط القصيرة(dashes).

- النقطة تعني إشارة قصيرةً.
- الخط القصير [5].

ومن الجدير بالذكر إن رمز مورس لا يقتصر استخدامه على أحرف اللغة الإنكليزية فقط وإنما يتعداه إلى أكثر من لغة مثل اللغة الكورية واليابانية [5].

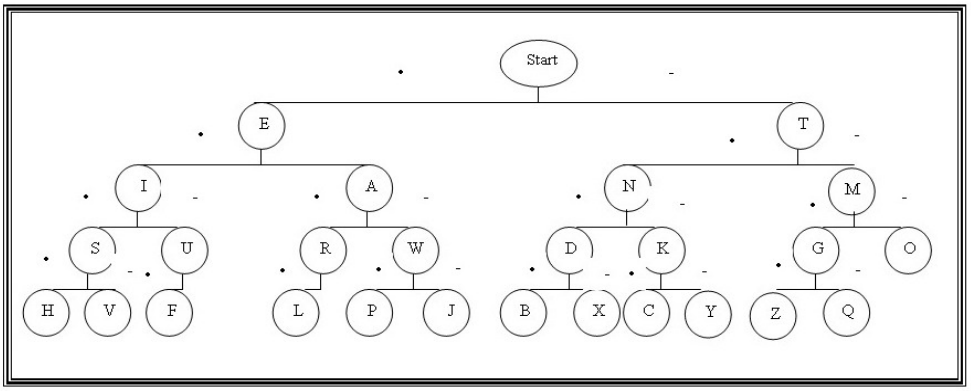
كما يعرف رمز مورس بالموجة المتواصلة وهو يستخدم نغمات طويلة وقصيرة لترميز الحرف.

- النغمة القصيرة تسمى (dot)
- النغمة الطويلة تسمى (dash).

فكرة اشتقاق رمز مورس على نفس مبدأ اشتقاق النظام الثنائي ولكن بالاعتماد على (. ، −) بدل (1،0) الخاصة بالنظام الثنائي، وتكون عملية الاشتقاق على شكل شجرة إلى أن نصل إلى النهاية [8,3].

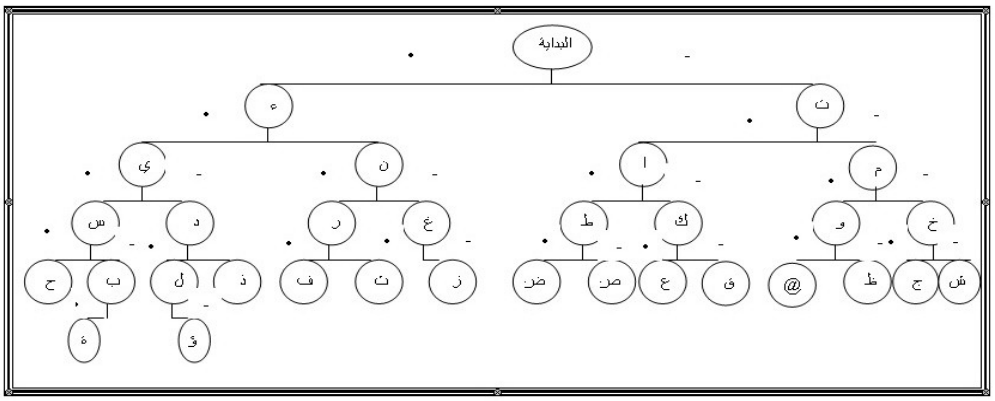
وطريقة اشتقاق رمز مورس للحروف الإنكليزية والعربية هو كالأتي:

الحروف الإنكليزية يمكن تمثيلها كتفرعات الشجرة تبدأ من الأعلى إلى الأسفل لعدد من المستويات ومن ملاحظة الشكل(1) نجد أن الحروف الأكثر تداولاً تكون في المستويات العليا ولهذا يكون رمزها قصيراً قياساً بالأحرف الأقل تداولاً التي تكون في المستويات السفلى من الشجرة.



شكل (1) شجرة رمز مورس للحروف الإنكليزية

وكذلك بالنسبة إلى الحروف العربية، كما في الشكل (2)



شكل (2) شجرة رمز مورس للحروف العربية

والجداول الآتية توضح رموز مورس العالمية الخاصة باللغة الإنكليزية والعربية انظر الجدولين (1)، (2) والتي تم استخدامها في مجال العمل.

A	.-	N	-.	0	-----
B	-…	O	---	1	.----
C	-.-.	P	.--.	2	..---
D	-..	Q	--.-	3	…--
E	.	R	.-.	4	….-
F	..-.	S	…	5	…..
G	--.	T	-	6	-….
H	….	U	..-	7	--…
I	..	V	…-	8	---..
J	.---	W	.--	9	----.
K	-.-	X	-..-		
L	.-..	Y	-.--		
M	--.	Z	--..		

الجدول (1) رمز مورس للحروف الإنكليزية

ء	.	ب	...-	0	-----	(	.-.--
ت	-	ل	..-.	1	----.	)	.--..
ا	-.	ذ	..--	2	---..	-	.--.-
ن	.-	ف	.-..	3	--...	+	.---.
ي	..	ث	.-.-	4	-....	=	-...-
م	--	ز	.---	5	.....	_	-..-.
س	...	ض	-...	6	....-	؟	-..--
د	..-	ص	-..-	7	...--	:	-.-..
ر	.-.	ع	-.-.	8	..---	"	-.-.-
غ	.--	ق	-.--	9	.----	،	-.--.
ط	-..	ظ	--.-	!	.--.	.	-.---
ك	-.-	ج	---.	@	--..	فراغ	--..-
و	--.	ش	----	%	..--.	÷	--.-.
خ	---	ه	..-..	^	.-...	.	--.--
ح	....	ة	...-.	&	.-..-		
ؤ	..-.-	ى	---.-	*	.-.-.		

الجدول (2) رمز مورس للحروف العربية

من أهم نقاط الضعف التي ممكن أن تسجل على أنظمة ترميز مورس:

1. استخدام النقاط والخطوط القصيرة فقط في الترميز، فأن تلك الرموز لا يفك ترميزها إلى جملة واحدة فقط وعلى سبيل المثال الجملة الآتية [...---...]

المفروض أن تعني هذه الجملة SOS ولكن قد تعني VMS أو EEETTTEEE أو عدداً من الأحرف الأخرى. كما انه قد تصل الكلمات المرمزة إلى الجهة المقابلة ناقصة أو محذوف منها بعض الأحرف يسبب ذلك ظهور كلمات تحمل معنى أخر أثناء فك الترميز، وعلى سبيل المثال SHEEPبدل SLEEP .فضلاً عن أن الرسائل القصيرة المرمزة برمز مورس ممكن أن تكشف بسهولة، وعلى سبيل المثال Attack at dawn والتي ترمز بالشكل الأتي:

[.- - - -. -.-. -.- .- - -.. .- .-- -.]

2. ترميز الحروف برمز مورس بدون فاصل مع ذكر أطوال الرموز في نهاية السطر، مثلاً لترميز كلمة ALI يكون بالشكل الأتي:

.- .-.. .. 242

إذ إن العدد 2 يمثل عدد عناصر رمز أول حرف والعدد 4 يمثل عدد عناصر رمز ثاني حرف وهكذا. أو قد تكون هذه الأرقام التي تمثل عدد العناصر في كل رمز والتي ترتب قي داخل مجاميع n بترتيب معكوس وقد استخدم هذا التطبيق بترميز الحروف اليابانية برمز مورس التابعة لها.

2_ميزات رمز مورس:

من خلال الإطلاع على الرموز وأنواعها وطرائق إرسالها فقد تمت ملاحظة إن الأنظمة التي تستخدم رمز مورس هي من أقدم أنظمة الإرسال في العالم وأكفأها والتي بقي استخدامها إلى حد ألان للأسباب الآتية [6]:

1. تعد أنظمة الترميز التي تستخدم رمز مورس أحد أساليب الكبس إذ أن الحرف E أكثر الأحرف استخداماً يُرمز بأقل عدد من الرموز(.)، أما الحرف Q الذي يعتبر اقل استخداماً يُرمز له (...)، وهذا يقلل من مساحة الخزن.

2.اختزال زمن الإرسال، إذ أن الحرف E الأكثر استخداماً يُرسل بوقت يقدر بجزء من ثلاثة عشر جزءاً من الوقت اللازم لإرسال الحرف Q الأقل استخداماً.

3. الترميز باستخدام رمز مورس تتطلب مكونات مادية اقل للإرسال والاستقبال مقارنةً مع الاتصالات الأخرى.

4. في حالة تدهور الأوضاع الجوية المحيطة بجو الكرة الأرضية فان رمز مورس يبقى فعالاً عن طريق تغير المفتاح ON/OFF وبالعكس.

5. إن أنظمة الترميز التي تستخدم رمز مورس تعتبر من الأنظمة الترميز ذات الأطوال غير الثابتة وهذا يساعد على زيادة السرية.

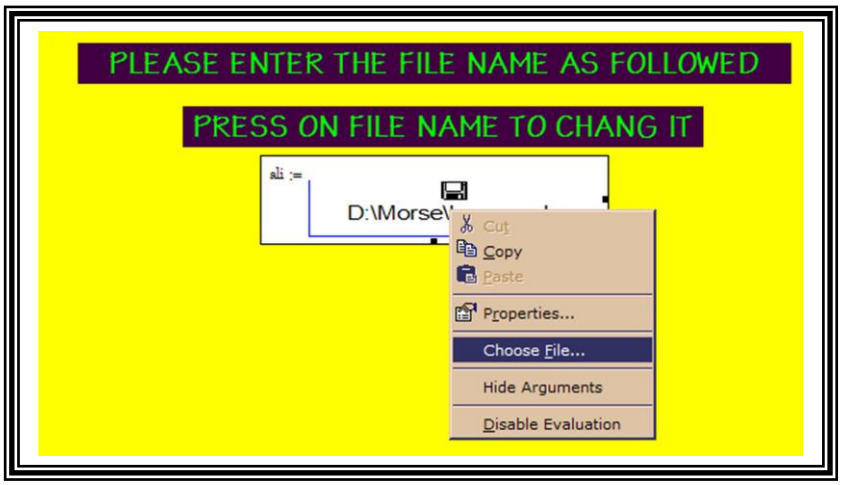
3_الخوارزمية المقترحة:

لقد تم الاعتماد في هذا البحث على رمز مورس الخاص باللغة العربية واللغة الإنكليزية لان النص العربي المشفر يرسل كنص مرمز برموز مورس الخاص باللغة الإنكليزية لزيادة سرية الملف. من الضروري كخطوة أولى أن يتم إدخال هذه الرموز كجدول ثابت في بداية النظام لكي تستخدم فيما بعد. ويمثل الشكل (3) جزءاً من هذا الجدول.

13	"ك"	"_._"	"C"	"_._._"
14	"ل"	"._.."	"D"	"_.."
15	"م"	"__"	"E"	"."
16	"ن"	"_."	"F"	".._."
17	"س"	"..."	"G"	"__."
18	"ع"	".._."	"H"	"...."
19	"ف"	"._._"	"I"	".."
20	"ص"	"._.."	"J"	".___"
21	"ق"	"__._"	"K"	"_._"
22	"ر"	"._."	"L"	"._.."

الشكل(3)جدول الحروف والرموز

ثم يتم اختيار الملف المراد تشفيره كما موضح بالشكل(4)

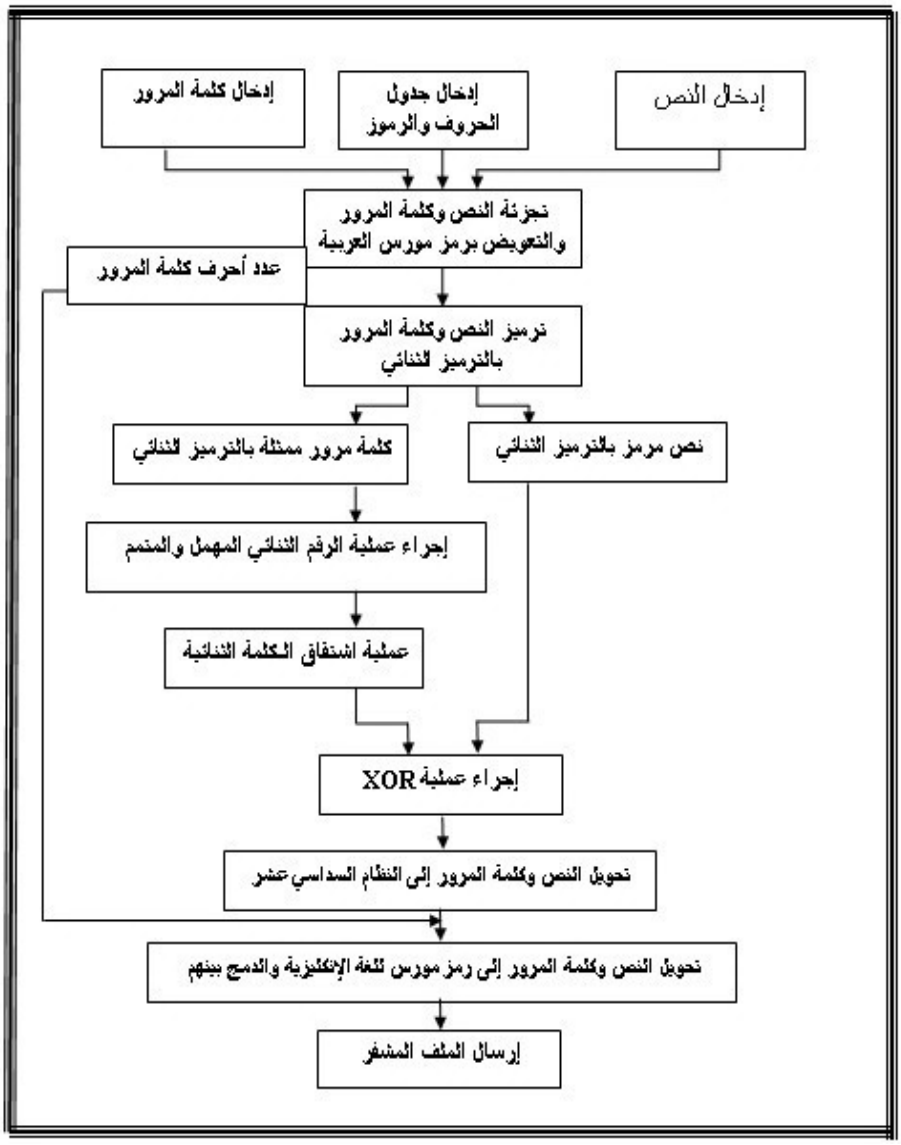


الشكل (4)عملية اختيار ملف

وقد تمت إضافة كلمة المرور ضمن عمليات المعالجة لتحقيق السرية إذ تم استخدام كلمة مرور متغيرة الطول والتي يتراوح طولها من(6–9) أحرف تُدخل من قبل الشخص الذي يشفر النص، والتي تمر أيضا بعدد من مراحل التشفير والترميز الموضحة في الخوارزمية وتدمج مع النص المرسل إلى الجهة الأخرى لكي تستخدم في عملية فك الشفرة.

اولاً: خوارزمية التشفير:-

لمعالجة نقاط ضعف ترميز مورس، فقد تم استخدام رمز مورس في هذا التطبيق بعد سلسلة من المعالجات وعمليات التشفير المتتابعة التي تجري على النص العربي المدخل ومن ثم يرمز برمز مورس، وقد تم استخدام الخوارزمية الممثلة بالشكل (5) في التطبيق.

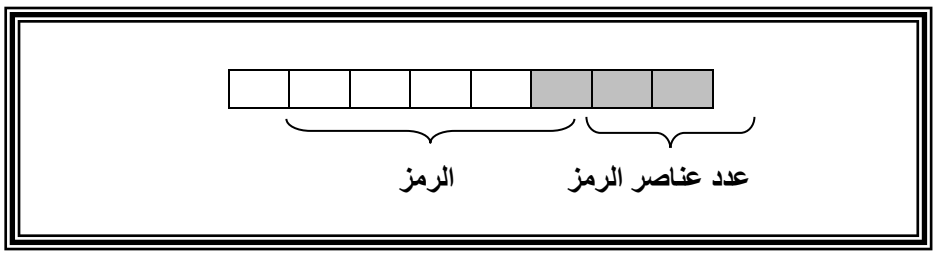


الشكل (5)خوارزمية التشفير

وفيما يأتي شرح للخطوات المبينة في الخوارزمية:

1. التجزئة ورمز مورس للغة العربية:يتم قراءة النص المدخل المكتوب باللغة العربية والذي يحوي (حروفاً، أرقاماً، رموزاً) ومن ثم تتم تجزئتة إلى وحدات منفصلة كل وحدة تمثل حرفاً واحداً فقط. ثم يتم تعويض كل حرف برمز مورس للغة العربية المكافئ له ودمج الناتج لجميع الأحرف مع الفصل بين رمز وأخر بفراغ.

2.الترميز الثنائي:تم الدمج بين طرائق الترميز غير ثابتة الأطول (رمز مورس) وطرائق الترميز الثابتة الطول (الترميز الثنائي). حيث يؤخذ النص الناتج من المرحلة السابقة ويرمز بالترميز الثنائي الذي يعتمد (1,0) على أساس انه كل رمز يتكون من ثمانية أرقام ثنائية وكما موضح بالشكل (6) يقسم إلى قسمين:

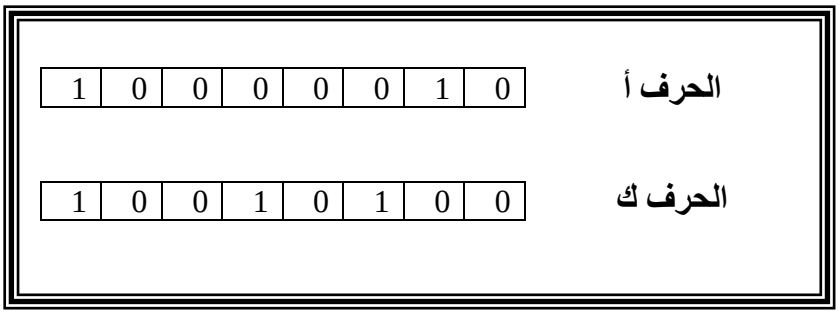


الشكل (6) تمثيل الكلمة الثنائية

القسم الأول: يتكون من ثلاثة أرقام ثنائية (المراتب الثلاثة الأولى) لتحديد عدد العناصر في رمز مورس للحرف الواحد ممثلة بالنظام الثنائي.

القسم الثاني: يتكون من خمسة أرقام ثنائية (المراتب الخمسة الأخيرة) لتمثيل رمز مورس نفسه بالترميز الثنائي، إذ أن النقطة تستبدل بـ (0) وكذلك الخط القصير يستبدل بـ (1)، وفي حالة كون عدد عناصر الرمز اقل من خمسة يستكمل بالا صفار.

بعد الانتهاء من عمل القسمين يتم دمج نتائجهما بدون فاصل أي يصبح طول كل رمز هو ثمانية أرقام ثنائية أي ما يعادل الـ 1.Byte لشكل (7) يوضح نتائج عملية تحويل الحرفين (أ، ك) إلى الترميز الثنائي.



شكل (7)تمثيل الحرفين (أ، ك) بالترميز الثنائي

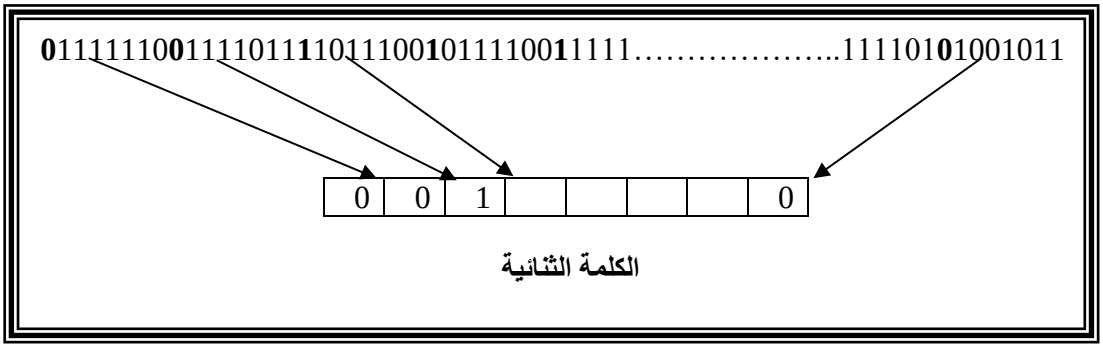
العملية التي ذكرت أخيرا تمر أيضا على كلمة المرور المدخلة مسبقا فضلاً عن النص.

3. عمليتا (الرقم الثنائي المهمل و المتمم):إن إحدى الإمكانيات المجهزة بها لغة التطبيق (MathCAD) هي عملية الرقم الثنائي المهمل إذ يمكن التعامل بصورة منفصلة مع الرقم الثنائي الواحد وإجراء العمليات المنطقية المختلفة عليه.فقد تمت الاستفادة من هذه العملية لتغير الهيئة الناتجة لكلمة المرور في المرحلة السابقة ومن ثم إجراء عملية المتمم لكل السلسلة الثنائية وبهذا فان كل (1) يصبح (0) وبالعكس.

4. عملية اشتقاق (الكلمة الثنائية):إن كلمة المرور الناتجة من عمليتي (الرقم الثنائي المهمل و المتمم) والتي تكون مرمزة بالترميز الثنائي وبدون فاصل، تقسم إلى أقسام كل قسم يكون بطول ثمانية أرقام ثنائية ثم يؤخذ أول رقم ثنائي من القسم الأول ويدمج مع أول رقم ثنائي للقسم الثاني وهكذا إلى نهاية الأقسام، وفي هذه الحالة سوف تتكون لدينا سلسلة من الأرقام الثنائية يتراوح طولها من (6 –9) أرقام ثنائية .

فإذا كان طول السلسلة الناتجة هو ستة أو سبعة أرقام ثنائية فسوف يستكمل بالأصفار إلى إن يصبح طول السلسلة ثمانية أرقام ثنائية، أما إذا كان طول السلسلة هو تسعة أرقام ثنائية فسوف يقطع منها أول ثمانية فقط.

السلسلة الناتجة هي الكلمة الثنائية، والتي سوف تستخدم في بعض المراحل القادمة، الشكل (8) يوضح عملية الاشتقاق.



الشكل (8)عملية اشتقاق الكلمة الثنائية

5. العملية المنطقية (XOR):في بداية العملية يتم تقسيم النص إلى أقسام يكون طول كل قسم ثمانية أرقام ثنائية ثم يتم أجراء العملية المنطقية بين الكلمة الثنائية وكل قسم من الأقسام المتكونة في هذه المرحلة ويدمج بين النواتج الأخيرة بحيث تتمثل سلسلة من الأرقام الثنائية وبدون فاصل.

6.النظام السداسي عشر: يتم في هذه المرحلة تقطيع النص إلى أجزاء رباعية ومن ثم يتم تحويل كل جزء إلى النظام السداسي عشر وتدمج النواتج كسلسلة من الحروف(A-Z) والأرقام (0-9) بدون فاصل بينها أيضا. إن كلمة المرور أيضا تمر بهذه المرحلة أي تتحول من النظام الثنائي إلى النظام السداسي عشر.

7. رمز مورس للغة الإنكليزية : فيها يتم تحويل النص الناتج إلى نص مرمز برمز مورس باستخدام الحقل الذي يحوي رمز مورس للغة الإنكليزية في الجدول.

حيث يتم البحث عن الحرف الواحد ضمن الجدول وفي حالة العثور عليه سوف لا يؤخذ مباشرة ولكن يؤخذ تسلسل الحرف وتضاف إليه إزاحة تعادل عدد حروف كلمة المرور المدخلة في البداية وبعدها يؤخذ الرمز المقابل لذلك التسلسل.إن كلمة المرور تعامل معاملة النص في هذه المرحلة، أي انه سوف ترمز ايضاً برمز مورس للغة الإنكليزية.

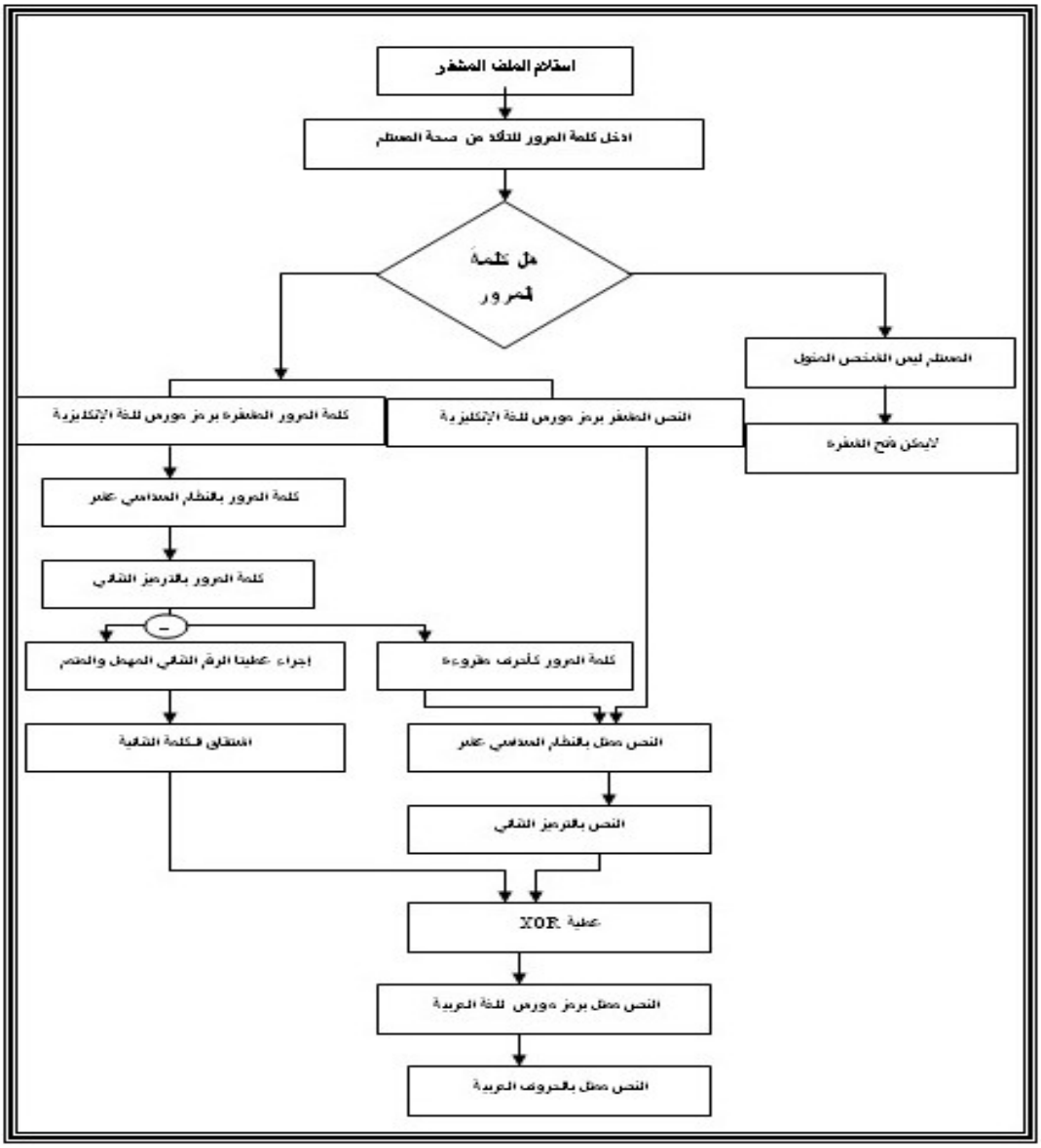
8. وفي هذه المرحلة يتم دمج رموز كلمة المرور مع رموز النص الأخير في ملف واحد وتوضع رموز كلمة المرور في مواقع يتفق عليها كل من المرسل والمستلم لكي يستطيع المستلم فيما بعد أن يفك شفرة النص وقراءة المعلومات الأصلية.
9. إرسال الملف المشفر.

. خوارزمية فك الشفرة:

تم في هذه المرحلة فك شفرة الملف المستلم باستخدام خوارزمية فك الشفرة والموضحة بالشكل (9) ليتسنى لمستلمها قراءة المعلومات الأصلية التي بداخلها.

ولفك تشفير أي ملف بصورة صحيحة نحتاج إلى ما يأتي:

1. الملف المشفر بدون أي تغير أو نقص بالمعلومات.
2. برنامج فك الشفرة والمعد على نفس أسس بناء برنامج التشفير.
3. معرفة موقع كلمة المرور المستخدمة ضمن الملف المشفر.



الشكل (9)خوارزمية فك الشفرة

4. الاستنتاجات:

إن النظام المقترح لتشفير النصوص العربية ممكن أن يستخدم لأي نص مكتوب بأية لغة مع تغير الرموز فقط في جدول المدخلات بما يناسب اللغة.وقد تم الدمج بين التشفير والترميز للاستفادة من خصائص كل منهما لزيادة السرية.إذ تم تحقيق مستوى عالٍ من السرية وبسرعة عالية حيث لم يكن هناك تأثير لعامل الزمن في عامل السرية. كما أن الاستخدام المتداخل لطرائق التشفير والترميز يجعل عملية كسر الشفرة معقدة حتى وان تم في بعض المراحل فأنه من الصعب الاستمرار في العملية مالم يعرف معلومات عديدة عن هذه الطرائق وكلمة المرور. كما أن الاستخدام المزدوج لرمز مورس للغتين العربية والإنكليزية يؤدي إلى إرباك الدخيل على الملف المرسل في كون اصل النص عربياً أم إنكليزياً.كما وفر البرنامج الذي تم بناؤه واجهة مرئية سهلة الاستخدام وواضحة للمستخدم.

5.التوصيات:

1. تم استخدام التشفير والترميز في تطبيق النظام الناتج لهذا نوصى باستعماله مع تقنيات الإخفاء للاستفادة من ميزة وهي عدم معرفة ان أخر ترميز تم استخدامه كان هو رمز مورس.

2.تحوير الخوارزمية من النوع المتماثل الى النوع غير المتماثل للتخلص من مشكلة إدارة وتوزيع المفتاح، أو المزج بين الأسلوبين.

3.استخدام تقنيات تشفير وترميز أخرى متداخلة في النص الواحد لزيادة تعقيد كسر الشفرة.

المصادر

(1) بد رخان، ستار (1989) ، "الرموز والشفرات_ مدخل إلى امن المعلومات".

[2] Chesson, F.w. (2000) “Secret Wires, Civil War Cryptology Origins of secret Messages on open Wires”. **http://pages.cthome.net/Fwc/ code .html.**

[3] Hitz, M. (2002) “Codierung”. **http://www.tm.informatik.unifrank rutde/pluf2/folien/comp6.pdf.**

[4] Lamb, A. and L. Johnson (1999) “The Topic: Codes, Ciphers & Secret Messages".**http://www.42explore.com/codes.html.**

[5] Mark L. (2004) “Security Inisde Out”, **The System Consulting, Inc.**, Research Report.

[6] Salomon, J.E. (2005) **Data Compression** , Springer-Verlag New York, Inc, united states of America.

[7] Shipley G. (2001) **Maximum Security**, Third Edition, Sams Publishing Company.

[8] Webster, C. (2002) “Communication, Codes and Cyphers”, Las Vegas, **UNLV_ university of Nevada** ,http://www.nevada.edu/~ Cwebster /teaching/notes/codes/introduction/examples.html.

[9] “Code” (2002) Principia Cybern Etic web. http://www.pespmc1.vub. ac.be/Asc/code.html.

[10] “Codes Versus Ciphers”. **http://www.albany.net/~cybernet/Codes. html.**