تشفير الملفات النصية باستعمال المفتاح المتناظر ومفتاح مستنبط من معلومات النص الصريح

حيدر محمد عبدالنبي، رعد عبد الحسن مهجر و نهلة عباس فليح

جامعة البصرة/كلية العلوم/قسم الحاسبات

ISSN –1817 –2695
الاستلام 2006/3/22, القبول 2006/10/5

المستخلص:

علم التشفير Cryptograph أحد المجالات المهمة والمعقدة في الوقت نفسه ، وقد ازداد الطلب على تقنيات التشفير مع انتشار الانترنت قبل أكثر من عشر سنوات بسبب الحاجة لنقل المعلومات السرية والخاصة على شبكة عمومية يسهل اعتراض المعلومات فيها والتجسس على اتصالاتها. وبالنظر لأهمية هذا الموضوع تطرقنا في هذا البحث إلى خوارزمية اقترحت لتشفير الملفات ذات النوع النصي Text File إن الخوارزمية المقترحة من خوارزميات التشفير بالمفتاح المتناظر، ارتكزت الخوارزمية المقترحة في عملها على توليد شفرة مختلفة لكل رمز في النص ، حتى في حالة تكرار الرمز نفسه فلا يشفر بالشفرة نفسها وبذلك يكون من الصعب كسر الشفرة الناتجة من عملية التشفير بدون معرفة الخطوات الدقيقة للخوارزمية. تستخدم الخوارزمية المقترحة مفتاح متناظر ذا طول 128 بت وتستخدم دالة Xor لإتمام عملية التشفير. بالإضافة إلى مفتاح أخر يتغير بتغير كل سطر في النص يتم استنباطه من معلومات نص الرسالة.

الكلمات المفاتيح

علم التشفيرCryptograph ، النص الصريحPlain text ، النص المشفرCipher text ، التشفير بالمفتاح المتناظر Symmetric key encryption ، التشفير بالمفتاح غير المتناظرAsymmetric key encryption.

(1) المقدمة

التشفير(cryptography): هو عملية الحفاظ على سرية المعلومات باستعمال طرائق أو خوارزميات لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز بحيث إذا ما وصل إليها من قبل أشخاص غير مخولين بذلك لا يستطيعون فهم أي شيء لأن ما يظهر لهم هو خليط من الرموز والأرقام و الحروف الغير مفهومة, ومن ثم نقلها عبر وسائل نقل المعلومات العامة إلى الجهة المرسل إليها ومن ثم إعادة صياغتها إلى صورتها المفهومة مرة أخرى[4] .

(2)أهداف نظام التشفير :

التشفير يهدف إلى تحقيق الأهداف التالية[1,2]:

1. السرية (Security) : هي عملية حفظ المعلومات أو البيانات وجعلها سرية بحيث لا يكون متعارف عليها أي تكون غير مفهومة بالنسبة للآخرين .
2. الصلاحية (Authentication) : معرفة إن الرسالة مرسلة في الوقت المناسب ومن الشخص المناسب وبدون تدخل ، لذلك يضاف مع الرسالة التوقيع و الوقت لغرض تثبيت صلاحية الرسالة .
3. التكاملية (Integration) : التأكد من إن الرسالة غير محذوف منها شيْ أو مضاف لها شيْ .
4. عدم التنكر (Non_repudiation) : هي الخدمة التي تمنع الشخص من إنكار الرسالة المرسلة أي الرسالة المنقولة .

(3)مكونات نظام التشفير:

إن نظام التشفير يتكون من الأجزاء التالية[5]:

1. النص الصريح (plaintext): ويرمز له بالرمز (M)، وهو النص المراد تشفيره.
2. النص المشفر (Ciphertext): ويرمز له بالرمز (C)، وهو النص المراد فتح الشفرة له.
3. المفتاح (Key) : ويرمز له بالرمز (K)،وهو المفتاح المستخدم في تشفير وفك الشفرة للنص.

4. خوارزمية التشفير(Encryption): ويرمز لها بالرمز(Ek)، وهي الخوارزمية المستخدمة لتحويل النص الصريح إلى نص مشفر ويمكن توضيحه بالعلاقة التالية:

$$Ek: M \longrightarrow C$$

5. خوارزمية فك الشفرة (Decryption): ويرمز لها بالرمز(Dk)، وهي الخوارزمية المستخدمة لتحويل النص المشفر إلى نص صريح ويمكن توضيحه بالعلاقة التالية:

$$Dk: C \longrightarrow M$$

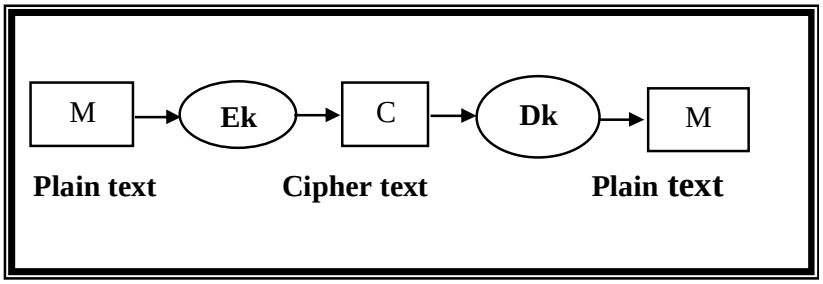
كما في الشكل(1) .

(4) أنواع نظم التشفير :

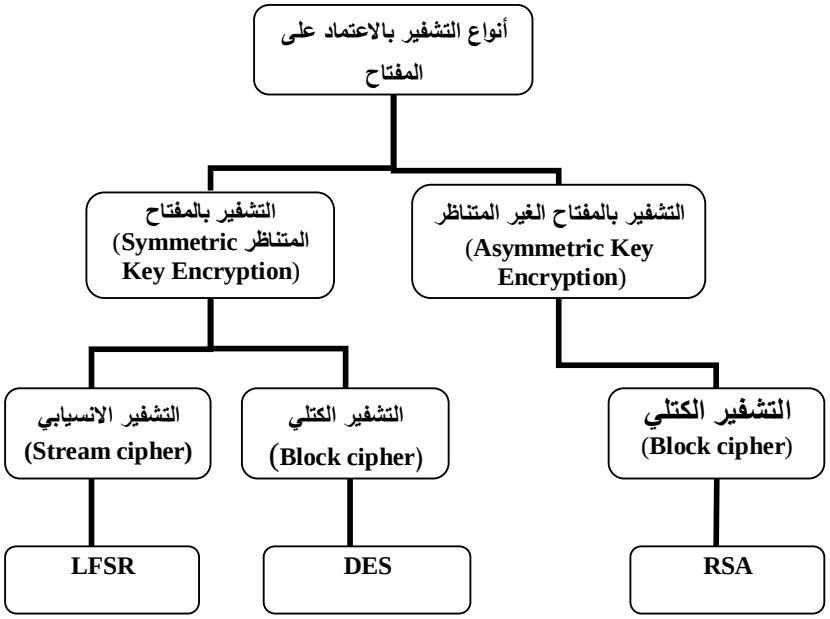
يقسم نظام التشفير اعتمادا على المفتاح إلى نوعين هما :

1-التشفير بالمفتاح المتناظر (Symmetric Key Encryption) :
هو أسلوب من أساليب التشفير يستعمل فيه مفتاح سري لتشفير رسالة ما وفك تشفيرها، ويسمى التشفير بالمفتاح المتناظر لأن المفتاح الذي يستعمل لتشفير الرسالة هو نفسه المستعمل لفك تشفيرها[6] ويقسم على نوعين:

أ- التشفير الكتلي (Block ciphers) : يعد التشفير الكتلي احد أنواع التشفير الحديثة بالإضافة الى التشفير الانسيابي . في هذا النوع، يقسم النص الصريح الى كتل بأحجام متساوية، ومن ثم تطبق خوارزمية التشفير على كل كتلة ويحولها الى كتلة أخرى مشفرة [6] . وكما موضح في الإشكال (2) و (3).



شكل 1 : مكونات نظام التشفير



شكل 2: انواع التشفير بالاعتماد على المفتاح

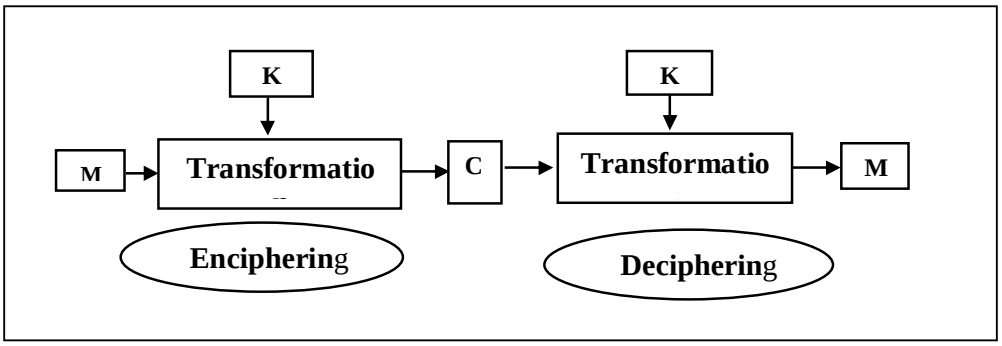
ب- التشفير الانسيابي(stream ciphers) : أنظمة التشفير الانسيابي تقسم النص الصريح (M) إلى ثنائيات (bit by bit) أو رموز متتابعةكما في الشكل (4) ، وتقوم بتشفير كل m_i باستخدام العنصر ki من سلسلة المفتاح $K=k_1,k_2,k_3,\ldots$ أي إن :

$$Ek\ (M) = Ek\ (m_1)\ Ek\ (m_2)\ Ek\ (m_3)\ldots.$$

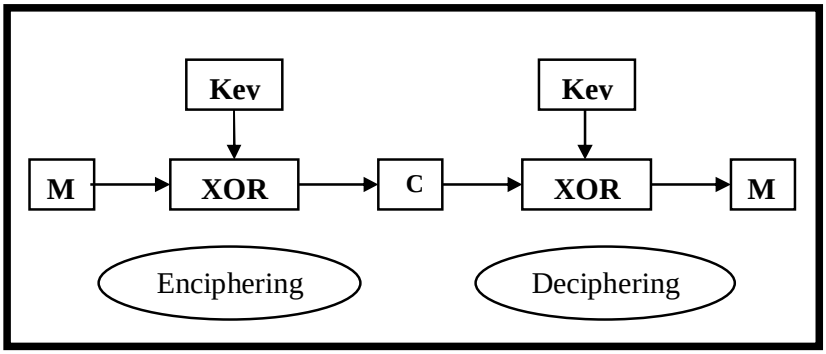
يتكون نظام التشفير الانسيابي من جزأين أساسين هما:

أ- خوارزمية توليد سلسلة المفتاح(سلسلة شبه عشوائية).
ب-المازج (MIXER).

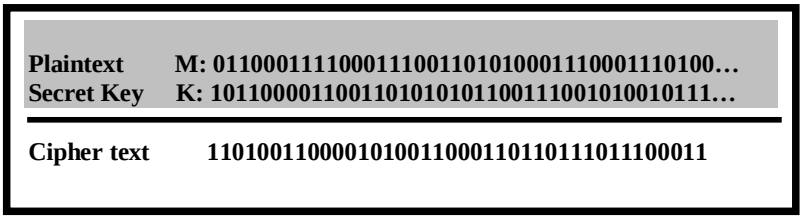
ج
تقوم الخوارزمية بتوليد سلسلة المفتاح اعتمادا على مفتاح يغذيها ، ثم تمزج السلسلة المتولدة مع النص الصريح بوساطة المازج لتوليد النص المشفر . يكون المازج عادة هو عملية (XOR) [3,7] ، كما موضحه بالشكل (5).



شكل 3: التشفير الكتلي



شكل 4: التشفير الانسيابي



شكل 5: عملية XOR

2- التشفير بالمفتاح الغير متناظر (Asymmetric key encryption):
هو أسلوب من أساليب التشفير يتم فيه تشفير البيانات باستعمال مفتاح ما، وفك تشفيرها باستعمال مفتاح آخر، ولهذا السبب سمي بالتشفير الغير متناظر، لأن مفتاح التشفير يختلف عن مفتاح فك التشفير، ومن ثم فإنه يسمح بتوزيع صلاحيات التشفير وفك التشفير على الجهات المختلفة بأن يعطي لبعضهم مفاتيح التشفير فقط ويعطي للآخرين مفاتيح فك التشفير .ويسمى هذا النوع من التشفير أيضا التشفير بالمفتاح العام (Public-key encryption)، لأنك تستطيع أن تنشر أحد المفتاحين وهو يسمى المفتاح العام (public-key)، وتحتفظ بالآخر سريا، ويسمى المفتاح الخاص (private-key)[6].

(5) الخوارزمية المقترحة

(5-1)عملية التشفير :

يتم التشفير في هذه الخوارزمية بأتباع الخطوات التالية:
1. اقتطاع سطر من ملف النص الصريح (Plain text)
2. إضافة مفتاحين للتشفير طول كل مفتاح 128 بت لزيادة أمنية الرسالة المراد إرسالها .
3. حساب معامل التشفير(المفتاح) كالتالي

Factor = charposition * line length

المفتاح= موقع الرمز *طول السطر
4. اقتطاع رمز(char) من السطر
5. تحويل الرمز المستقطع الى شفرة الاسكي
6. تشفير الرمز المستقطع للحصول على الرمز المشفر (B) بإدخال الرمز في دوارة وتجرى عليه العملية التالية:

B= char Xor key

7. تشفير الرقم الناتج من الخطوة السابقة حسب المعادلة:

C=B Xor Factor

8. تجميع الرموز المشفرة بشكل سطر.
9. إضافة السطر المشفر الى الملف الجديد (ملف التشفير).
10. تستمر هذه العملية لحين انتهاء النص الصريح (Plaintext)

(5-2)عملية فك الشفرة :

تتم عملية فك الشفرة بأتباع الخطوات التالية :
1. اقتطاع رمز من النص المشفر(cipher text) .
2. حساب معامل التشفير (المفتاح) كالتالي:

أ- حساب طول السطر .

ب- حساب موقع الرمز.

3. فك شفرة الرموز المستقطعة للحصول على الرمز المشفر (B) بإدخال الرموز في دوارة وتجرى عليها العملية التالية:

B= char Xor Factor

حيث key هو نفس المفاتيح في عملية التشفير.
4. فك شفرة الرموز الناتجة حسب المعادلة التالية:

D=B Xor Key

5.تجميع الرموز على شكل سطر
6. إضافة السطر الى الملف الجديد (الملف الناتج بعد عملية التشفير والذي يكافيء ملف النص الصريح Plain text).
7.تستمر العملية الى نهاية الملف المشفر.

(6) تحليل الأمنية ونتائج الاختبارات:

بالمقارنة مع طرائق التشفير بالمفتاح المتناظر الأخرى ، الطريقة المقترحة ذات أمنية عالية ويمكن أن تقاوم كل أنواع الهجمات المعروفة مثل

Known plain text attack, cipher text only attack, ..etc.

تم شرح بعض نتائج تحليل الأمنية على هذه الطريقة وهذه الاختبارات تتضمن اختبار مجال المفتاح ، وغيرها وكالتالي:

(6-1) اختبار حجم المفتاح:

مجال المفتاح يجب أن يكون كبير كفاية لجعل Brute-Force attack غير ممكن. الاختبارات الأساسية ونتائجها كما يلي:

- حجم المفتاح: إذا كان حجم المفتاح كبير فهذا معناه أمنية كبيرة لكن ربما يبطئ من سرعة عملية التشفير وفك الشفرة. حجم المفتاح المستعمل في الطريقة المقترحة هو 128 بت لذلك تكون أمنية هذه الخوارزمية كبيرة.
- اختبار حساسية المفاتيح: تم استعمال 16 رمز كمفتاح تشفير. وهذا يعني أن المفتاح يتكون من 128 بت.

اختبار حساسية المفتاح النموذجي تمت على أساس الخطوات التالية:

1. تم تشفير النص الصريح باستعمال مفتاح الاختبار التالي "1234567890123456" . وكانت نتيجة التشفير كما يلي:

النص الصريح:

Cryptography: is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

النص المشفر باستخدام المفتاح "1234567890123456":

106 248 141 278 265 442 625 515 730 653 803 950 949 1114 1106 1186 1391 1322 1475
1434 1631 1788 1778 1877 1807 1995 2163 2111 2292 2182 2385 2531 2494 2622 2574
2775 2713 2855 3046 2951 3143 3099 3242 3426 3387 3523 3538 3616 3813 3838 3931
3858 4047 4218 4129 4230 4239 4438 4598 4598 4713 4615 4754 4924 4915 5110 5010
5207 5128 5289 5501 5394 5594 5511 5680 5845
96 245 143 350 260 421 555 551 721 641 843 1004 940 1084 1103 1231 1161 1321 1509
1469 1604 1536 1749 1895 1909 2041 1947 2131 2077 2284 2367 2335 2521 2457 2603
2795 2744 2896 2821 3035 3169 3105 3321 3212 3398 3359 3555 3685 3644 3712 3743
3929 4084 4007 4155 4119 4289 4241 4413 4583 4538 4681 4608 4838 4963 4927 5070
5022 5200 5353 5305 5489 5379 5574 5526
2 60 23 199 160 155 323 319 264 460 429 406 592 575 529 646 674 667 895 807 774
1013 992 919 1128 1059 1036 1214 1184 1156 1393 1382 1344 1532 1495 1415 1632
1627 1539 1791 1736 1676

2. ثم تم تشفير النص الصريح باستعمال نفس المفتاح مع تغيير الخانة الأقل أهمية أي "1234567890123457" .

النص المشفر باستعمال المفتاح: "1234567890123457":

107 249 140 279 264 443 624 514 731 652 802 951 948 1115 1107 1187 1390 1323 1474
1435 1630 1789 1779 1876 1806 1994 2162 2110 2293 2183 2384 2530 2495 2623 2575
2774 2712 2854 3047 2950 3142 3098 3243 3427 3386 3522 3539 3617 3812 3839 3930
3859 4046 4219 4128 4231 4238 4439 4599 4599 4712 4614 4755 4925 4914 5111 5011
5206 5129 5288 5500 5395 5595 5510 5681 5844
97 244 142 351 261 420 554 550 720 640 842 1005 941 1085 1102 1230 1160 1320 1508
1468 1605 1537 1748 1894 1908 2040 1946 2130 2076 2285 2366 2334 2520 2456 2602
2794 2745 2897 2820 3034 3168 3104 3320 3213 3399 3358 3554 3684 3645 3713 3742
3928 4085 4006 4154 4118 4288 4240 4412 4582 4539 4680 4609 4839 4962 4926 5071
5023 5201 5352 5304 5488 5378 5575 5527
3 61 22 198 161 154 322 318 265 461 428 407 593 574 528 647 675 666 894 806 775
1012 993 918 1129 1058 1037 1215 1185 1157 1392 1383 1345 1533 1494 1414 1633
1626 1538 1790 1737 1677

3. ونلاحظ من المثال السابق أن النص المشفر المتولد باستعمال المفتاح الأول يختلف عن النص المشفر المتولد من المفتاح الثاني بنسبة كبيرة جدا".

أما بالنسبة لعدد الجولات (No. Of Rounds) : الخوارزميات التي تنفذ باستعمال جولة واحدة تكون أمنيتها غير جيدة، لكن عندما تكون هناك عدة جولات فهذا سيزيد من أمنية الخوارزمية المقترحة وهنا تم اعتماد 16 جولة للمفتاح.

(7) المناقشة والنتائج :

تعد هذه الخوارزمية ذات أمنية جيدة بسب ان الرمز الأصلي سوف يشفر على مرحلتين :
المرحلة الأولى بجمع الملف الأصلي مع قيمة المفتاح بتطبيق دالة Xor والمرحلة الثانية بتطبيق دالة Xor بين قيمة الرمز الجديد من المرحلة الأولى وقيمة المفتاح الناتج من الـ Factor .

كما إن الخوارزمية المقترحة سريعة التنفيذ في عملية التشفير وفك الشفرة. والمثال التالي يمثل نص صريح تم تشفيره باستخدام الخوارزمية المقترحة(تم برمجة هذه الخوارزمية باستخدام لغة Visual Basic):

مثال على تشفير الخوارزمية المقترحة باستعمال كلمة السر "HELLOAbCdEf2006" والنص الصريح أدناه علما" أن حجم النص الصريح 834 بايت فقط :

((*علم التشفير Cryptograph أحد المجالات المهمة والمعقدة في الوقت نفسه ، وقد ازداد الطلب على تقنيات التشفير مع انتشار الانترنت قبل أكثر من عشر سنوات بسبب الحاجة لنقل المعلومات السرية والخاصة على شبكة عمومية يسهل اعتراض المعلومات فيها والتجسس على اتصالاتها. وبالنظر لأهمية هذا الموضوع تطرقنا في هذا البحث إلى خوارزمية جديدة اقترحت لتشفير الملفات ذات النوع النصي Text File إن الخوارزمية المقترحة من خوارزميات التشفير بالمفتاح المتناظر، ارتكزت الخوارزمية المقترحة في عملها على توليد شفرة مختلفة لكل رمز في النص ، حتى في حالة تكرار الرمز نفسه فلا يشفر بالشفرة نفسها وبذلك يكون من الصعب كسر الشفرة الناتجة من عملية التشفير بدون معرفة الخطوات الدقيقة للخوارزمية. تستخدم الخوارزمية المقترحة مفتاح متناظر ذا طول 128 بت وتستخدم دالة Xor لإتمام عملية التشفير. بالإضافة إلى مفتاح أخر يتغير بتغير كل سطر في النص يتم استنباطه من معلومات نص الرسالة.*))

النص المشفر أدناه علما" أن حجم النص الناتج بعد عملية التشفير 5718 بايت وهو تقريبا" يساوي 1: 6 من حجم النص الصريح وذلك بسبب تحول الرموز إلى أرقام تم إضافة رمز "*" للتفريق بين رمز مشفر وأخر:

The cipher text is :

12309*11639*10938*10002*9026*8208*7428*6788*5699*4880*4275*3464*2413*1541*81122382*21506*20988*20134*19074*18210*17540*16751*15727*14870*14308*13486*33412*32323*31525*30901*30063*29025*28166*27622*26728*25649*24931*24250*23510*43422*42412*41491*40932*40040*38949*38248*37537*36626*35707*34856*34052*54219*53401*52438*51549*50874*50153*48971*48148*47364*46731*45672*44826*44173*64080*63479*62279*61481*60676*60064*59007*58123*57511*56706*55724*54799*74776*74185*73362*72332*71649*70824*70024*68973*68105*67539*66703*65579*64889*84770*84032*83349*82287*81453*80872*80001*79062*78199*77457*76792*75634*95563*94765*94156*93288*92334*91615*90626*89874*88903*88064*87534*86688*85605*104826*104016*103380*102252*101398*100846*99981*98925*98082*97344*96640*114147*113251*112250*111399*110721*109935*108989*108286*107325*106600*105534*123266*122284*121580*120806*119938*118802*118135*117417*116707*115590*114709*132117*131438*130746*130019*128875*128012*127236*126624*125567*124683*124071*141323*140738*139908*138867*138003*137347*136610*135493*134892*134082*133289*150606*149871*148806*147999*147407*146566*145465*144723*143952*143349*142151*159848*158743*158033*157374*156628*155489*154644*154102*153248*152143*151304*168768*167938*167406*166499*165477*164640*164015*163217*162145*161298*160716*178145*177283*176533*175453*174609*174028*173160*172081*171345*170686*169962***

*187364*186498*185378*184685*183965*183267*182150*181261*180715*179877*178758
*196370*195397*194593*193796*193177*192065*191264*190605*189830*188844*187915
*205439*204560*203945*203119*202059*201261*200673*199823*198716*198012*197305
*214553*213983*213120*212182*211311*210595*209891*208774*207874*207301*206487
*223824*223199*222073*221219*220608*219747*218689*217893*217152*216456*215405
*233127*232063*231186*230533*229768*228780*227882*227277*226456*225303*224623
*242001*241181*240421*239744*238641*237905*237220*236527*235383*234508*233732
*251220*250541*249825*248643*248037*247289*246434*245349*244705*243853*243099
*260603*259730*258661*257808*257088*256392*255341*254493*253926*253082*252118
*269731*268716*267793*267240*266344*265275*264567*263825*263163*262022*261135
*278555*277904*277175*276435*275266*274448*273668*273122*272002*271116*270506
*287756*286980*286370*285309*284448*283712*283038*281967*281118*280357*279701
*297024*296347*295249*294429*293836*292968*291861*291198*290490*289747*288635
*306319*305366*304490*303761*303070*301958*301071*300482*299682*298575*297742
*315255*314376*313837*312931*311935*311084*310336*309653*308591*307757*307168
*324368*323762*322988*321889*321029*320293*319631*318487*317779*317102*316408
*333780*332930*331817*331106*330426*329490*328545*327716*327146*326309*325221
*343029*341831*341030*340462*339623*338533*337688*337073*336366*335276*334347
*351859*351201*350376*349576*348525*347695*347096*346242*345137*344445*343632
*361007*360424*359567*358460*357776*357047*356307*355180*354321*353785*352942
*370365*369659*368518*367654*367040*366179*365164*364327*363687*362910*361822
*379537*378433*377644*377001*376175*375115*374317*373734*372886*371772*371041
*388585*387820*387008*386220*385238*384375*383633*382972*381760*380930*380405
*397669*396957*396050*395250*394400*393564*392759*391810*391047*390153*389411
*407022*406115*405093*404256*403588*402857*401750*401132*400322*399529*398354
*416111*415051*414253*413670*412841*411691*410999*410298*409362*408438*407554
*425020*424289*423613*422904*421766*420900*420334*419479*418431*417580*416945
*434216*433645*432739*431726*430862*430221*429440*428357*427756*426946*426134
*443456*442762*441709*440864*440101*439430*438288*437623*436897*436192*435013
*452773*451798*450901*450208*449525*448390*447490*446917*446091*445039*444170
*461632*460831*460036*459401*458362*457488*456894*456107*454987*454380*453592
*470792*470080*469418*468316*467467*466725*466063*464919*464211*463510*462820
*480194*479401*478226*477545*476833*475922*474951*474118*473537*472736*471631
*489447*488289*487460*486883*486025*484935*484102*483406*482671*481642*480772
*498280*497421*496819*496028*495020*494102*493540*492708*491734*490871*490170

***507403*506831*505960*504875*504157*503445*502773*501638*500771*500195*499362**
***516769*516085*514928*514277*513507*512674*511553*510747*510081*509353*508271**
***525998*524907*524257*523405*522652*521577*520749*519973*519311*518188*517498**
***534880*534252*533457*532608*531497*530809*530000*529384*528197*527395*526791**
***544144*543382*542709*541511*540683*540131*539286*538219*537569*536762*535982**
***553410*552608*551525*550667*549952*549256*548205*547359*546772*545957*544831**
***562543*561517*560680*560091*559273*558294*557431*556689*555985*554876*554020**
***571454*570723*570040*569338*568198*567298*566725*565902*564837*563981*563369**
***580837*580094*579223*578163*577505*576691*575915*574826*573963*573391*572520**
***590014*589191*588141*587500*586694*585879*584765*584033*583248*582609*581442**
***599193*598230*597367*596625*595957*594754*593935*593397*592551*591464*590817**
***608075*607252*606468*605856*604792*604129*603303*602539*601414*600600*600002**
***617247*616580*615842*614731*613894*613157*612495*611351*610682*609956*609263**
***626626*625833*624686*623953*623288*622354*621436*620580*619976*619107*618088**
***635666*634688*633883*633323*632419*631397*630547*629935*629128*628035*627436**
***644675*643879*643262*642437*641452*640552*639960*639131*637971*637328*636625**
***653869*653286*652434*651304*650623*649913*648978*648059*647208*646404*645764**
***663226*662290*661345*660516*659911*659110*657985*657160*656448*655785*654667**
***672384*671343*670478*669760*669064*668013*667183*666569*665743*664599*663927**
***681470*680629*679797*678972*678041*677335*676354*675667*674774*673965*673028**
***690515*689744*689141*687943*687119*686576*685726*684623*683792*683072*682252**
***692370*691223**

(8) الاستنتاجات

ان الخوارزمية المقترحة ذات كفاءة جيدة في التشفير، كما تم توضيحه في المناقشة والنتائج ولكن ملف النص الصريح يكون اصغر من ملف النص المشفر أي لو كان الملف حجمه مثلا" 834 بايت فيصبح حجمه بعد تشفيره 5718 بايت وهذا معناه أن حجم ملف النص الصريح أصغر من حجم الملف المشفر بمقدار 6:1 تقريباً" وهذه ملاحظة مهمة لهذا النظام حيث أن الرموز تتحول إلى أرقام أما من ناحية السرعة فالخوارزمية كفوءة ويمكن الاعتماد عليها من هذه الناحية لان المعالجة المطلوبة للنصوص المراد تشفيرها تتمثل بعملية Xor فقط .

المصادر

1. A. Menezes, P. Vanoorschot, and S. Vanstone,
"Hand book of applied cryptography", CRC Press, Inc, 1996 .

2. Beker H. And Piper F.

"Cipher systems", the Protection and Communications
London :Northward, Book, 1982.

3.Siegenthaler, T.
"Decrypting a class of stream ciphers using cipher text
only". IEEE Transition on computers, PP.18-85, 1985

4.Dorothy E. and Robling D.
"Cryptography and Data Security", Purudue University, 1988.

5.Schneier, B.,
" Applied Cryptography", John Wiley & Son , 1996.

6. Simons, G.J.
" Symmetric and Asymmetric Encryption ", Computing
Surveys Vol.11(4), PP.305-330, Dec. 1979.

7. William Stallings,
"Cryptography and network security principles and practices third edition", Person education , Inc, 2003.

Encryption of Text Files Using Symmetric Key and a Key Deducted from the Plain Text Information

Haider M. Abdul-Nabi, Ra'ad A. Mhajar And Nahla A. Flaeeh
Basrah University, College of Science, Dep.of Computer Sciences

Abstract

Cryptograph is one of the most important and at the same time of complicated field of analysis, The wide use of internet over the last ten years give the reason of increasing requirement of cryptograph techniques for save the security of transmit information in global network.

The proposed algorithm in this paper offers a strong protection for encoding text files, For the importance of this subject, we proposed in this research a new algorithm for encoding text file. The new algorithm is a Symmetric key encryption algorithm , this algorithm depending on generate a different code for all symbol on the text . In the case of symbol repetition the code will be different, for this reason the result is difficult to attack without Knowing the algorithm.

The suggested algorithm using variable key for every symbol in the text and using XOR function to complete the coding, the length of key is changing from one line to other.