انشاء نظام يقوم بأستخدام حركات التشكّل العربية في توليد مفاتيح التشفير للبيانات السرية (الامن المعلوماتي للبيانات عبر الشبكات الالكترونية)

م.م. استبرق عبد الرضا كاظم الشمري

الخلاصة

ان موضوع الأمن المعلوماتي يرتبط ارتباطا و ثيقا بأمن الحاسوب فلا يوجد أمن للمعلومات إذا لم يراعى أمن الحاسوب ، و في ظل التطورات المتسارعة في العالم و التي أثرت على الإمكانات التقنية المتقدمة المتاحة و الرامية الى خرق منظومات الحاسوب بهدف السرقة أو تخريب المعلومات أو تدمير أجهزة الحاسوب ، كان لا بد من التفكير الجدي لتحديد الإجراءات الدفاعية و الوقائية و حسب الإمكانات المتوفرة لحمايتها من أي اختراق أو تخريب ، و كان على إدارة المنظمات أن تتحمل مسؤولية ضمان خلق أجواء امنية للمعلومات تضمن الحفاظ عليها .

يعد التشفير من احدى الطرق الرئيسية والمهمة في الوقت الحاضر في مجال امنية المعلومات. و لا يخفى ان الخوارزميات والطرق المستخدمة لتشفير الرسائل عن طريق استخدام اللغة العربية قليلة وقديمة ولا توجد خوارزميات تشفير او خوارزميات توليد لمفاتيح للتشفير حديثة تستثمر الخصائص الموجودة في اللغة العربية على غرار اللغة الانكليزية ، وان وجدت فهي قليلة وغير شائعة الاستخدام. في هذا البحث المقترح سيتم توليد مفتاح قوي يقوم بتشفير البيانات السرية (كالرسائل والصور السرية) عن طريق استخدام ترددات حركات التشكل العربية داخل النصوص العربية (والمقصود بالترددات هو عدد مرات ظهور كل حركة داخل النص الواحد) والدمج بين نوعين من الحركات عن طريق استخدام نظرية (الالتفاف (الالتواء) الرياضية) . ولكي يتم التأكد من قوة مفتاح التشفير المتولد من هذه الطريقة يجب تقييس عشوائية هذا المفتاح ، فأذا كانت العشوائية عالية ، معناها ان المفتاح هو مفتاح رصين ولا يمكن كسره او اختراقه من قبل المخترقين او (الهكرز) ويمكن اعتماده في تشفير البيانات السرية.

ان مفاتيح التشفير المتولدة في هذه الطريقة المقترحة قد اثبتت نجاحها وكفائتها وكانت النتائج جيدة جدا بعد ان تم اختبارها من قبل المقاييس المعتمدة في هذا المجال .

مقدمة عن مفهوم التشفير

ان التطورات الحديثة في تقنية المعلومات أحدثت تغيرات مستمرة و مضطربة في أساليب العمل و الميادين كافة إذ أصبحت عملية انتقال المعلومات عبر الشبكات المحلية و الدولية و أجهزة الحاسوب من الأمور الروتينية في عصرنا الحالي و إحدى علامات العصر المميزة التي لا يمكن الإستغناء عنها لتأثيرها الواضح في تسهيل متطلبات الحياة العصرية من خلال تقليل حجم الأعمال و تطوير أساليب خزن و توفير المعلومات حيث أن انتشار أنظمة المعلومات المحوسبة أدى الى أن تكون عرضة للإختراق لذلك أصبحت هذه التقنية سلاحا ذو حدين تحرص المنظمات على إقتناءه و توفير سبل الحماية له .

إن الحاجة الى أمنية المعلومات ناتجة من الحاجة إلى تناقل المعلومات الخاصة لكل البيانات السرية كالعبارات العسكرية والدبلوماسية. هذه الحاجة هي قديمة بقدم الحضارة نفسها. فقد كان الأسبان القدماء، «يشفرون» عباراتهم العسكرية والتشفير هو احدى الاليات التي تحمي تلك المعلومات القيمة، مثل المستندات أو الصور أو المعاملات الإلكترونية داخل الإنترنت، من الأشخاص غير المرغوب فيهم للحيلولة دون الوصول إليها أو تغييرها. يعمل التشفير

باستخدام صيغة رياضية (شفرة) ، ومفتاح لتحويل البيانات المقروءة (نص عادي) إلى شكل لا يستطيع الآخرون فهمه (نص مشفر)». والشفرة هي الوصفة العامة للتشفير، والمفتاح الخاص بك يجعل البيانات المشفرة فريدة من نوعها بحيث يمكن فك تشفيرها فقط ممن يعرف هذا المفتاح. وعادة ما تكون المفاتيح عبارة عن سلسلة طويلة من الأرقام التي تحميها آليات المصادقة المشتركة مثل كلمات المرور، أو الرموز، أو القياسات الحيوية مثل بصمة الأصبع.

أهداف نظام التشفير

يحقق التشفير الأهداف التالية :

١. السرية: هي عملية حفظ المعلومات أو البيانات وجعلها سرية بحيث لا يكون متعارف عليها أي تكون غير مفهومة بالنسبة للآخرين.

٢. الصلاحية: معرفة إن الرسالة مرسلة في الوقت المناسب ومن الشخص المناسب وبدون تدخل ، لذلك يضاف مع الرسالة التوقيع و الوقت لغرض تثبيت صلاحية الرسالة .

٣. التكاملية: التأكد من إن الرسالة غير محذوف منها شيٌ أو مضاف لها شيٌ .

٤. عدم التنكر : هي الخدمة التي تمنع الشخص من إنكار الرسالة المرسلة اليه أي الرسالة المنقولة.

مكونات نظام التشفير

إن نظام التشفير يتكون من الاجزاء التالية

- النص الصريح :(plaintext) : وهو النص المراد تشفيره. ،ويرمز له بالرمز (M)
- النص المشفر :(Cipher text) وهو النص المراد فتح الشفرة له. ،ويرمز له بالرمز (C)
- المفتاح : (Key) وهو المفتاح المستخدم في تشفير وفك الشفرة للنص.، ويرمز له بالرمز (K) والمفتاح عبارة عن كلمة السر المستخدمة في خوارزمية التشفير أو فك التشفير ويعتبر من أهم الأشياء التي يجب إخفائها ولا يجب معرفتها إلا من قِبل المخول لهم فك الشفرة
- خوارزمية التشفير :(Encryption)وهي الخوارزمية المستخدمة لتحويل النص الصريح إلى نص مشفر ،ويرمز لها بالرمز (Ek)
- خوارزمية فك الشفرة (Decryption) :وهي الخوارزمية المستخدمة لتحويل النص المشفر إلى نص صريح ،ويرمز لها بالرمز (Dk)

×× شكل رقم (١) توضح الاليات والعمليات الاساسية لنظام التشفير :

شكل رقم (١) يوضح توضح عملية التشفير

اهمية للغة العربية في مجال تشفير البيانات

اللغة هي وسيلة من وسائل الاتصال الفكري بين أبناء المجتمع وهي أداة التفاهم ونقل الأفكار والحضارة من جيل

إلى آخر ،وتعد اللغة الركيزة الاساسية في المجتمع، فعبر اللغة يتم نقل المعلومات والتقنيات والحضارة من جيل إلى آخر. إن الاهتمام باللغة نابع من أهمية اللغة في حياة الشعوب، فاللغة هي الوسيلة التي يمكن بها تحليل أية صورة أو فكرة ذهنية إلى أجزائها أو خصائصها، والتي بها يمكن تركيب هذه الصورة مرة أخرى في أذهاننا وأذهان غيرنا، وذلك بتأليف كلمات ووضعها في ترتيب خاص.

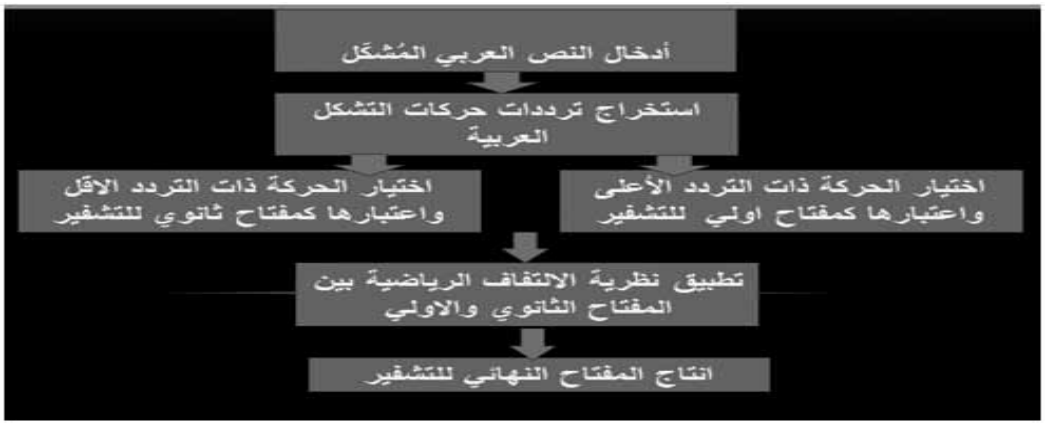
اللغة العربية هي إحدى اللغات الإنسانية المنحدرة من اللغات السامية، وعلى الرغم من كون أنَّ للعربية السبق في مجال اللسانيات ولكن الأبحاث في معالجة اللغة العربية حاسوبيا كانت متأخرة، واحدى أسباب تأخر العمل في مجال اللسانيات الحاسوبية العربية هو مشاكل التشكيل في اللغة العربية.

أن الهدف الاساسي من وجود هذه الحركات هو للتمييز بين كلمة واخرى لها نفس الحروف وتختلف بالمعنى مثلا (يَكونْ ، يُكَّوْن) . تعد النصوص العربية المشكلة وسيلة فعالة وممتازة في مجال تشفير البيانات السرية وذلك من خلال استخدام حركات التشكيل العربية في استخراج مفاتيح قوية خاصة بالتشفير . تعد اللغة العربية من اهم اللغات التي تحتوي على معلومات غنية جدا لم يتم التعرف عليها لحد الان بشكل تام ومتكامل بطريقة تدعم انظمة التشفير وأمنية المعلومات . حيث من الممكن استحداث خوارزميات تشفير على اسس علمية ورياضية حديثة معتمدة بشكل اساسي على اللغة العربية ومن اهم الخصاصئص التي من الممكن استغلالها في هذا المجال هو وجود حركات التشكّل العربية وقواعد اللغة العربية والمرادفات اللغوية ..... الخ

نظام التشفير المقترح بأستخدام حركات التشكل العربية

في هذا البحث ، قمنا بأقتراح طريقة جديدة لتوليد مفاتيح التشفير القوية وذلك من خلال استخلاص تلك المفاتيح من النصوص العربية المشكلة وبالاعتماد على ترددات حركات التشكيل العربية (اي عدد مرات ظهور الحركة في النص الواحد) . ايضا وقد تم استخدام نظرية الالتفاف الرياضية (Convolution) وذلك من اجل زيادة العشوائية على المفتاح المتولد وجعله اكثر قوة وعشوائية. بعدها سيتم حصر معدل الارقام المتولدة ضمن نطاق معين من خلال الاستفادة من وجود نظرية الاعداد الاولية في التشفير . الشكل رقم (٢) يوضح الية سير عمل النظام المقترح في البحث.

شكل رقم (٢) : يوضح الخطوات الاساسية والاليات لتوليد المفاتيح القوية للتشفير



خطوات عمل النظام المقترح

١. يتفق كل من الطرفان (المرسل والمستلم) على نص عربي مشكل
٢. يتم ادخال هذا النص الى النظام المقترح ويتم العمل بما يلي:

أ. يتم استخراج ترددات كل حركة من حركات التشكل العربية وخزن مواقعها في مصفوفة (والمقصود بالتردد هو عدد مرات ظهور كل حركة داخل النص)

ب. يتم أختيار التردد الاعلى من بين ترددات الحركات ليكون هو المفتاح الاولى للتشفير

ت. يتم اختيار احدى مصفوفات الترددات الخاصة ببقية الحركات لكي تكون عبارة عن مفتاح ثانوي.

ث. تطبيق نظرية الالتفاف(convolution) من المفاتح الثانوي للمفتاح الاولي (النهائي) للتشفير للحصول على مفتاح قوي جاهز للتشفير (مفتاح رئيسي)

ج. تقليص قيمة الارقام الخاصة بالمفتاح الرئيسي ضمن عدد اولي معين (اي حصر الارقام من ٠ الى العدد الاولي (٩٩٧)) .

٣. يتم استخدام المفتاح الرئيسي الناتج في عمليات تشفير النصوص والصور السرية لارسالها بشكل امن عبر شبكات الانترنت

مثال كامل يوضح الية عمل النظام

١. يتم الاتفاق على النص الاتي من قبل المرسل والمستلم:

فَيَجُوزَ عَلَيْه الانْتقَالُ وَلَوْ وَهَبَ مَا تَنَفَّسَتْ عَنْهُ مَعَادنُ الْجبَال وَضَحكَتْ مَا اخْتَلَفَ عَلَيْه دَهْرٌ فَتَخْتَلفَ منْهُ الْحَالُ عَنْهُ أَصْدَافُ الْبحَار منْ فلَز اللُّجَيْن وَسَبَائك الْعقْيَان وَنُثَارَة الدُّرِّ وَحَصيدَ الْمَرْجَان لبَعْض عَبيده مَا أَثَّرَ ذَلكَ في جُوده وَلاَ أَنْفَدَ سَعَةَ مَا عنْدَهُ وَلَكَانَ عنْدَهُ منْ ذَخَائر الإنْعَام مَا لاَ تَخْطُرُ لكَثْرَته عَلى بَال وَلاَ تُنْفدُهُ مَطَالبُ الأَنَام ؛ لأَنَّهُ الْجَوَادُ الَّذي لاَ يَغيضُهُ سُؤَالُ السَّائلينَ وَلاَ يُبَخِّلُهُ إلْحَاحُ الْمُلْحّينَ وَإنَّمَا أَمْرُهُ إذَا أَرَادَ شَيْئًا أَنْ يَقُولَ لَهُ كُنْ فَيَكُونُ فَمَا ظَنُّكُمْ ب

٢.أ. استخراج ترددات كل حركة وخزن مواقعها داخل الحقيقة داخل النص

- **استخراج ترددات حركة الفتحة**

١	٣	٨	١١	١٣	٢٨	٣٤	٣٦	٤١	٤٣
٤٥	٤٨	٥٢	٥٩	٦	٥٤	٥٧	٤	٧١	٧٣
٨٨	٩٤	٩٦	١٠٠	١٠٥	١١٢	١١٤	١١٦	١١٩	١٢١
١٢٨	١٣٥	١٣٧	١٤١	١٤٥	١٥٨	١٦٤	١٧١	١٧٥	١٨٨
٢٠١	٢١١	٢١٨	٢٢٠	٢٢٢	٢٣٧	٢٤٣	٢٤٧	٢٥٠	٢٦٤
٢٦٦	٢٧٦	٢٨٠	٢٩٠	٢٩٧	٣٠٦	٣١٠	٣١٣	٣١٥	٣١٨

٣٢٢ ٣٣٦ ٣٣٩ ٣٤٢ ٣٤٦ ٣٤٨ ٣٥١ ٣٥٣ ٣٥٥ ٣٥٨

٣٦٦ ٣٧١ ٣٧٣ ٣٧٥ ٣٧٨ ٣٨٥ ٣٩٧ ٣٩٩ ٤١٣ ٤١٩

٤٢٤ ٤٢٧ ٤٣٨ ٤٤٢ ٤٤٩ ٤٥٤ ٤٦٠ ٤٦٣ ٤٧٧ ٤٧٩

٤٨٩ ٤٩١ ٥٠١ ٥٠٤ ٥١٢ ٥١٤ ٥٢٢ ٥٢٨ ٥٣١ ٥٤٢

٥٥١ ٥٥٨ ٥٦١ ٥٦٤ ٥٦٩ ٥٨٣ ٥٩٩ ٦٠٤ ٦٠٩ ٦١١

٦١٥ ٦٢٦ ٦٣٠ ٦٣٢ ٦٣٥ ٦٣٨ ٦٤٦ ٦٥١ ٦٥٦ ٦٥٩

٦٦٩ ٦٧١ ٦٧٩ ٦٨١ ٦٨٥

- **استخراج ترددات حركة الضمه**

٥ ٣١ ٦٨ ٧٨ ١٥٢ ١٦١ ١٦٨ ١٧٨ ٢٠٩ ٢٤٥

٢٥٨ ٣٢٨ ٣٦٨ ٤٣١ ٤٣٣ ٤٦٦ ٤٧٢ ٤٧٤ ٤٨٤ ٣٨٧

٥٠٦ ٥١٧ ٥٣٥ ٥٣٧ ٥٤٠ ٥٤٥ ٥٦٧ ٥٧٤ ٥٧٦ ٥٨٦

٥٩٢ ٦١٩ ٦٢١ ٦٥٣ ٦٦١ ٦٦٤ ٦٧٣ ٦٧٦ ٦٨٨ ٦٩٠

- **استخراج ترددات حركة السكون**

١٥ ٢٤ ٣٨ ٦١ ٦٦ ٨٤ ١٠٢ ١١٠ ١٢٣ ١٣٠

١٣٩ ١٥٠ ١٥٦ ١٦٦ ١٧٣ ١٨٤ ١٩٦ ٢١٣ ٢٣١ ٢٣٥

٢٧٤ ٢٧٨ ٢٩٢ ٣٤٤ ٣٦٤ ٣٨٣ ٣٩٤ ٤١١ ٤٢٩ ٤٤٠

٤٦٨ ٥١٠ ٥٨١ ٥٩٠ ٦١٧ ٦٤٠ ٦٤٨ ٦٦٦ ٦٩٢

- **استخراج ترددات حركة الشدة**

٥٦ ٢٠٨ ٢٥٧ ٢٦٠ ٣١٢ ٥٠٣ ٥٢١ ٥٥٠ ٥٧١ ٥٩٦

٦٠٨ ٦٨٧

- **استخراج ترددات التنوين (ضم وفتح وكس)**

١٣٢ ٦٤٣ ٤٥٧

.ب. يتم اختيار مصفوفة ترددات (الفتحة) لان نسبة تكرارها داخل النص هي الاكثر ويتم اعتبارها المفتاح الاولي للتشفير.

١ ٣ ٨ ١١ ١٣ ٢٨ ٣٤ ٣٦ ٤١ ٤٣

٤٥ ٤٨ ٥٢ ٥٩ ٦ ٥٤ ٥٧ ٤ ٧١ ٧٣

٨٨ ٩٤ ٩٦ ١٠٠ ١٠٥ ١١٢ ١١٤ ١١٦ ١١٩ ١٢١

١٢٨ ١٣٥ ١٣٧ ١٤١ ١٤٥ ١٥٨ ١٦٤ ١٧١ ١٧٥ ١٨٨

٢٠١ ٢١١ ٢١٨ ٢٢٠ ٢٢٢ ٢٣٧ ٢٤٣ ٢٤٧ ٢٥٠ ٢٦٤

٢٦٦ ٢٧٦ ٢٨٠ ٢٩٠ ٢٩٧ ٣٠٦ ٣١٠ ٣١٣ ٣١٥ ٣١٨

٣٢٢ ٣٣٦ ٣٣٩ ٣٤٢ ٣٤٦ ٣٤٨ ٣٥١ ٣٥٣ ٣٥٥ ٣٥٨

٣٦٦ ٣٧١ ٣٧٣ ٣٧٥ ٣٧٨ ٣٨٥ ٣٩٧ ٣٩٩ ٤١٣ ٤١٩

٤٢٤ ٤٢٧ ٤٣٨ ٤٤٢ ٤٤٩ ٤٥٤ ٤٦٠ ٤٦٣ ٤٧٧ ٤٧٩

٤٨٩ ٤٩١ ٥٠١ ٥٠٤ ٥١٢ ٥١٤ ٥٢٢ ٥٢٨ ٥٣١ ٥٤٢

٥٥١ ٥٥٨ ٥٦١ ٥٦٤ ٥٦٩ ٥٨٣ ٥٩٩ ٦٠٤ ٦٠٩ ٦١١

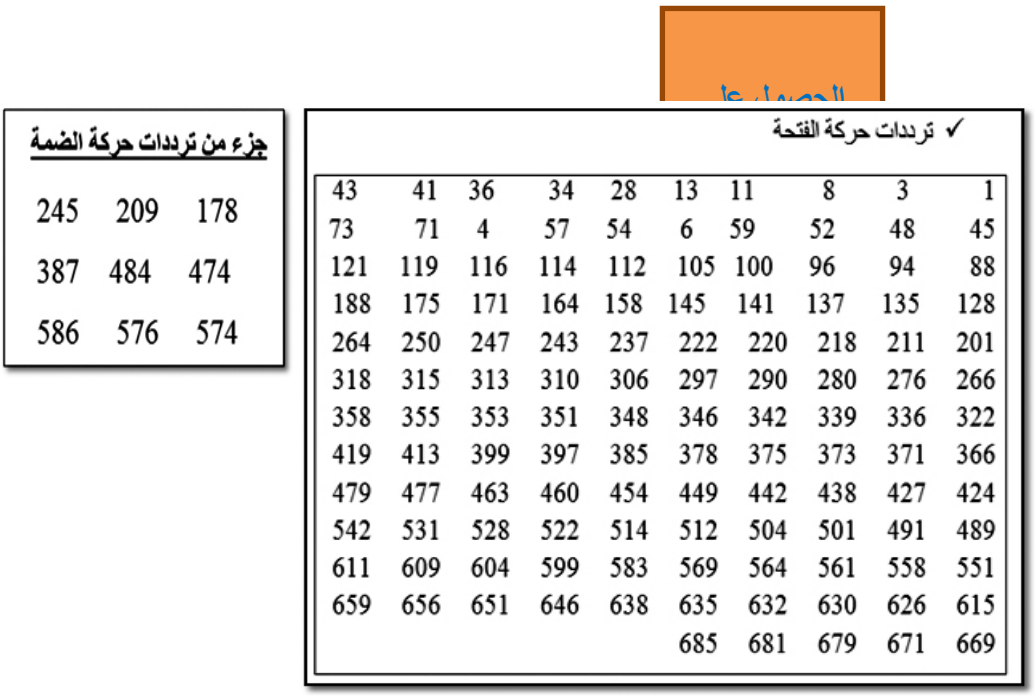
٦١٥ ٦٢٦ ٦٣٠ ٦٣٢ ٦٣٥ ٦٣٨ ٦٤٦ ٦٥١ ٦٥٦ ٦٥٩

٦٦٩ ٦٧١ ٦٧٩ ٦٨١ ٦٨٥

٣.ت. يتم اختيار مصفوفة حركة اخرى (على سبيل المثال حركة الضمة) ويتم استقطاع جزء منها واعتباره كمفتاح ثانوي للتشفير.

٣.ث. تطبيق الية ال (convolution) بين المفتاح الثانوي والاولي كما يلي :

اجراء عملية الالتفاف بين هاتين المصفوفتين



٤.ث. تقليل وحصر قيمة كل رقم من خلال ضغطها نسبة الى قيمة العدد الاولي (٩٩٧) للحصول على المفتاح النهائي للتشفير:

٥. بعد ان تم توليد مفتاح قوي وامن للتشفير . اصبح بألامكان استخدامه في تشفير مختلف البيانات (رسائل

135665	270438	356918	340197	323700	313956
208342	414573	605720	586766	572274	548978
290246	579001	849767	824576	807089	777817
372095	741821	1093811	1071904	1058905	1036049
437998	880239	1296965	1271887	1257740	1240687
505118	1009393	1483629	1449674	1428779	1412253
563697	1143170	1686118	1660498	1630120	1608467
640143	1300155	1923283	1900699	1874142	1850880
715524	1453216	2158391	2138726	2113983	2085930
613079	1281638	1937249	1924514	1901502	1873809
386174	764000	1137608	1130076	1119638	1110402
10396	6573	4365	2296	743	178
49142	40721	43377	35944	19855	8484
147720	133120	145284	130495	81954	37568
304608	292066	308994	292883	191402	90326
525491	503025	489584	472778	310153	146962
749355	722878	708165	687343	453238	216094
1011900	987515	969333	943156	623564	298774
1220833	1199367	1181294	1157099	769284	370460
1392970	1378883	1365160	1345909	895956	433784
1584014	1567027	1548969	1532244	1020983	498102

سرية بلغات مختلفة أو صور) عن طريق احدى طرق التشفير الشائعة .
كما هو مبين بالمثال الاتي :

21 14 114 22 71 183 88 198 217 98 50 33 83 25 142 136 80 85
226 74 202 186 137 159 172 32 228 35 192 26 93 237 125 120
109 135 216 119 19 214 65 82 70 14 143 251 239 148 113 154
225 194 116 38 96 34 198 21 226 161 213 249 152 184 98 223 36
138 105 229 158 118 134 236 240 98 216 22 160 196 126 47 146
162 116 148 253 240 229 178 55 115 201 221 66 3 202 251 79
196 228 46 63 114 80 160 194 119 183 76 256 155 211 215 200
194 130 125 147 214 91 121 186 223 82 140 83 205 122 85 83
123 30 78 233 0 54 225 123 98 30 10 179 36 128 161 185 186 10
130 160 53 233 99 36 92 167 36 22 235 251 236 51 55 234 102
132 149

١. الرسالة السرية (على شكل جملة) :

سيكون موعد اللقاء القادم يوم السبت»

٢. تحويل الرسالة الرسالة السرية الى مجموعة من الكودات (الرموز الرقمية) او ما يسمى (بالاسكي) :

١٥٨٧ ١٦١٠ ١٦٠٣ ١٦٠٨ ١٦٠٦ ٣٢ ١٦٠٥ ١٦٠٨ ١٥٩٣ ١٥٨٣ ٣٢ ١٥٧٥ ١٦٠٤
١٦٠٤ ١٦٠٢ ١٥٧٥ ١٥٦٩ ٣٢ ١٥٧٥ ١٦٠٤ ١٦٠٢ ١٥٧٥ ١٥٨٣ ١٦٠٥ ٣٢ ١٦١٠
١٦٠٨ ١٦٠٥ ٣٢ ١٥٧٥ ١٦٠٤ ١٥٨٧ ١٥٧٦ ١٥٧٨

٣. تشفير الرسالة باستخدام المفتاح النهائي للتشفير الذ تم توليد مسبقا :

الرسالة بعد التشفير

المناقشة والنتائج :

BR¯X? ×? RB? WÊ©ku? Û²ÞÌd%bà;?

٢. عملية تحديد ترددات الحركة الاولية والثانوية وكيفية اختيار المفتاح الثانوي .
٣. تطبيق نظرية الالتفاف الرياضي بين مصفوفتي الحركة الاولية والحركة الثانوية الذي يزيد من عشوائية المفتاح (حيث تم استخدام دالة الالتفاف الرياضي الموجودة في برنامج الماتلاب)
٤. حصر الارقام المتولدة ضمن عدد اولي معين (prime) مما يزيد أكثر في عشوائية المفتاح
٥. واخيرا يمكن إثبات سرية بعض طرق التشفير على أساس افتراض صلابة المشاكل الحسابية مثل تحليل حاصل ضرب عددين أوليين كبيرين أو حساب لوغاريتم منفصل. وفي الطريقة المقترحة تم تقييس المفتاح المتولد وفق طريقة تقييس رصينه تعتمد على اساس العامل المشترك الاصغر بين كل رقمين ضمن المفتاح. واثبتت نجاحها بنسبة اكثر من ٦٠٪

الاستنتاجات

١. تعد حركات التشكيل العربية من انسب المصادر لتوليد مفاتيح التشفير العشوائية وتستخدم كمفتاح في تشفير الرسائل السرية (بأية لغة كانت) وكذلك تشفير الصور السرية.
٢. سرية مفتاح التشفير تعتمد وبشكل رئيسي على اختيار النص العربي المشكل بين الطريفين (المرسل والمستلم) وعلى كثافة ترددات الحركات العربية بداخله.
٣. ان اختيار المفتاح الثانوي يعتمد على اختيار كلا الطرفين له (اي يمكن اختيار ترددات اي حركة تشكل عربية عدا الحركة ذات التردد الاعلى(حركة المفتاح الاولي).

المصادر

[1] «الأمن المعلوماتي لأنظمة المعلومات»، متوفر على الموقع الالكتروني:
. DOC.١~٤٥D٠/www.ao-academy.org/docs

[2] « التعريف بتقنيات التشفير وأمنية المعلومات» متوفر على الموقع الالكتروني:
doc.٧٧٧/www.profawad.info

[3] استبرق عبد الرضا كاظم، هالة بهجت عبد الوهاب، سهاد مال الله كاظم، « تضمين رسالة سرية داخل نص عربي مشكل « ، المؤتمر الدولي الثالث للغة العربية ، دولة الامارات ، ٢٠١٤

[4] حيدر محمد عبدالنبي، رعد عبد الحسن مهجر و نهلة عباس فليح ، « تشفير الملفات النصية باستعمال المفتاح المتناظر ومفتاح مستنبط من معلومات النص الصريح»، جامعة البصرة/كلية العلوم/قسم الحاسبات / ٢٠٠٦

[5] د.نبيل علي، «اللغة العربية والحاسوب دراسة بحثية»، تعريب للنشر/الكويت ١٩٨٨م.

[6] "علم التشفير او التعمية» ، متوفر على الموقع الالكتروني :
http://faculty.ksu.edu.sa/ghathbar/Information%٢٠Security%٢٠Articls/%D٨%B٩%D٩%٨٤%D٩%٨٥%٢٠%D٨%A٧%D٩%٨٤%D٨%AA%D٨%B٤%D٩%٨١%D٩%٨A%D٨%B١%٢٠%D٨%A٧%D٩%٨٨%٢٠%D٨%A٧%D٩%٨٤%D٨%AA%D٨%B٩%D٩%٨٥%D٩%٨A%D٨%A٩ .pdf

[7] Adnan. Gutub, Lahouari M. Ghouti, Yousef S.Elarian, Sameh M. Awaideh, Aleem K. Alvi," Utilizing Diacritic Marks for Arabic Text Steganography", Kuwait Journal of Science & Engineering