اعتماد التغيرات الحرفية والثنائية لتشفير المعلومات

ساهرة عبيد سعد

جامعة البصرة/كلية العلوم/قسم الحاسبات

المستخلص

يقدم البحث الحالي خوارزمية لتشفير النص الصريح حيث شملت الخوارزمية على مرحلتين رئيسيتين هما مرحلة التشفير ومرحلة فك التشفير تضمنت مرحلة التشفير على مجموعة من العمليات وهي عملية تبادل مواقع حروف النص الى مواقع أخرى وباستخدام مفتاح مزج محدد عشوائيا ،بالإضافة الى مجموعة من عملبات التحويلات على الحروف ، وعمليات على الثنائيات التي تتكون منها الرموز المدخلة ،أي ادخال الثنائيات الناتجة الى عدة عمليات منها عملية التعويض وعملية العكس،وعملية التحويل اعتمادا من جدول الرموزAscii،وبتطبيق العامل XOR على قيم Ascii ومع مفتاح تشفير محدد ، وبتوليد الرموز المقابلة للشفرات الناتجة من العمليات السابقة مكون ملف مرمز يحتوي على مجموعة من الرموز وهو ملف التشفير الناتج ، اما المرحلة الرئيسية الثانية في الخوارزمية هي مرحلة فك التشفير والتي تضمنت على مجموعة من العمليات تسير بالاتجاه المعاكس للعمليات السابقة لغرض الحصول على النص المدخل ،وكذلك لتأكد من صحة العمليات السابقة والتي أدت في النهاية بالحصول على النص الصريح المدخل.

المقدمة Introduction

بعد ظهور الحاسبات برزت الحاجة الى تبادل المعلومات في مراكز الحاسبات عن طريق وسائل الاتصال المعروفة [1] ،حيث تزايدت الاهتمام بالمعلومات في الأعوام الأخيرة بشكل ملفت للنظر واصبح حماية المعلومات من الأشخاص غير المخولين أمرا لابد منه وان إحدى الطرق المستخدمة لحماية المعلومات هي استخدام أنظمة التشفير وان أنظمة التشفير تستخدم في أنظمة الاتصالات والخزن كوسيلة أمنه للحفاظ على المعلومات وتزداد أهمية هذا الجانب عندما تكون هناك شبكة محلية او شبكة عالمية [2] .

كما ان المخاوف الأخيرة من جرائم الحاسبات والحاجة الى خصوصية المعلومات أدت أيضا الى زيادة الاهتمام في التشفير ليكون وسيلة لاخفاء وحماية البيانات السرية ويمكن للتشفير ان يعطي درجة عالية من الآمن بأقل كلفة وبما ان طرق التشفير التقليدية قد لاتعطينا الدرجة المطلوبة من الأمن،لذا فقد تم تطوير تقنيات جديدة بحيث تعطي مستويات عالية من الأمن عند تطبيقها على نظام الحاسبات هذه التقنيات الجديدة تستخدم مبادى طرق التشفير التقليدية ومبادى رياضية تطبق على الحاسبات [3]

ان الاحتياج لتحسين آمن البيانات والمعلومات في أنظمة الحاسبات هو نتيجة مباشرة للاستخدام المتزايد للحاسبات من قبل المصانع الحكومية والخاصة في معالجة وخزن وإيصال البيانات القيمة والحساسة وإضافة الى ذلك فأننا نرى اهتماما حكوميا وعاما في مجال آمن البيانات والمعلومات [5] ان البيانات يمكن ان تتكون من مجموعة أو تجمع من الحقائق والإحصائيات التي تكون تسجيلا لمشاهدة حدث ما ،ويمكن النظر للمعلومات بصفتها بيانات تمت معالجتها لجعلها مقيدة وان المصطلحين "بيانات ومعلومات " غالبا ما تكون متطابقا فالأمن هو حماية البيانات والمعلومات بحيث تكون :-

١- غير قابلة للتحوير

٢- غير قابلة للتحطيم

٣- غير قابلة للإفشاء او التسوية اما بصورة متعمدة او غير متعمدة .

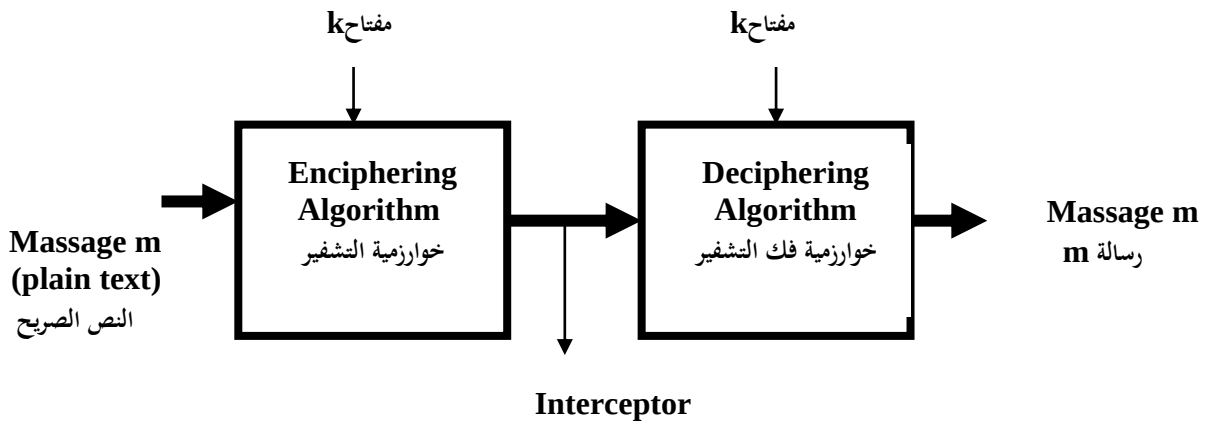
ان تهديدات آمن البيانات تكون في مجالين الأول يجب ان نأخذ بالاعتبار حقيقة ان بيانات كثيرة تعالج بالحاسبات وترسل بأجهزة الإرسال الإلكتروني وبذلك ففي أنظمة اتصالات البيانات نكون مهددين بالاستراق والذي يغطي مدى واسعا من الفعاليات غير الشرعية ، ولمواجهة التهديدات المؤشرة هنا ،أي لحماية البيانات العابرة خلال خطوط الاتصال او الأوساط الخزنية فان البيانات والمعلومات يمكن ان تخفى او ترمز وإذا كان نظام الاتصال او نظام الحاسب مبنيا بصورة مثلى ،وجدت دخول غير شرعي فلذلك سيكون استخلاص المعلومات المفيدة من قبل الفرد أمرا صعبا ويستغرق زمنا طويلا ،وان إخفاء المعلومات المفيدة في صورة غير مفهومة هو الحلم الذي حققه التشفير[1].

مفاهيم التشفير

التشفير هو مجموعة التحويلات التي تجرى على النص الصريح للحصول على النص المشفر ،هذه التحويلات تشمل خوارزمية التشفير بالإضافة الى المفتاح ،ويعتبر التشفير طريقة لحماية المعلومات من الوصول غير الشرعي وتطبق لحماية قنوات الاتصال وقواعد البيانات ،أي وسيلة تطبيقية لحماية المعلومات المرسلة خلال قنوات الاتصال المعلنة ،والتشفير يمكن ان يكون على شكل مجموعة من الايعازات أو جزء من الجهاز **hardware** او برنامج **software** [2] ، حيث ان التشفير يمكن اعتباره عملية معالجة الرسالة (النص) المشفرة بحيث يكون معنى الرسالة غير واضحة ، عملية تحويل الرسالة الواضحة إلى رسالة مشفرة تسمى **cryptogram** [4].

أنظمة التشفير

الشكل(١)يبين نظام التشفير[5]



الشكل(١) المخطط الكتلي للنظام التشفير

حيث ينقسم

١-خوارزمية التشفير **Encryption Algorithm**

٢-خوارزمية فك التشفير **Decryption Algorithm**

خوارزمية التشفير

هي مجموعة من العمليات التي تهدف الى تحويل النص الصريح الى نص مشفر .

مفتاح التشفير

أمنية أنظمة التشفير الحديثة تعتمد على مفتاح التشفير cryptographic key(k) ،مجال القيم التي يمكن ان يأخذها مفتاح التشفير تسمى فضاء المفتاح key space .

خوارزمية فك التشفير

هي العملية المعكوسة أي تحويل الرسالة المشفرة الى شكلها الأصلي .

فإذا كانت M هي فضاء الرسالة و C هي فضاء الرسالة المشفرة وK هي فضاء مفتاح التشفير فأن خوارزمية التشفير Enciphering Algorithm (E)

$$E_k : M \longrightarrow C \quad or \quad E_k(m) = c$$

$$k \epsilon K \ , \ m \epsilon M \ , \ c \epsilon C$$

اما خوارزمية فك التشفبر فتكون كما يلي:-

$$E_k^{-1} = D_k$$

$$D_k(c) = D_k[E_k(m)] = m$$

المعترض او الخصم Interceptor (opponent)

هو الشخص الذي يعترض الرسالة المشفرة بين المرسل والمستلم بشكل غير شرعي حيث انه لا يعرف المفتاح المستخدم في عملية التشفير فيقوم بقطع الاتصال او التنصت او تغير محتوى الرسالة [7]

ملفات النصوص

يتكون الملف النصي من سطر واحد او اكثر من الأرقام او الكلمات او الأحرف وتختلف الملفات النصية عن ملفات المستندات التي تحتوي على شفرات تنسيق وعن الملفات التنفيذية التي تحتوي على تعليمات لنظام التشغيل ، ان الملفات النصية يتعرف عليها مستكشف ويندوز على أنها Text Document او التي تحمل الملف txt او ini او log او inf او dat او bat ،البحث الحالي يبين كيفية تشفير السلاسل النصية وفك تشفيرها بشكل آمن.

دراسة في بعض طرق التشفير

فيما يلي عرض موجز لبعض طرق التشفير:-

١-الإبدال الهجائي الأحادي Monoalphabetic Transposition Ciphers

في هذا النوع من التشفير يأخذ كل اربعة حروف متتالية ويتم تبديلها بالمواقع المحددة حسب الدالة f حيث ان f=(2,3,4,1) ولتوضيح هذه الطريقة نأخذ النص الصريح الأتي:-computer science

(الدالة)	2	3	4	1
c	o	m	p	
p	c	o	m	

4 3 2 1 (التسلسل) وبتالي يكون النص المشفر :- pcomrteu escince

٢- نظـام الكلمــة المفتاحيــة المبــدل Transposed Keyword Mixed General Monolaphabetic Ciphers

في هذا النوع من التشفير يتم استخدام كلمة السر ،حيث يتم تكوين مصفوفة يكون السطر الاول من المصفوفة يمثل حروف كلمة السر وتترك الحروف المتكررة ويتم تكملة حروف المصفوفة من الحروف الأبجدية الإنكليزية وبصورة متتالية وفقط الحروف الغير موجودة في كلمة السر ،فمثلا اذا كانت كلمة السر المستخدمة STAR WARS فتكون المصفوفة كمايلي :-

S B C D E
F T G H I
J K A L M
N O P R Q
U V X Y W
Z

بعدها تقرأ المصفوفة (عمود_عمود) وتكتب الاعمدة المقروءة بشكل سطر تحت الحروف الانكليزية(يجب ان يكون عناصر المصفوفة ٢٦ حرف) وكما يلي:-

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z (الابجدية الانكليزية)

S B G L Q Z T C H M U A D I N V R E J O X W F K P Y (حروف المصفوفة)

فمثلا اذا كان النص الصريح IKNOW ONLY THAT IKNOW NOTHING

ويكون النص المشفر H UINF NIAP OCSO H UINF INOCHIF

٤- نظام فيجينير Vigenere Cipher

في هذا النوع من التشفير يعطى كلمة السر (الكلمة المفتاحية) إضافة الى النص الصريح المراد تشفيرة ، في البداية يكتب الجدول التالي(الذي يتكون من الحروف الأبجدية الانكليزية مع الترقيم):-

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z ثم

يتم تقسيم النص الصريح الى مجاميع وبطول كلمة السر ونضع اسفل كل مقطع كلمة السر ومن ثم تطبق العلاقة الاتية:-

$$F(a) = (a + k) \bmod 25 \quad \ldots\ldots\ldots\ldots(1)$$

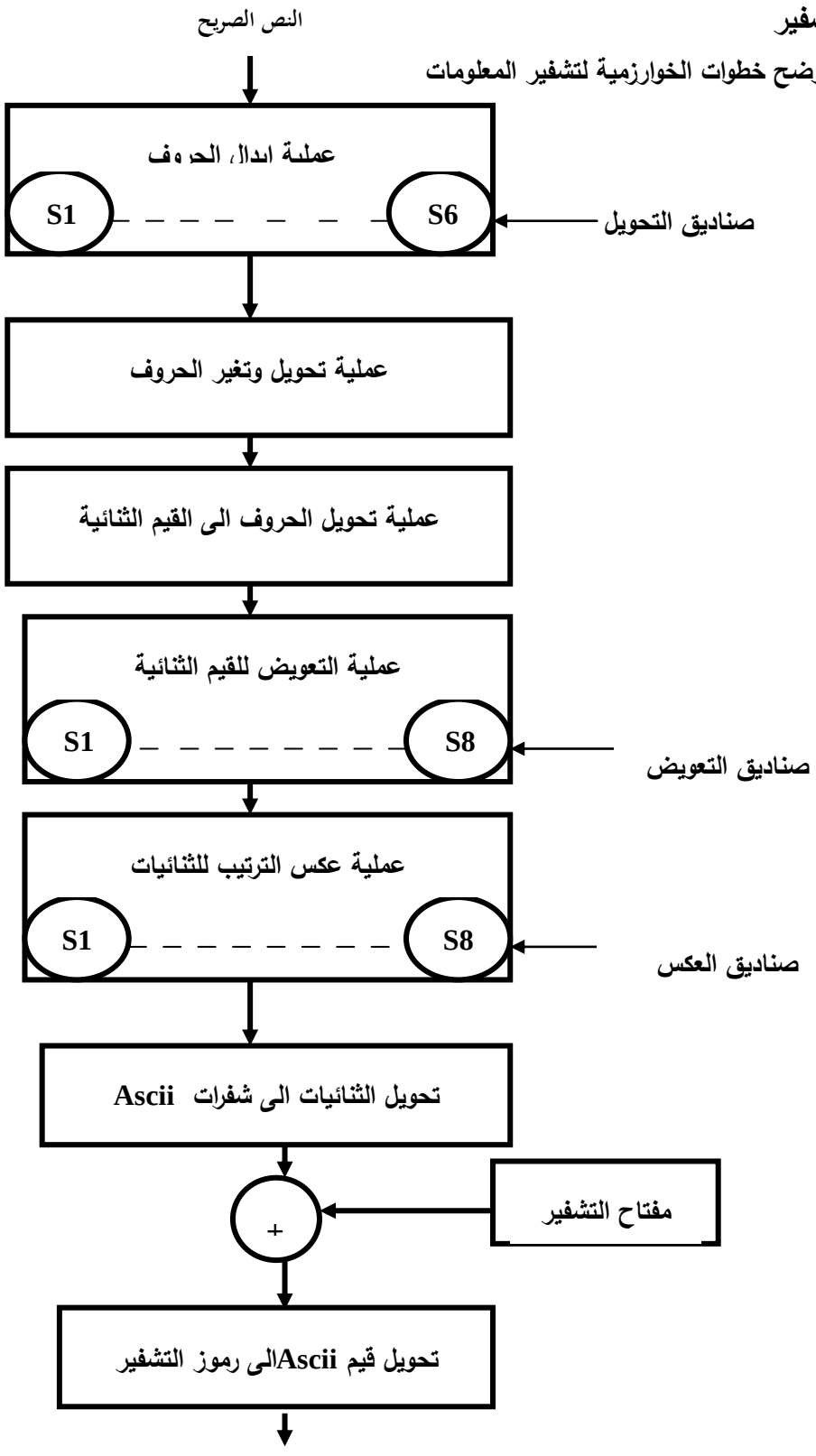
حيث ان a تمثل الموقع القديم للحرف وان k تمثل موقع المفتاح ، فأن الناتج من العلاقة (١) يمثل موقع الحرف المشفر ومع مراعاة الـ mode في حالة تجاوز الجمع الرقم ٢٥، فكان النص المشفر :-

PBVBCWVNHZUAHFSVASJ

نلاحظ ان في طرق التشفير السابقة تم اعتماد في تشفيرها على عملية تحويل واحد على الأكثر حيث يتم إجراءها على النص الصريح، اما في طريقة التشفير المعتمدة في خوارزمية التشفير المقترحة في البحث الحالي فقد تضمنت على مجموعة من التحويلات المتتالية على حروف النص الصريح ،ومن ثم مجموعة من التحويلات المتتالية على الثنائيات المكونة لرموز النص وهذا ما سيتم توضيحه في الفقرات آلاتية.

خوارزمية التشفير

الشكل (٢) يوضح خطوات الخوارزمية لتشفير المعلومات

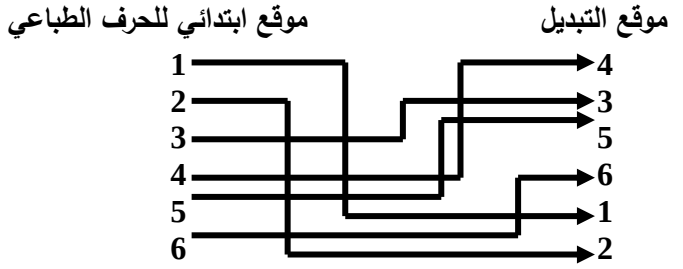


الشكل(٢) عمليات تشفير النص المدخل

وفيما يلي شرح مفصل للخطوات التشفير :-

١-عملية ابدال الحروف

وهي نوع من المبادلة وان العدد او الحرف او الرمز الطباعي في موقع ابتدائي يحول او ينقل الى موقع آخر وباستخدام مفتاح مزج محدد واحد، حيث تم توليد مفاتيح عددية عشوائية وبطول محدد ايضا ، وان احدى الأساليب لتوفير طريقة موضوعية لاختيار المفاتيح نستخدم الطريقة العشوائية وبأستخدام برامج الحاسب حيث يقوم البرنامج بتوفير المفاتيح بأطوال اثنين الى عشرة حروف مشتقة من الارقام(0,1,….,9)،فمثلا تم اختيار احد هذه المفاتيح المتولدة عشوائيا فكان المفتاح المختار بطول ستة احرف وهو (435612) وكما يوضح المثال آلاتي :-



ان عملية التبديل تكون بأخذ كل ستة حروف متتالية من النص أي وضعها في صناديق التحويل (s1….s6) وأجراء عليها عملية التبديل وذلك بوضع الحرف الرابع بالموقع الاول والحرف الثالث بالموقع الثاني وهكذا مع الحرف الثاني في الموقع السادس اوالاخير وباستخدام كلمة SYSTEM يمكننا القول بأن عمل التحويل والمبادلة تكون كالاتي :-

الناتج	الكلمة	موقع التبديل	الموقع الابتدائي
T	S	4	1
S	Y	3	2
E	S	5	3
M	T	6	4
S	E	1	5
Y	M	2	6

ان الغرض من التبادل هو مزج الحروف بحيث لايمكن كسرها بسهولة،وان هذه التقنية تقوي الخوارزمية وتجعلها مقاومة لهجوم محلل الشفرة ،حيث يتم تغير النص الصريح بطريقة معقدة.

٢-عملية تحويل وتغير الحروف

في هذه العملية يتم اختيار كلمة السر(أي الكلمة المفتاحية)،فمثلا تم ادخال كلمة السر STAR WARS ،وتكتب بحروف متصلة لا توجد بينها فراغات وتهمل الحروف المتكررة فيها ويتم توزيع حروف الكلمة على القطر الرئيسي للمصفوفة(ويستخدم القطر الثانوي في حالة الحاجة لتكملة حروف كلمة السر)، ومن ثم تكتب حروف الابجدية الانكليزية (26) حرف غير الموجودة في كلمة السرلتكملة المصفوفة سطر_سطر ،وكما موضح:-

S B C D E
F T G H I
J K A L M
N O P R Q
U V X Y W
Z

ثم تقرا المصفوفة بصورة متدرجة من اليسار الى اليمين،وتكتب الحروف المقروءة بشكل سطر تحت الحروف الانكليزية ،حيث تقرا الحروف في الخط المائل من الاعلى الى الاسفل (يجب ان تكون عناصر المصفوفة ٢٦ حرفا) وكما يلي:-

ABCDEFGHIJKLMNOPQRSTUVWXYZ
EDICHMBGLQSTARWFKPYJOXNVUZ

ولعمل التشفير تقرا الحروف من الاعلى الى الاسفل (أي تقرا الحروف في تسلسل الابجدية الانكليزية) وما يناظره اسفله يكون هو الحرف المطلوب والذي نكتبه ،فمثلا اذا كان النص الصريح

I HAVE TWO BOOKS
L GEXH JNW DWWSY

ومن ثم يتم تقسيم الحروف الناتجة الى مجاميع وبطول كلمة السر المدخلة وكما يلي:-

L	**G**	**E**	**X**	**H**	**J**	**N**	**W**
S	**T**	**A**	**R**	**W**	**A**	**R**	**S**
O	**Z**	**E**	**O**	**D**	**J**	**E**	**O**

D	**W**	**W**	**S**	**Y**			
S	**T**	**A**	**R**	**W**	**A**	**R**	**S**
V	**P**	**W**	**J**	**U**			

وبأخذ الابجدية وترقيمها وكما يلي:-

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

ومن ثم تطبق العلاقة (1)السابقة.

ناتج التشفير :-

OZEODJEOVPWJU

٣-عملية تحويل الحروف الى الثنائيات المقابلة

يتم في هذه العملية اولا تحويل كل حرف الى قيم Ascii المناظرة له ،فمثلا

T S E M S Y

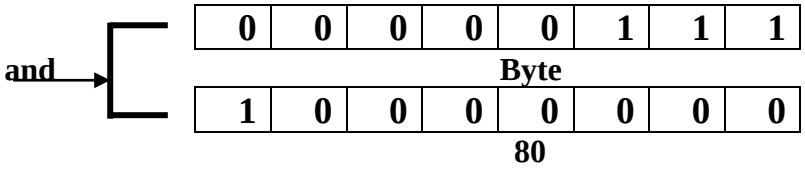
تحول الى قيم اسكي

64 65 66 67 68 69

ومن ثم يتم اخذ كل بايت يحوي على قيمة اسكي وتفكيك الى الثنائيات المكونة لها ،حيث يتم ذلك من خلال تطبيق العامل and على كل بايت ومع المعيار 80$أي ان

byte and $80

وملاحظة النتيجة اما صفر او واحد ،بعد ذلك تزحف البايت الى اليسار بمقدار واحد (1 shl) واعادة تطبيق بنفس العامل والقيمة (80 $) على البايت المزحف وهكذا الى ان تنتهي بتوليد كل الثنائيات الخاصة بهذا البايت ،فمثلا اذا كان البايت يحوي على الرقم 7 أي ان (byte= 7)



وبتطبيق and نحصل علىالقيمة (0) وبعد هذا نعمل على تزحيف البايت الى اليسار وتستمر هذه العملية الى ان نحصل على الشفرة الكاملة للبايت الحالي وهي (00000111) أي ان عدد مرات التزحيف الى اليسار بعدد ثنائيات البايت (أي ثمانية مرات)، من خلال هذه المرحلة تم تحويل قيم اسكي المخزونة في البايتات الىالثنائيات المقابلة لها.

٣-عمليات علىالقيم الثنائيات

يتم في هذه العملية اولا اخذ كل ثمانية ثنائيات متتالية أي في صناديق التعويض S1,……..S8,(من اليسار الى اليمين) واجراء عليها عملية تعويض للقيم حيث يتم عكس للقيم هذه الثنائيات(أي 0 الى 1 و 1 الى 0)، فمثلا سلسلة الثنائيات الاتية (01111010) يتم تحويلها(10000101).

ومن ثم العمل على عكس ترتيب الثنائيات وذلك بأخذ كل ثماني ثنائيات متتالية ومن اليسار الى اليمين وداخل الصناديق العكس S1,……..,S8 ويجرى عليها عكس لترتيبها فمثلا الثنائيات الناتجة من العملية السابقة(10000101) تحول الى (10100001) .

ومن بعد ذلك تحول الثنائيات الناتجة من العمليات السابقة الى قيم Ascii ،حيث يتم في هذه العملية اخذ كل ثمانية ثنائيات متتالية ومن اليسار الى اليمين وتطبيق عليها عملية التحويل أي اعتماد عملية التحويل من النظام الثنائي الى النظام العشري .

٤-عملية تطبيق العامل XOR

يتم في هذه العملية اخذ القيم الناتجة من العملية السابقة وتطبيق عليها XORوبأستخدام مفتاح تشفير محدد(k) وكما موضح في المعادلة (2) .

$$Ci = E_{ki}(mi) = mi \ (+) \ ki \quad .....(2)$$

حيث Ci, mi , kiتمثل رموز او مراتب ارقام عشرية يتم ادخال خلال عملية التشفير ،و (+) تمثل المازج ،اما عملية فك الشفرة فتتم حسب المعادلة (3)

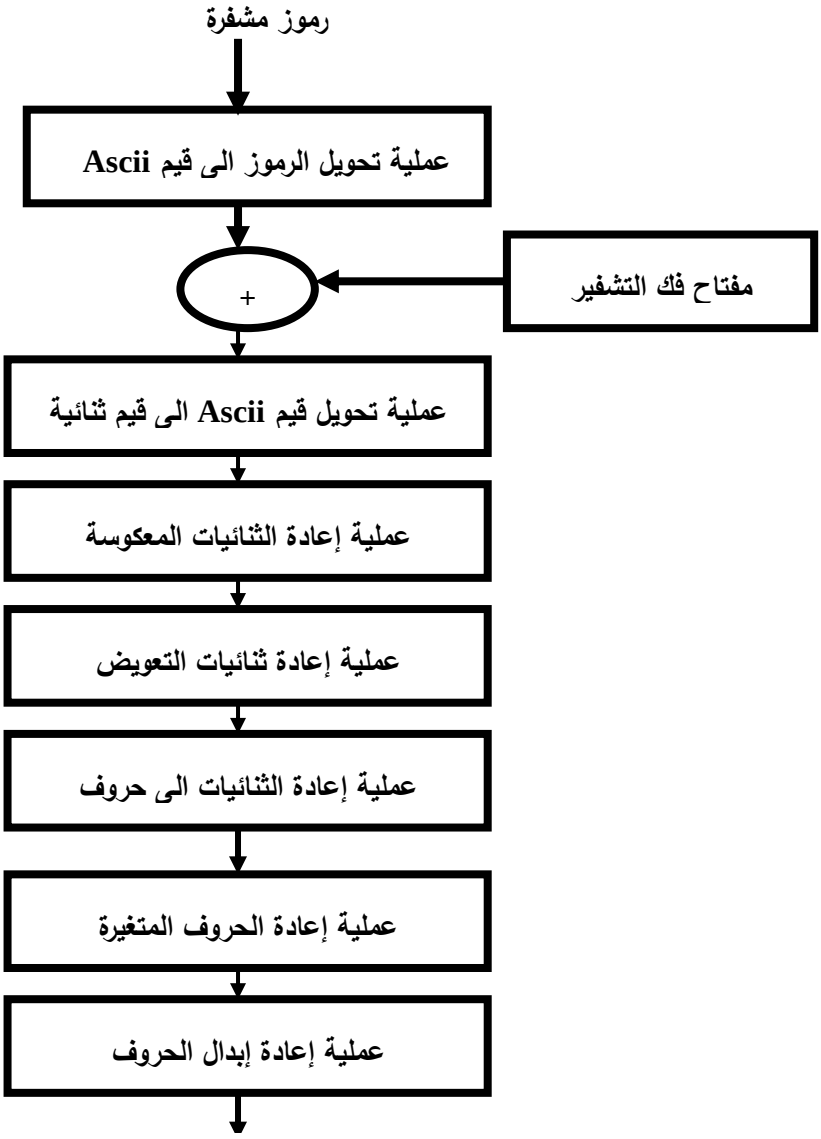
$$D_{ki}(Ci) = Ci \ (+) \ ki = (mi(+) \ ki) \ (+) \ ki = mi \quad .....(3)$$

حيث يتم إنتاج قيم جديدة فمثلا (1 =2 xor 3) أي ان (01=10 xor 11)، ومن المعروف بأن تطبيق xor تنتج واحد للقيم المختلفة وتنتج صفر للقيم المتشابهة ولغرض ارجاع هذه القيم الى قيمها الأصلية في عملية فل التشفير يتم ذلك بإدخال نفس مفتاح التشفير المستخدم هنا وتطبيق عليه xor ايضا،فمثلا للإرجاع القيمة(3)الى ملف التشفير يتم ذلك (11=10 xor 01) او (3= 2 xor 1) ان افضل الأدوات لتشفير القيم الرقمية هي استعمال + (exclusive or) xor وهي دالة يتم تطبيقها على جمع الـ Bits التي يتألف منها الرقم .

وفي الخطوة الاخيرة يتم تحويل القيم الناتجة من العملية السابقة الى الرموز المقابلة لها وبتطبيق دالة التحويل على القيم الناتجة نحصل على مجموعة من الرموز والتي تمثل رموز التشفير للنص المدخل.

فك التشفير

وهي العملية الرئيسية الاخرى في هذا النظام ،الشكل (3) يبين هذه العملية ، حيث تشمل على عمليات مماثلة للعمليات تشفير النص المدخل ولكن تبدا وتسير هذه العمليات بأتجاه معاكس للعمليات السابقة حيث تبدا من عملية الحصول على قيم Ascii من الرموز المشفرة الناتجة من عملية التحويل الى رموز وهي العملية الأخيرة في عمليات التشفير وتنتهي بعملية عكس التبادل للحروف للغرض الحصول على حروف النص المدخل في النهاية ،أي ان هذه العملية تكون سيرها معاكس للعمليات السابقة وكذلك عمل كل عملية منها تكون باتجاه معاكس ،وقد حصلنا على ملف النص المدخل في نهاية هذه العملية فأن هذا يدل على نجاح نظام التشفير المقترح وهذا ماتم الحصول عليه فعلا.



الشكل(٣) عمليات فك التشفير

وفيما يلي شرح موجز للخطوات فك التشفير:-

١-عملية تحويل الرموز الى قيم Ascii

يتم في هذه العملية تحويل رموز التشفير الى قيم Ascii المقابلة لها وبنفس الطريقة المستخدمة في عملية التشفير.

٢-عملية إعادة تطبيق العامل XOR

تتم هذه العملية حسب المعادلة(3) أي تطبيق XOR على قيم المشفرة وباستخدام نفس المفتاح المستخدم في عملية تشفير النص المدخل .

٣-عملية تحويل قيم Ascii الى قيم ثنائية

يتم هنا تفكيك كل بايت الى الثنائيات المقابلة لها ،حيث تم ذلك بتطبيق العامل and وباستخدام المعيار $80مع كل بايت أي ان byte and $80 ،حيث نحصل على الثنائيات المقابلة للقيم .

٤-عملية إعادة الثنائيات المعكوسة

يتم اخذ كل ثماني ثنائيات متتالية(من اليسار الى اليمين)أي في صناديق اعادة العكس(s1,…,s8) واجراء عليها عملية اعادة لعكس ترتيبها ،أي عند تطبيق هذه العملية على الثنائيات(10100001)تحول الى (10000101).

٥-عملية إعادة ثنائيات التعويض

يتم في هذه العملية اخذ كل ثمانية ثنائيات متتالية (ومن اليسار الى اليمين)أي بأستخدام صناديق اعادة التعويض(s1,…,s8) حيث يتم عليها عملية اعادة للقيم ،فمثلا عند ادخال الثنائيات (10000101)تحول الى (01111010).

٦-عملية إعادة الثنائيات الى حروف

تم في هذه العملية تحويل القيم الثنائية الى الرموز وذلك عن طريق تحويل القيم الثنائية الى قيم Ascii وباستخدام طريقة تحويل الاعداد الثنائية الى الاعداد العشرية، ثم تحول القيم الناتجة الى رموز Ascii المقابلة لها.

٧-عملية إعادة الحروف المتغيرة

يتم في هذه العملية عكس التغيرات على الرموز ،حيث يتم اولا عملية ايجاد موقع الحرف القديم(a)وحسب المعادلة (٤).

$$a = f(a) - k \text{……..(4)}$$

وان $f(a) = j + i$

حيث j تمثل موقع الحرف المشفر، i تمثل موقع حرف كلمة السرالمقابل للحرف المشفر(أي يجب استخدام نفس كلمة السرالمستخدمة في التشفير) ،فمثلا حروف التشفيرOZEODJEOVPWJU

نأخذ كل ثماني حروف متتالية منها اي OZEODJEO مع كلمة السر

S	T	A	R	W	A	R	S
O	Z	E	O	D	J	E	O

نحصل على الحروف الاتية:-

L	G	E	X	H	J	N	W

ثم نأخذ ثماني حروف التالية

S	T	A	R	W	A	R	S
V	P	W	J	U			

نحصل على الحروف الاتية:-

D	W	W	S	Y			

أي يتم في هذه العملية اعادة الحروف الى حروفها قبل التحويل ،أي ان ناتج الحروف السابقة يكون L GEXH JNW DWWSY ومن ثم تدخل الحروف الى عملية اعادة الى الحروف الأبجدية وذلك عن طريق اخذ كل حرف واستخراج الحرف الأبجدي المقابل له أي حروف مصفوفة كلمة السر هي EDICHMBGLQSTARWFKPYJOXNVUZ اما الحروف الابجدية فتكون ABCDEFGHIJKLMNOPQRSTUVWXYZ فيكون ناتج الحروف المشفرة السابقة هي :- I HAVE TWO BOOKS

٨-عملية إعادة إبدال الحروف

يتم اخذ كل ستة رموز متتالية واجراء عليها عملية عكس لتبديل مواقع الحروف وحسب المفتاح المحدد في عملية التشفير (435612)،حيث يبدل الحرف الاول في مع الحرف الخامس والحرف الثاني يبدل بالحرف السادس ويبدل الحرف الثالث بالحرف الثاني ويبدل الحرف الرابع بالحرف الاول ويبدل الحرف الخامس بالحرف الثالث ويبدل الحرف السادس بالحرف الرابع ،وتعتبر هذه العملية هي العملية الاخيرة والتي بعدها نحصل على النص المدخل .

المصادر

[1] Beker H. & piper F. ,"Cipher Systems The Protection of Communications",Nothwood publications,U.K.,1982.

[2] Seberry J. & Pieprzyk J. ,"Cryptography An Introduction to computer Security",prentice-Hall Inc.,U.S.A,1989.

[3] Dennig D.E.R , "Cryptography and data security",Addison-wesley publishing company Inc.,U.S.A., 1982.

[4] بروس بوزورت ،"الرموزالشفرات والحاسبات مقدمة الى آمن المعلومات" ، الطبعة الاولى،١٩٨٩.

[5] الحمداني ،وسيم عبد الامير، "ا نظمة التشفير" ،الطبعة الاولى،١٩٩٢.

[6] د.وسيم عبد الامير الحمداني وسن شاكر عواد ، "انظمة التشفير الانسيابي "،كتاب غير منشور ،بغداد،١٩٩٧.

[7] Schneier B. , "Applied Cryptography protecols, Algorithm and source code in c ", John wiley and sons ,Inc.,U.S.A,1996.

الملحق

ولغرض توضيح عملية التشفير تم اخذ الملف النصي والذي يحوي على المعلومات الاتية:-

رقم الحساب	الاسم	العنوان	
101	Jones Tool Co	Chicago,IL	60605.
102	HAL Computers ,Inc	Armonk,NY	10504.
103	Going Systems Group	Seattle,WA	98124.
104	TOH Steel Co	Pittsburgh,PA	15213.
105	Cipher System,Inc	Arlington,VA	22209.
106	G & O Co,Inc	Houston,TX	77002.
107	LSI Co, Inc	New Haven,CT	06520.
108	I/O Devices Corp,	Holmdel,NJ	07733.
109	CRT Inc,	Fresno,CA	93710
110	Crypto Systems,Ltd	Rockville,MD	20852.

حيث ادخل الملف السابق الى عملية التبديل للحروف وذلك بأخذ كل ستة حروف متتالية ومن اليسار الى اليمين وأجراء عليها عملية التحويل او التبديل وحسب مفتاح المزج المحدد(435612) مع ملاحظة ان الحروف الأخيرة اذا كانت اقل من ستة تترك كما هي بدون تحويل اوتبديل فكانت النتائج التي حصلنا عليها كما يلي:-

```
1  10oJne  T oos oC  l C hi  og,Ica   6L 501006    2  LCoHAtuermpI,ncs mron AYN
 k,1 05  013 04  Go   gSyinmes stuop GrtatlSeAW  e,8912  40  41T OH  etel S o
C   p  stbuit,hPArg5121  50  31  Ci  re Sphetm,ys c AInnigtrlV,A on2 22  016 09
  G  O  C &nIc o,      sutoHoXT  n,  77  120700       ICoLSnIc ,       we H Nne
,Cav   0T 021065    8 O/ D Iciesevrop, CoHlm  ,lNJde      373107    09RCT   ,c
In      F re  ,oCAsn      7310 9 0  11C ry   oSyptmes,st dRoLtivllckDM  e,0285
2_
```

ومن ثم ادخلت الحروف الناتجة من العملية السابقة الى عمليات التحويلات وتغيرات للحروف واعتمادا على كلمة السر المدخلة والتي كانت **STAR WARS** فكانت النتائج التالية:-

```
1  10wQrh  J wwy wI  t I gl  wb,Lie   6T 501006    2  TIwGEjohpafL,riy apwr EUR
 s,1 05  013 04  Bw   bYulrahy yjowf BpjejtYhEN  h,8912  40  41J WG  hjht Y w
I   f  yjdolj,gFEpb5121  50  31  Il  ph Yfghja,uy i ELrrlbjptX,E wr2 22  016 09
  B  W  I &rLi w,      yojwGwVJ  r,  77  120700       LIwTYrLi ,       nh G Rrh
,Iex   0J 021065    8 W/ C Lilhyhxpwf, IwGta  ,tRQch      373107    09PIJ   ,i
Lr      M ph  ,wIEyr      7310 9 0  11I pu   wYufjahy,yj cPwTjlxttisCA  h,0285
2
```

وبتقسيم الحروف الناتجة الى مجاميع وبطول كلمة السر واستخراج الحروف حسب العلاقة(١)السابقةنحصل على النتائج الاتية:-

```
1  10pKry  G wor pC  t Z dl  ot,Ece   6L 501006    2  QIoYWdoymawE,kcy rmwj WNL
 s,1 05  013 04  St   bQnelayv ybhpy BhgebmRbEF  e,8912  40  41J OY  zdhl V w
Z   x  rddgij,xXWjb5121  50  31  Zi  py Rxzhbw,uq b WFrjibbimR,E oo2 22  016 09
  B  O  B &kFi o,      vobpYqVB  o,  77  120700       LZpMSrDf ,       ny Y Klh
,Zbx   0B 021065    8 P/ U Fideyyqiqf, ZtGls  ,mLQte      373107    09PZC   ,b
Fr      E mh  ,oBWsr      7310 9 0  11Z mu   oRnyjrey,qc uJwLglpmmcsTW  h,0285
2
```

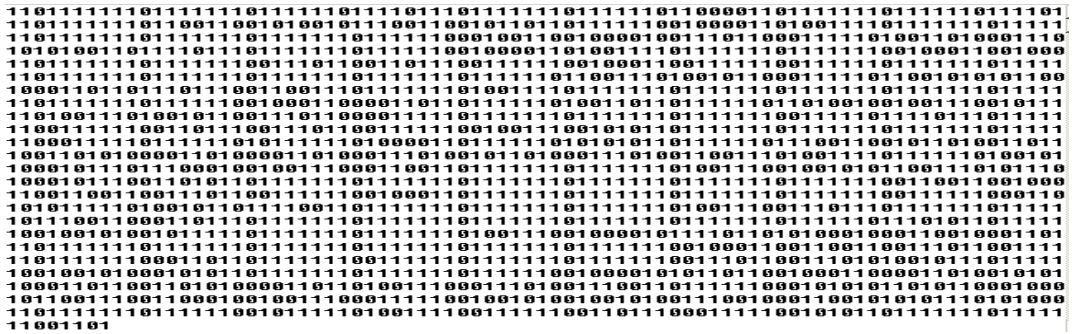
ومن ثم ادخلت النتائج السابقة الى عملية التحويل الى قيم **Ascii** وكما يلي:-

```
32493232494811275114121323271321191111143211267323211632903210010832321111164469
99101323232547632534849484854323232325032328173111898710011112110997119694410799
12132114109119106328778763232115444932485332324849513248523232831163232329881110
10110897121118321219810411212132661041031019810982986970323210144565749503232524
83232524974327989323212210010410832863211932323290323232120323211410010010310510
64412088871069853495049323253483232514932329010532321121212328212012210498119441 1
71133298328770114106105989810510982446932111111503250503232484954324857323232663
23279323266323810770105321114432323232323211811198112891138666323211144323255553
23249504855484832323232323232769011277831146810232443232323232323211012132893275
10810444909812032323248663248504948545332323232563280473285327010510010112112111
31051131024432901167110811532324410976811161013232323232325155514948553232323248
57809067323232449832327011432323232323269321091043232441116687115114323232323232
55514948325732483232494990321091173232321118211012110611410112144113993211774119
76103108112109109991158487323210444485056533232 50
```

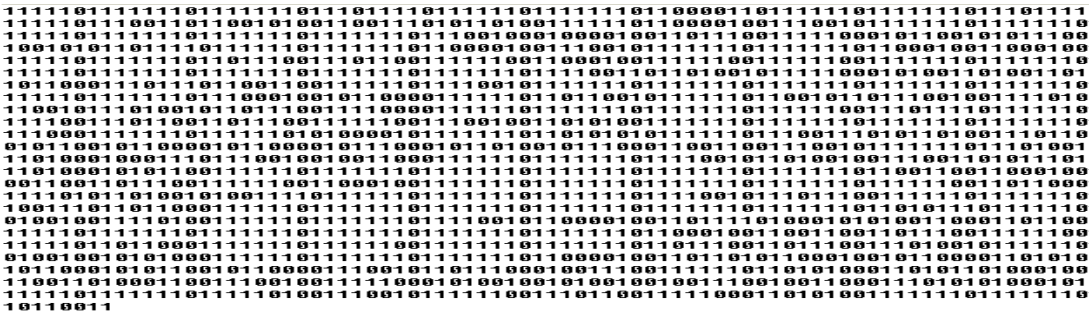
```
00100000001001100110101101000110011010010000001101111001011000010000000100000
00100000001000000010000000100000001111011001111110110001001110000010110010111000 1
01011100100001000100000001000000011011110011011000000100000011011100110110111
00100000001000000011000100110010000110000001101110011000000011000000100000000100000
00100000001000000010000000100000001001100011011000000100000011000000100000000100000
01110010010001000110011000100000001011000010000000100000001000000010000000100000
00100000001000000011011100111001000000010111000010000000100000001000000010000000100000
00100000001000000010000000100000001011000010000000100000001000000010000000100000
00111000100100000101101100010000001011100010000000100000001000000010000000100000
00110000001000000011000100110010000110000001101110011000000011000000100000000100000
00111000001011010011000100111100000100000001000000010000000110000010000100000
00110000001100100011000100110000001101110011010100100000001000000010000000100000
01100010101111001011110010111000010110101001111000101100110001011000010000001011010
01110100011000111011011000111001000000010000000100000001011000011011011001100000100
01110100011000100100000100000001000000010000000100000001000000011000000111001
00110011001100010011000000110111001000000010000000100000001000000010000000110000001110010
01010000010111010010000011001000000010000000100000001011000110000100000010000000
01000110011100100010000000100000001000000010000000100000001000000010000100010100100000
01101101110100000100000001000000010111011111010000100101011101110010
00100000001000000010000000100000001000000010000000100000001101110011001100110001001100000
00100000001110010010000000110000010000000100000011000010011000010000000
01110101011101010010000000100000001000000011011110101000110111001111001011010
01110010011001010111100100101110000111000101110001100100000001110101010010100111011
01001100011001110110111000111000001101101011101011100011010100000010000000
00100000001000000011010000010110000011000000110000101110000111000001101010010000000100000
00110010
```

ومن ثم تم تحويل القيم السابقة الى الثنائيات المقابلة لها كما يلي:-

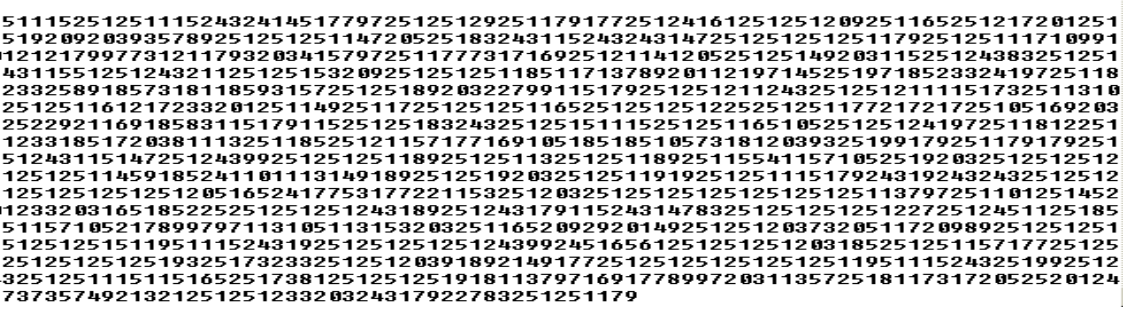
ومن ثم تم إجراء عدة عمليات على هذه الثنائيات الاولى عملية التعويض حيث تم تعويض(0) بالـ(1) فكانت النتائج كما يلي:-



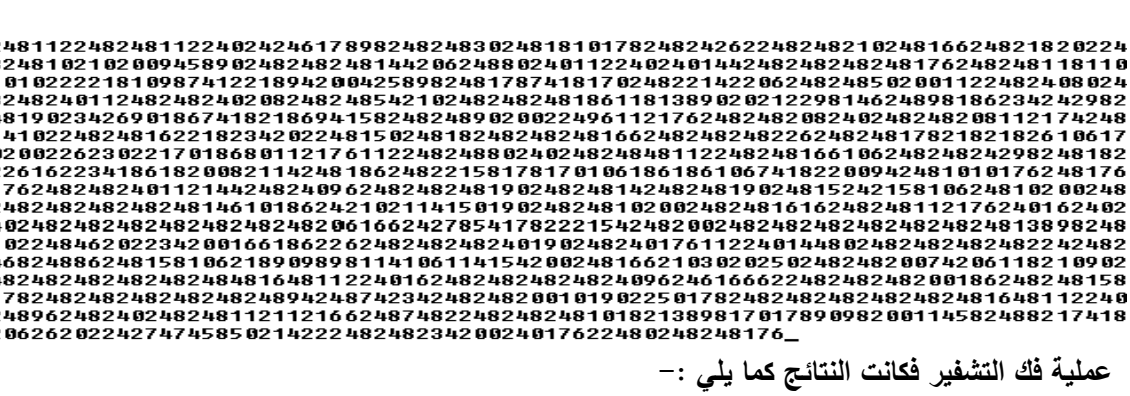
وبعد ذلك تم إجراء عملية عكس حيث تم أيضا تم اخذ كل ثمانية ثنائيات متتالية من اليسار الى اليمين فكانت النتائج كما يلي:-



ومن بعد ذلك تم تحويل الثنائيات الى قيم Ascii بعد هذه التحويلات فكانت النتائج كما يلي:-

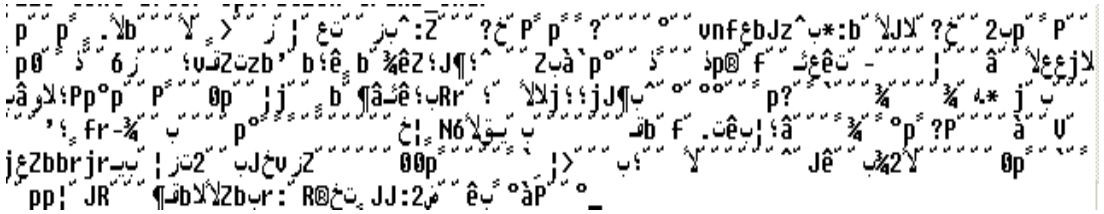


وبعد ذلك تم تطبيق العامل xor على القيم الناتجة مع مفتاح محدد ويجب هنااستخدام نفس المفتاح عند



عملية فك التشفير فكانت النتائج كما يلي :-

وبعد ذلك ادخلت القيم الناتجة الى عملية التحويل الى رموز المقابلة للقيم السابقة ،حيث تم الحصول على سلسلة من الرموز تمثل رموز التشفير الناتجة للنص المدخل والتي تمثل النص المشفر كما يلي:-



ومن ثم تبدا العملية الرئيسية الثانية في النظام وهي عملية فك التشفير تبدا بالعملية الاولى لها وهي عملية

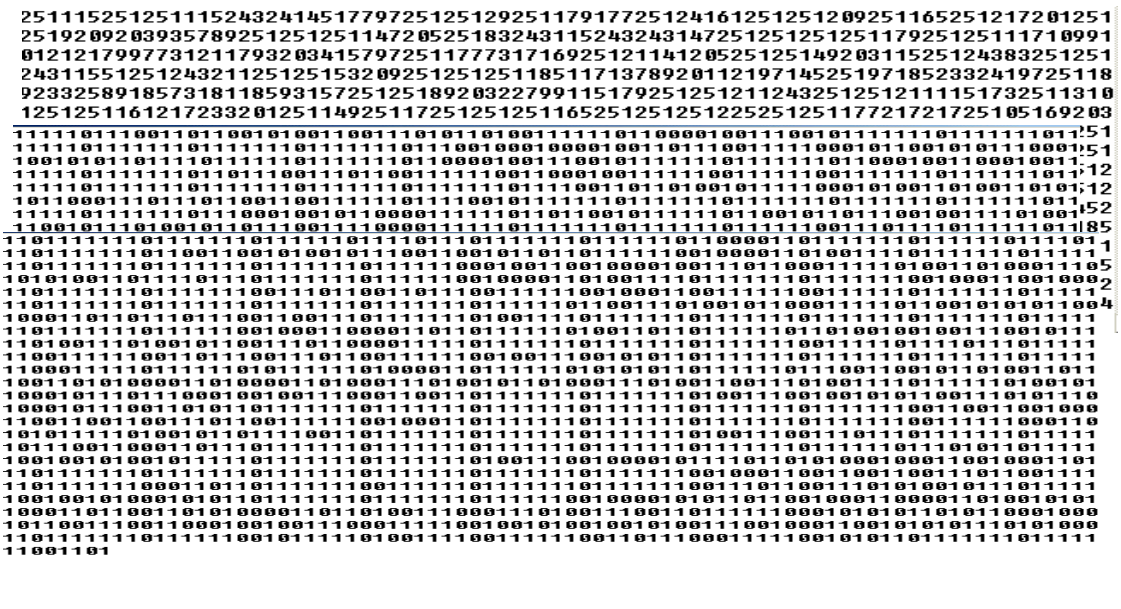
تحويل الرموز الناتجة من التشفير الى قيم Ascii فكانت النتائج كما يلي:-

ومن بعد ذلك تم ادخال النتائج السابقة الى العملية الثانية من عمليات فك التشفير وهي عملية اعادة تطبيق العامل XOR ومع المفتاح المستخدم في التشفير وكما يلي:-

ومن بعد ذلك تم ادخال النتائج السابقة الى العملية الثالثة من عمليات فك التشفير وهي عملية تحويل قيم Ascii الى قيم ثنائية فكان الناتج كما يلي:-

ومن ثم ادخال النتائج السابقة الى العملية الرابعة من عمليات فك التشفير وهي عملية إعادة الثنائيات المعكوسة فكانت النتائج لهذه العملية كما يلي:-

ومن ثم تم ادخال النتائج السابقة الى العملية الخامسة من عمليات فك التشفير وهي عملية إعادة ثنائيات التعويض فكانت النتائج كما يلي:-



ومن ثم ادخلت النتائج الى العملية التالية من عمليات فك التشفير وهي عملية إعادة الثنائيات الى حروف حيث تحول الثنائيات اولا الى قيم عشرية ومن ثم تحول القيم الى الرموز المقابلة لها فكانت النتائج كمايلي :-

```
 109 119 106 32 87 78 76 32 32 115 44 49 32 48 53 32 32 48 49 51 32 48 52 32 32
83 116 32 32 32 98 81 110 101 108 97 121 118 32 121 98 104 112 121 32 66 104 103
 101 98 109 82 98 69 70 32 32 101 44 56 57 49 50 32 32 52 48 32 32 52 49 74 32 7
9 89 32 32 122 100 104 108 32 86 32 119 32 32 32 90 32 32 32 120 32 32 114 100 1
00 103 105 106 44 120 88 87 106 98 53 49 50 49 32 32 53 48 32 32 51 49 32 32 90
105 32 32 112 121 32 82 120 122 104 98 119 44 117 113 32 98 32 87 70 114 106 105
 98 98 105 109 82 44 69 32 111 111 50 32 50 50 32 32 48 49 54 32 48 57 32 32 32
66 32 32 79 32 32 66 32 38 107 70 105 32 111 44 32 32 32 32 32 32 118 111 98 112
 89 113 86 66 32 32 111 44 32 32 55 55 32 32 49 50 48 55 48 48 32 32 32 32 32 32
 32 76 90 112 77 83 114 68 102 32 44 32 32 32 32 32 32 32 32 110 121 32 89 32 75 10
8 104 44 90 98 120 32 32 32 48 66 32 48 50 49 48 54 53 32 32 32 32 56 32 80 47 3
2 85 32 70 105 100 101 121 121 113 105 113 102 44 32 90 116 71 108 115 32 32 44
109 76 81 116 101 32 32 32 32 32 32 32 51 55 51 49 48 55 32 32 32 32 48 57 80 90 67
 32 32 32 44 98 32 32 70 114 32 32 32 32 32 32 69 32 109 104 32 32 44 111 66 87
115 114 32 32 32 32 32 32 55 51 49 48 32 57 32 48 32 32 49 49 90 32 109 117 32 3
2 32 111 82 110 121 106 114 101 121 44 113 99 32 117 74 119 76 103 108 112 109 1
09 99 115 84 87 32 32 104 44 48 50 56 53 32 32 50
**********************************
 1  10pKry  G wor pC  t Z dl  ot,Ece    6L 501006     2  QIoYWdoymawE,kcy rmwj WNL
  s,1 05  013 04  St   bQnelayv ybhpy BhgebmRbEF  e,8912  40  41J OY  zdh1 V w
 Z   x  rddgij,xXWjb5121  50  31  Zi  py Rxzhbw,uq b WFrjibbimR,E oo2 22  016 09
   B  O  B &kFi o,      vobpYqVB  o,  77  120700       LZpMSrDf ,        ny Y K1h
,Zbx   0B 021065    8 P/ U Fideyyqiqf, ZtG1s  ,mLQte      373107     09PZC    ,b
Fr      E mh  ,oBWsr       7310 9 0  112 mu   oRnyjrey,qc uJwLg1pmmcsTW  h,0285
2_
```

ومن ثم تم ادخال النتائج السابقة الى العملية التالية وهي عملية إعادة الحروف المتغيرةوالتي تشمل على عملتين

```
 1  10wQrh  J wwy wI  t I gl  wb,Lie   6T 501006    2  TIwGEjohpafL,riy apwr EUR
  s,1 05  013 04  Bw   bYulrahy yjowf BpjejtYhEN  h,8912  40  41J WG  hjht Y w
 I   f  yjdolj,gFEpb5121  50  31  Il  ph Yfghja,uy i ELrrlbjptX,E wr2 22  016 09
   B  W  I &rLi w,      yojwGwVJ  r,  77  120700      LIwTYrLi ,       nh G Rrh
,Iex   0J 021065    8 W/ C Lilhyhxpwf, IwGta  ,tRQch      373107    09PIJ   ,i
Lr      M ph  ,wIEyr      7310 9 0  11I pu   wYufjahy,yj cPwTjlxttisCA  h,0285
2
=========================

 1  10oJne  T oos oC  1 C hi  og,Ica   6L 501006    2  LCoHAtuermpI,ncs mron AYN
  k,1 05  013 04  Go   gSyinmes stuop GrtatlSeAW  e,8912  40  41T OH  etel S o
 C   p  stbuit,hPArg5121  50  31  Ci  re Sphetm,ys c AInnigtrlV,A on2 22  016 09
   G  O  C &nIc o,      sutoHoXT  n,  77  120700      ICoLSnIc ,       we H Nne
,Cav   0T 021065    8 O/ D Iciesevrop, CoH1m  ,lNJde      373107    09RCT   ,c
In      F re  ,oCAsn      7310 9 0  11C ry   oSyptmes,st dRoLtivllckDM  e,0285
2
```

كما يلي:-

وبتطبيق العملية الاخيرة من عمليات فك التشفير(عملية إعادة إبدال الحروف)نحصل النص الصريح الذي تم تشفيره(مع ملاحظة ان البيانات لهذا النص تم اخراجها بشكل متتالي نتيجة للملفات المستخدمة في الخزن)

ومن الجدير بالذكر ان النظام تم تصميمه باستخدام لغة باسكال بمترجم Turbo Pascal ver.7وكما يلي:-

```
101     Jones  Tool Co     Chicago,IL    60605102     HAL Computers ,Inc Armonk,
NY     10504103     Going Systems Group Seattle,WA    98124104     TOH Steel Co
       pittsburgh,PA  15213105      Cipher System,Inc  Arlington,VA    22209106
     G & O Co,Inc       Houston,TX      77002107      LSI Co, Inc        New Hav
en,CT    06520108      I/O Devices Corp,  Holmdel,NJ      07733109      CRT Inc,
          Fresno,CA      93710110      Crypto Systems,Ltd Rockville,MD    2085
2_
```

Depending Character and Binary Changes for Information Coding

S. A.Sead / college of science /computer science department

Abstract

The research introduces Algorithm to coding the plain text. This Algorithm includes the Enciphering stage and the deciphering stage:

The Enciphering stage can doing set from the operations, the first can swap the text symbols locations to other locations using merge key was limited randomly, the second doing some transformation operations on characters and the others on binaries that contain the entered symbols, it's meaning entering the result binaries to some operations as substitute operation, inverse operation and transfer operation depending on ASCII symbols. when applying the XOR operand on the ASCII values by limited enciphering key and generating the symbols of the code that was results from the previous operations, then a symbolic file was completed which contain a set of symbols represents the Enciphering file.

The Deciphering stage includes some of operations which execute in inverse way of previous operations to obtaining on the entered plain text, also to know that all stages was right.