تصميم تشفير انسيابي لتوليد المفاتيح الجزئية لإخفاء رسالة اجهزة الجوال (SMS) النصية داخل رسالة الوسائط المتعددة (MMS) الصوتية

يحيى نجار[1] ، محمود شعار[1]، إقبال عرب[1] ، مشاري بن عايد بن عسكر الشمري[2]

[1] قسم هندسة الحواسيب ، كلية الهندسة الكهربائية والإلكترونية ، جامعة حلب ، حلب ، سوريا

[2] طالب دراسات عليا (دكتوراه)

الملخص

تستخدم رسائل أجهزة الجوال (SMS) النصية بشكل واسع في مجال الحياة العملية والتي ترسل من خلال أجهزة الجوال عبر شبكة الاتصالات، وتكون كلاً من الرسائل المرسلة عبر شبكة الاتصالات والمخزنة داخل أجهزة الجوال مهدده من قبل المهاجمين أو المتطفلين. إن أجهزة الجوال تتطور بشكل كبير حسب حاجة المستخدم ، بينما حماية (الرسائل أو المعلومات) تتم بمجرد قفل الجوال بمفتاح خاص و إن هذا المفتاح يمكن فتحه عن طريق برامج الفتح الموجودة في أجهزة الحاسوب ، لذلك فإن هذه الرسائل بحاجة إلى تصميم نظام برمجي لحمايتها . الغاية من هذا البحث هو بناء خوارزمية لإخفاء رسالة أجهزة الجوال (SMS) النصية داخل رسالة الوسائط المتعددة (MMS) الصوتية بسرية عالية جداً وذلك من خلال تصميم نظام تشفير أنسيابي (stream cipher) لتوليد سلسلة المفاتيح الشفر ية لتلك الخوارزمية .إن هذا التصميم يتكون من ثلاثة مسجلات إزاحة مختلفة الأطوال ،حيث يتم توليد سلسلة من الأصفار والواحدات إن هذه السلسلة الناتجة هي مصفوفة المفاتيح الجزئية التي من خلالها يتم اختيار مواقع البايتات من رسالة الوسائط المتعددة (MMS) الصوتية بسرية عالية جداً يصعب على العدو معرفة تلك المواقع . لتحقيق ذلك تم استخدام البتات الأقل أهميه (LSB) وباستخدام مفتاح سري مكون من 21 بايت (168bits) . وبالتالي فإن عدد الاحتمالات التي يمكن أن تأخذها الحالة الابتدائية لتغذية المسجلات هو (2^{168}-1) احتمال ، وتم تنفيذ هذه الخوارزمية على أجهزة جوال من نوع HTC .

الكلمات المفتاحية : رسائل والوسائط المتعددة ، خدمة الرسائل القصيرة ، البتات الأقل أهمية .

المقدمة

لقد تطورت تقنيات أجهزة الجوال ودخلت في مختلف مجالات الحياة العملية (عمل الأشخاص أو الشركات أو البنوك بالإضافة إلى كافة مؤسسات الدولة) وهذا التطور السريع أدى إلى استخدام أجهزة الجوال كثيراً في أنحاء العالم ليقضوا أعمالهم وذلك من خلال إرسال رسائلهم SMS النصية عبر شبكة الاتصالات أو الأنترنت مما جعل الأعداء أو المتطفلين يريدون معرفة تلك الرسائل والتلاعب بها وتدميرها في بعض الأحيان ، ولا يقتصر عمل الأعداء على الرسائل (SMS) المرسلة عبر شبكة الاتصالات بل على الرسائلالمخز نة داخل أجهزة الجوال سواء الدخول اليدوي على هذه الرسائل (SMS) أو الدخول البرمجي و الذي يحدث عند صيانة أجهزة الجوال من خلال جهاز الحاسوب فيقوم المتطفلون بنسخ هذه الرسائل المخزونه داخل ذاكرة الجوال ، وتكون هذه الرسائل نصية أو صورية أو فيديوية أوصوتية وبالتالي يقوم الأعداء بمساومة أصحاب تلك الرسائلوا لا سوف ينشرونها ، إضافةً إلىالأسماء وأرقامها السرية المخز نة ضمن قائمة الأسماء داخل أجهزة الجوال ومن خلال أهمية الرسائل (SMS) النصية المرسلة عبر شبكة الاتصالات أوالمخزنة داخل أجهزة الجو ال ومن هنا توجه اهتمامنا نحو بناء وتنفيذ خوارزمية لإخفاء رسالة أجهزة الجوال (SMS) النصية داخل رسالة الوسائط المتعددة (MMS) الصوتيةيمكن تطبيقها عملياً في الشركات أو مؤسسات الدولة بكافة أنواعها بالإضافة إلى الأشخاص . حيث قام كلاً من الباحثين Liu Ying ,Huang Dinglong ,Zhu Haiyi, patrick Rau [1]ض2 عام 2008 بدراسة أمن معلومات الجوال ،و الرسائل الأقتحامية المزعجة والبرامج التي تقوم بسرقة البيانات وعلى سبيل المثال منها(Leavitt، 2005) (Leem& Kim 2005) وبأي صيغة كانت مثل الصور أو الرسائل النصية أو غيرها من البيانات المخز نة في أجهزة الجوال والتي يتم استلامها عبر البلوتوث ، هذا واضافة الى المخاطر الناجمة عند فقدان أجهزة الجوال التي تمتلك رسائل شخصية أو غيرها من البيانات [1] . كما قام كذلك كلاً من الباحثان A Tom Kary , Wayne Jansen في المعهد الوطني للمعايير والتكنلوجيا (الصين) بقسم أمن الحاسوب بدراسة أمن أجهزة الجوال وتقليل الحمل على شبكة الاتصالات بدون أن يعمل تطبيق أو بناء خوارزمية لحماية رسائل أجهزة الجوال [2] .وقامت دائرة الأمن في حكومة منطقة هونك كونك بنشر مقالة علمية في فبراير عام 2008 حول أمن رسائل (SMS) النصية وأكدت هذه المقالة بأن الرسائل (SMS) النصية أثناء إرسالها يتم نسخ تلك الرسالة من خلال برامج التجسس مثل FlexiSpy7 الذي يقوم بنسخ كل الرسائل (SMS) النصية الواردة والصادرة، وأكدوا على أن الأمن وحماية الرسائل (SMS) النصية لم يكن متطوراً وذلك لصعوبة التنفيذ من الناحية العملية ، فقدموا دراسة فقط بدون تطبيق ، إضافة إلى تحذير منتسبيهم حول فقدان أجهزة الجو ال لما تحتوي من معلومات مهمة [3] .

أهمية البحث

تعد رسائل أجهزة الجوال (SMS) النصية من أهم الخدمات التي تقدمها شركات الاتصالات ، وذلك كونها قصيرة وذات كلفة قليلة ،

ومع تزايد استخدام أجهزة الجوال بشكل واسع في العالم مما انعكس ذلك على استخدام تلك الرسائل بشكل كبير جداً ، والسبب يعود كون أن تلك الرسائل تخدم كافة المستخدمين وكذلك الشركات ومؤسسات الدولة بكافة مستوياتها.

مما دفع المتطفلين أو الأعداء لمحاولة اختراق شبكات الاتصالات للتجسس على هذه الرسائل ومن ثم تغيير محتوياتها.و أن حماية الرسائل المخز نة أو المرسلة مهمة جداً لضمان أمن رسائل المستخدمين.

أهداف البحث

يهدف البحث إلى:

1- بناء وتنفيذ خوارزمية لإخفاء رسالة أجهزة الجوال (SMS) النصية داخل رسالة الوسائط المتعددة الصوتية (MMS) وذلك لحمايتها بسرية عالية جداً من الأعداء أو المتطفلين الذين يحاولون اختراق عملية تبادل الرسائل عبر شبكة الاتصالات والأنترنت من أجل سرقة محتوياتها .

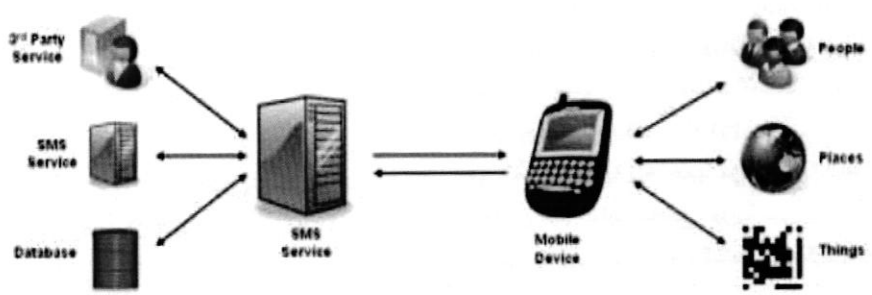
2- حماية الرسائل (SMS) النصيةالمخز نة داخل أجهزة الجوال من الأعداء الذين يراقبون فقدان أجهزة الجوال أو سرقتها لمعرفة تلك الرسائل وهذا يحدث كثيراً في الشركات والأشخاص المهمين ورجال الأعمال وحتى الأشخاص البسطاء و لا يقتصر هدفنا على الرسائل فقطوا ,نما على الأسماء وأرقامها، بل وعلى الملاحظات الشخصية والتي قد تكون رقم رصيد مالي وغيرها من المعلومات المهمة لصاحب الجوال .

3- بناء برنامج تطبيقي لمؤسسات الدولة على كافة مستوياتها بالإضافة إلى الشركات المالية (الحوالات المالية الفورية) من أجل عدم التلاعب بتلك الرسائل التي تحتوي على قيمة الحوالة المالية ،ودراسة كيفية برمجة أجهزة الجوال لتعمل على إخفاء رسالة (SMS) النصية داخل رسالة الوسائط المتعددة (MMS) الصوتية .

طريقة البحث

رسائل (SMS) النصية

هي خدمة الرسائل القصيرة (Short Messages Service) ذات الاستخدام الشائع جداً لمستخدمي الهاتف الجوال ويكون عدد الأحرف للرسالة 70 حرفاً مكتوبة باللغة العربية للصفحة الواحدة للرسالة ويمكن زيادة عدد صفحات الرسالة إلى 10صفحات وبالتالي فإن أكبر عدد من الأحرف للرسالة المكتوبة باللغة العربية هي 700 حرف ، بينما عدد الأحرف المكتوبة باللغة الإنكليزية للصفحة الواحدة للرسالة هو 160 حرفاً وبالتالي فأن أكبر عدد من الأحرف يمكن كتابته هو 1600حرف وذلك لأن الرسالة الواحدة تصل 10 صفحات [4] ، لذلك هذه الرسائل بحاجة لحمايتها من الأعداء أو المتطفلين ، وفي بحثنا هذا نقوم بإخفاء تلك الرسائل داخل رسائل وسائط متعددة (MMS) . والشكل (1) يمثل أساس نظام رسائل (SMS)[4] .



الشكل (1) أساس نظام رسائل (SMS)

رسائل (EMS)

وهي خدمة الرسائل المحسنة (Enhancement Messages Service) التي تسمح بإنشاء رسائل قصير ة تتكون من صورة بسيطة أو الحان أو رسم متحرك أو نص ذو نمط معين [4] .

مركز خدمة الرسائل القصيرة (Short Messages Service Center) وهو مسؤول عن تسليم وتوجيه الرسائل (SMS) النصية بين المرسل والمستلم، لذلك فأن المرسل عندما يرسل رسالة عندها يقوم مركز خدمة الرسائل القصيرة (SMSC) بتطبيق عدة برامج لتلك الرسالة منها تحديد مسارها أو تخزينها، بحيث يتم تخزين الرسالة مؤقتاً و من ثم ترسل إلى الجوال المقصود هذا في الحالة التي يكون فيها الجوال ضمن منطقة تغطية SMS ، وهذا مشابه لعمل رسائل البريد الإلكتروني ، وربما يتم تمرير رسائل (SMS) عبر عدد من مراكز خدمة الرسائل القصيرة (SMSC) أو بوابات خدمة الرسائل القصيرة (SMS gateways) قبل أن تصل الجوال المقصود[5,4] .

رسائل الوسائط المتعددة (Multimedia Message Service) وهي تعتبر من أكثر الأنواع تقدماً و أغلى كلفة بحيث تسمح لمستخدمي الجوال بإرسال رسالة تشمل ملفات صورية أو صوتية أو فيدوية أو نماذج بالإضافة إلى النصوص، حيث أن هذه التقنية تتوفر في الجوالات الحديثة . في هذا البحث تم استخدام خدمة رسائل الوسائط المتعددة (MMS) وذلك لأن الملفات الصوتية ترسل من الجوال عبر شبكات الاتصالات بواسطة هذه الخدمة [8,7,6] .

التشفير الانسيابي Stream Cipher

وهو من أكثر الأنظمةلتخداماً في توليد المفاتيح الجزئية لتشفير النصوص الصريحة والمكالمات الهاتفية (الصوتية) ، وأن التشفير الانسيابي مناسباً لتشفير المكالمات الهاتفية وذلك لسرعة توليد المفاتيح الجزئية وقلة الأخطاء في حال حدوثها. حيث أن التشفير الانسيابي يتكون من عدة مسجلات بالإضافة إلى دوال الربط [9] ، وفي بحثنا تم تصميم تشفير أنسيابي خاص لتوليد المفاتيح الجزئية لخوارزمية الإخفاء وفك الإخفاء .

هيكلية نظام التشفير الانسيابي

تتكون معظم أنظمة التشفير الانسيابي من مجموعة من مسجلات إزاحة ذات تغذية خلفية خطية ودوال ربط خطية ولا خطية مختلفة لتوليد متتابعات شبه عشوائية (المفاتيح) لضمان عدم انتقال خواص النص الصريح إلى النص المشفر حيث يتم فيها التشفير (بتا بعد بت) بدالة متغيرة زمنيا .

نظام التغطية (Steganography System)

يعرف نظام التغطية بأنة فن وعلم إخفاء البيانات باستخدام ملف حامل لها بهدف منع أي متطفل خارجي من الشك بوجود رسالة مخفية داخل الملف الحامل وهي وسيلة من وسائل الاتصال السري بأسلوب يخفي وجود الاتصال . أما كلمة steganogrraphy فيرجع أصلها إلى اللغة اليونانية وتتكون من المقطع stegano وتعني المغطاة والمقطع graphy أي الكتابة أو الرسم والمعنى الحرفي لها هو الكتابة المغطاة . [10]

أنواع المفاتيح

يوجد نوعان من المفاتيح هما:

1- المفتاح العام

هي الطريقة التي يتم فيها استخدام مفتاحين وان كل طرف يمتلك مفتاح عام ومفتاح خاص، حيث إن المفتاح العام يستخدم في الإخفاء ويكون معلن للجميع ، بينما المفتاح الخاص هو الذي يستخدم في فك الإخفاء [10] .

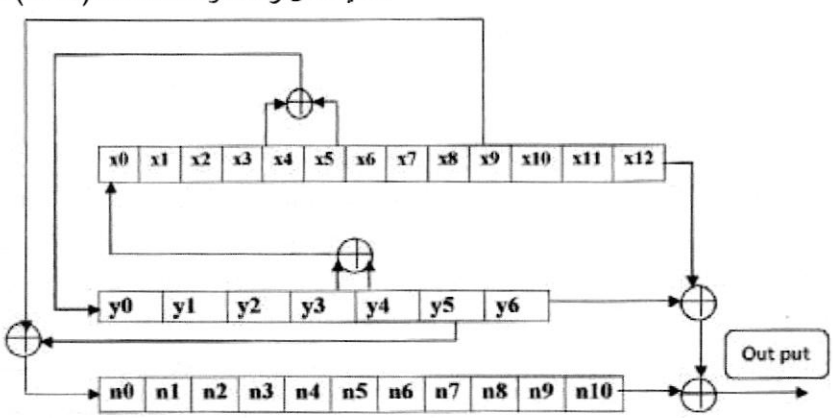
2- المفتاح السري

هو المفتاح الذي يستخدم عند إخفاء الرسالة وفك الإخفاء، وبالتالي فإن المرسل والمستلم يمتلكان نفس المفتاح ويكون سري جداً ، وفي هذا البحث تم استخدام المفتاح السري بطول 21 بايت ، ومن هذا المفتاح يتم تغذية مسجلات الأزاحة لتوليد المفاتيح الجزئية [12-10] .

الطريقه المقترحه لتوليد المفاتيح الجزئية

يتكون نظام التشفير الانسيابي المقترح لتوليد المفاتيح الجزئية من ثلاثة مسجلات ودوال الربط ، حيث أنه وفق الشكل (2) يتم تغذية المسجل y من المسجل x من خلال x4⊕x5 ، بينما المسجل x يتغذى من المسجل y من خلال y3⊕y4 ، إضافةً إلى المسجلn يتغذى من خلال المسجلين x,y كالتالي x9⊕y5 . وأن خرج التشفير الانسيابي نضعه في مصفوفة array of part keys وبالتالي فإن عدد المفاتيح الجزئية المتولدة هو $(2^{11}-1)(2^{7}-1)(2^{13}-1)$ ويساوي 2129406079 . تكون دالة الأخراج وفق التالي :

out of stream cipher=((x12⊕y6)⊕n10)) ، حيث يتم توليد سلسلة من الأصفار والواحدات بعدد مساوٍ إلى عدد بتات رسالة (SMS) النصية مضروباً بالعدد 8 أي number of out of (stream cipher=s*8) ، حيث s هي عدد بتات الرسالة (SMS) النصية وتم ضربها بالعدد 8 وذلك لتوليد بايت وثم تحويل محتويات ذلك البايت إلى رقم عشري ، وبالتالي فإن هذا الرقم هو الذي يحدد لنا مواقع البايتات من رسالة الوسائط المتعددة (MMS) الصوتية لإخفاء داخل هذه المواقع بتات رسالة (SMS)النصية ، حيث أن المسجلات في الحالة الابتدائية تأخذ قيمها من مصفوفة المفتاح السري ، والشكل (2) بين كيفية توليد المفاتيح الجزئية لخوارزمية إخفاء رسالة (SMS) النصية داخل رسالة الوسائط المتعددة (MMS) الصوتية .



الشكل(2) يبين توليد المفاتيح الجزئية

الخوارزمية المقترحه لتصميم تشفير أنسيابي لإخفاء رسالة أجهزة الجوال (SMS) النصية داخل رسالة الوسائط المتعددة (MMS) الصوتية

```
INPUT:MMS [n],SMS[m],Secret key [z] .
OUTPUT:MMS [n]has embedded SMS[m] .
i=151,sum=h=0;
 s= length of sms by bits;
For f= 0 to 20
K[a] = convert secret key[f] to binary ;
Next f
 In The beginning x0,…….x12,y0,……..y6,n0, ……
..n10= take value from K[a] ;
for p = 0 to ( s*8)
t1=x4⊕x5; t2=y3⊕y4;t3=x9⊕y5;t4=x12⊕y6; output
of stream cipher=t4⊕n10 ;
x12=x11,x11=x10,x10=x9,x9=x8,x8=x7,x7=x6,x6=x
5,x5=x4,x4=x3,x3=x2,x2=x1,x1=x0,x0=t2 ;
y6=y5,y5=y4,y4=y3,y3=y2,y2=y1,y1=y0,y0=t1 ;
n10=n9=,n9=n8,n8=n7,n7=n6,n6=n5,n5=n4,n4=n3=n
2,n2=n1,n1=n0,
n0=t3 ;
string1[b]= output of stream cipher ;
next p
Generator of part keys[j]= convert string1[b] to array
of char;
for L =0 to (length of generator of part keys[j]-1)
k1=generator of part keys [j];k2=convert k1 to
ascii;L=L+1;sum =sum +k2
next L
s1=i+sum; IF(s1>n) thenexite
else
For g = 0 to m-1
Char = SMS[g], d[u]= convert Char to binary,w=
lenth of d[u],u=0 ;
While (u =<( w-1))do
B1=d[u],u =u+1,j=0 ;
while i < n do
k1=generator of part keys[j];k2=convert k1 to ascii;i
=i+k2 ,
the first bit for byte MMS[i]=B1,j=j+1, Break
end while
end while
next g
end
d1[h]=convert s to binary v = lenth of d1[h] by
bits,h=0 ;
while (h =<(v-1)) do
i= 150, the first bit for byte MMS[i]=d1[h],i = i -
1,h=h+1
end while
if( h <50) then
begin
while i<>100 do
the first bit for byte MMS[i] =0,i=i-1end while
end if
now sms into mms and ready to send
end algorithm
```

توصيف عمل الخوارزمية المقترحه لتصميم تشفير أنسيابي لإخفاء رسالة أجهزة الجوال(SMS) النصية داخل رسالة الوسائط المتعددة (MMS) الصوتية

يتم إدخال ثلاثة مصفوفات إلى الخوارزمية : الأولى مصفوفة رسالة الوسائط المتعددة MMS[n] والثانية مصفوفة رسالة SMS[m] النصية المراد إخفاؤها والثالثة مصفوفة المفتاح السري Secret key[z] ، بينما خرج الخوارزمية مصفوفة رسالة الوسائط المتعددة MMS[m] مخفي داخلها رسالةSMS النصية. في البداية نوجد طول الرسالة المراد إخفاؤها ونضعها في المتغير s ، وبعدها نقوم بتحويل مصفوفة المفتاح السري إلى مصفوفة من العدد الثنائي (binary) ، وبالتالي فإن الحالة الأولى لقيم المسجلات يتم إدخالها من المصفوفة k[a] ، وبعدها يتم توليد سلسلة من الأصفار والواحدات نضعها في المصفوفة string1[b] ونقوم بتحويل محتويات هذه المصفوفة إلى أحرف ونضعها في مصفوفة توليد المفاتيح الجزئية generator of part keys[j] ، وبعدها نقوم بإيجاد مجموع قيم المفاتيح الجزئية المتولدة ونضعه في المتغير sum ، (في البداية i=151 لأننا نقوم بإخفاء رسالة (sms) النصية ابتدأ من البايت 151 لرسالة الوسائط المتعددة (MMS) الصوتية وبعدها نضيف قيمة sum إلى المتغير i ونضعه في المتغير s1 ،ومن خلال مصفوفة توليد المفاتيح الجزئية يتم تحديد مواقع bytes من رسالة الوسائط المتعددة MMS لنقوم بإخفاء بتات bits رسالة SMS النصيةداخل تلك المواقع المحددة من قبل مصفوفة توليد المفتاح السري ، ثم نفحص قيمة s1 أذا كانت أكبر من n وفي حال تحقق الشرط فأن الخوارزمية لاتقوم بعملية الإخفاء وذلك لأن حجم رسالة الوسائط المتعددة MMS الصوتية صغير بالنسبة لقيمة المفتاح ورسالة SMS النصية، أما في حال عدم تحقق ذلك الشرط فإن الخوارزمية تقوم بعملية الإخفاء ، حيث أن حلقة for تقوم بقراءة محتويات الرسالة SMS[g] النصية ووضعها في المتغير Char وثم تحويل هذا المتغير إلى مصفوفة ثنائية d[u] ثم نقوم بإيجاد طول المصفوفة d[u] ونضعه في المتغير w ومن خلال حلقة while نقوم بقراءة محتويات تلك المصفوفة ونأخذ كل bit ونضعه في المتغير B1 وبالتالي فأن محتويات ذلك المتغير هي المراد إخفاؤها. نقوم بقراءة محتويات الملف الصوتي من خلال الحلقة while (i<n) do وبعدها نقوم بتحويل محتويات مصفوفة توليد المفاتيح الجزئية في المتغير k1 ومن ثم تحويلها إلى ascii . وبعدها نحدد الموقع الذي نخفي داخله B1 وهو البت المراد إخفاؤه من رسالة SMS النصية ونضعه في البت الأول من البايت المحدد من خلال i=i+k2 . يتم تكرار عمل الخوارزمية إلى أن نخفي كافة بتات الرسالة SMS النصية . نقوم بتحويل محتويات المتغير s إلى عدد ثنائي ووضعه في المصفوفة d1[u] وبعدها نقوم بإخفاء هذه المصفوفة(لكي يعرف المستلم كم هو عدد البتات المخفية) في البايتات من الموقع 150 نزولاً إلى الموقع 101 وفي حال بتات المصفوفة d1[u] أقل من

ISSN:1813 – 1662

50 بت نقوم بإضافة أصفار في المواقع حتى نصل الموقع 101 ، وفي النهاية يكون خرج الخوارزمية رسالة الوسائط المتعددة SMS الصوتية مخفي داخلها رسالة SMS النصية ، والآن الرسالة جاهزة للإرسال عبر شبكة الاتصالات بأمان وكذلك الرسائل المخزنة أو الملاحظات أو الأرقام المهمة يمكن إخفاؤها وثم خزنها.

الخوارزمية المقترحة لتصميم تشفير أنسيابي لفك إخفاء رسالة SMS النصية من رسالة وسائط متعددةMMS الصوتية

INPUT : MMS[n], Secret key[z].
OUTPUT:SMS[m].
Note : i=101,b=1
For i= 101 to 150
D[g] = content the first bit for byte MMS[i]
Next i,x= convert D[g] to dec
For f= 0 to 20
K[b] = convert secret key[f] to binary;b=b+8;
Next f , In The beginning x0,…x12,y0,…y6,n0,…n10= take value from K[b]
for p = 0 to (x*8)
t1=x4⊕x5; t2=y3⊕y4;t3=x9⊕y5;t4=x12⊕y6; output of stream cipher=t4⊕n10;
x12=x11,x11=x10,x10=x9,x9=x8,x8=x7,x7=x6,x6=x5,x5=x4,x4=x3,
x3=x2,x2=x1,x1=x0,x0=t2;
y6=y5,y5=y4,y4=y3,y3=y2,y2=y1,y1=y0,y0=t1;
n10=n9=,n9=n8,n8=n7,n7=n6,n6=n5,n5=n4,n4=n3=n2,n2=n1,n1=n0,
n0=t3;
string1[f]= output of stream cipher;
next p ,Generator of Part keys[d]= convert string1[f] to array of char;
for L =0 to (length of generator of part keys[d]-1)
k1=generator of part keys[L];k2=convert k1 to ascii;L=L+1;
for i = 0 to (n-1) do
string3[g]= content of the first bit for byte of MMS[i+k2];break;
nexti
next L
SMS[m]=convert string3[g] to string
end algorithm

توصيف الخوارزمية المقترحه لتصميم تشفير أنسيابي لفك إخفاء رسالة SMS النصية من رسالة وسائط متعددة MMS الصوتية

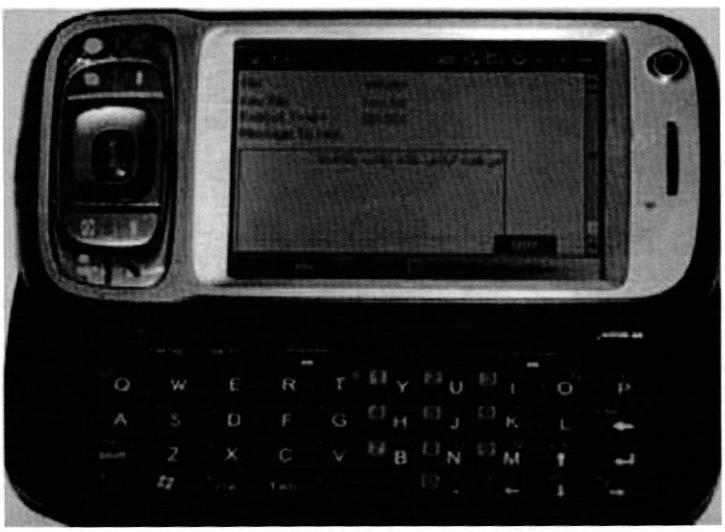
يتم الإدخال إلى الخوارزمية مصفوفتان : الأولى مصفوفة رسالة الوسائط المتعددة (MMS) الصوتية والتي مخفي داخلها رسالة (SMS) النصية والثانية مصفوفة المفتاح السري Secret key[z] ، بينما خرج الخوارزمية هو مصفوفة رسالة(SMS) النصية. ويكون عمل الخوارزمية كالتالي : في البداية نقوم باستخراج حجم رسالة (SMS) النصية من رسالة الوسائط المتعددة (MMS) الصوتية ابتداء من الموقع 101 إلى 150 ، بحيث نقوم باستخراج محتويات البت الأول للبايت المحدد من قبل المؤشر i ونضعه في المصفوف D[g] وبعدها نحول محتويات تلك المصفوفة إلى رقم عشري ونضعه في المتغير x ، ثم نقوم بقراءة محتويات مصفوفة المفتاح السري وتحويلها إلى عدد ثنائي(binary) ونضعه في المصفوفة K1[b] ، حيث إن المتغيرات x0…x11,y0…y11,n0…n11 تأخذ قيمتها من المصفوفة K[b] وبعدها يتم خرج التشفير الانسيابي stream cipher سلسلة من الأصفار والواحدات ونضعه في المصفوفة string1[f] ونحول محتويات تلك المصفوفة إلىأحرف ونضعها في المصفوفة generator of part keys[d] ومن خلال هذه المصفوفة يتم توليد مصفوفة المفاتيح الجزئية ، وبعدها نأخذ محتويات كل بايت من مصفوفة توليد المفاتيح الجزئية ونضعه في المتغير K1 ومن ثم تحويل محتويات تلك المتغير إلى ASCII ونضعه في المتغير K2 ، وبعدها نقوم بقراءة محتويات رسالة الوسائط المتعددة (MMS) الصوتيةومن خلال المتغير ان K2,i يتم تحديد البايتات لرسالة الوسائط المتعدد (MMS) الصوتية والتي مخفي داخلها بتات الرسالة (SMS) النصية ، حيث يتم استخراجها كالتالي :

String3[g]=Content of the first bit for byte of MMS[i+k2 ، وهكذا يستمر عمل الخوارزمية حتى يتم استخراج كافة بتات الرسالة (SMS) النصية ووضعها في المصفوفة string3[g] ، وثم تحويل محتويات تلك المصفوفة إلى سلسلة نصية ووضعها في مصفوفة الرسالة (SMS) النصية وبالتالي أصبحت الرسالة جاهز ة للمستخدم .

النتائج و الاستنتاجات

تم تطبيق البرنامج للخوارزمية المقترحة باستخدام لغة#C على أجهزة الجوال من نوع htc، وتم إخفاء عدة رسائل (SMS) النصية ذات أحجام مختلفة داخل رسائل وسائط متعددة (MMS) الصوتية ، حيث تم إرسال رسائل أجهزة الجوال (SMS) النصية عبر شبكة اتصالات سيريانتيل، و هذه الرسائل تم تمريرها عبر عدة مراكز خدمة الرسائل القصيرة و البلوتوث ، وحققت الخوارزمية سرية عالية جداً للمستخدم، إضافة إلى حماية رسائل (SMS) النصية من الأعداء أثناء تشغيل البلوتوث في المنطقة التي توجد فيها عدة أجهزة جوال تشغل البلوتوث، حيث إن الرسائل (SMS) النصية عندما ترسل يتم خزنها في شبكة الاتصالات داخل مركز خدمة الرسائلSMSC وبعدها يتم إرسالها إلى الجوال المقصود وهذا حسب SIM، و إثناء تطبيق الخوارزمية للعمل مع الرسائل(SMS) النصية المكتوبة باللغة العربية تبين أن أحرف اللغة العربية تحجز 16 بت لكل حرف عند استخدام أجهزة الجوال ، ومن هذا المنطلق فإن عدد أحرف رسالة أجهزة الجوال(SMS) النصية هو 70 حرف ، بينما أحرف اللغة الإنكليزية تحجز 8 بت لكل حرف والسبب هذا يجعل رسالة أجهزة الجوال(MMS) النصية المكتوبة باللغة الإنكليزية تأخذ 160 حرف . والشكل (3) يبين عمل واجهة عمل البرنامج التطبيقي ، كما تم تطبيق عدة مفاتيح لتوليد المفاتيح الجزئية . والجدول (1) يبين المفاتيح المستخدمة وحجم الرسائل (SMS) النصية، وتم تطبيق مقاييس التشويه العالمية للملفات

الصوتية كما مبين في الجدول (2) ، حيث إن قيمة MAS=MSE وذلك لأننا نقوم بإخفاء البيانات في البت الأول ، وأن مقدار أكبر خطئ هو واحد، بينما قيمة نسبة الضجيج للإشارة الصوتية SNR هي قليلة جداً بالنسبة لحجم رسائل وسائط متعددة (*MMS*) الصوتية المستخدم، ومن خلال تنفيذ الخوارزميه المقترحه تبين لنا ان المفاتيح المستخدمة في الإخفاء غير متكررة ومن لصعب جداً كسرها، لأن المهاجمين أو المتطفلين عليهم أولاً معرفة مصفوفة المفتاح السري التي تغذي المسجلات في الحالة الابتدائية ومنها معرفة المفاتيح الجزئية وعددها وهذا يتطلب التالي : محاولة التجربة لمعرفة الحالة الابتدائية للمسجلات هي (2^{168}-1) احتمال، وبالتالي فإن عدد المحاولات هو ($3.7*10^{50}$) محاولة وا ذا تمكن المهاجم تجربة معرفة احتمال واحد للحالة الابتدائية للمسجلات في كل1 ميكرو ثانية ، وبالتالي فإن الوقت المطلوب لتجربة جميع الاحتمالات هو ($5.9*10^{36}$) سنة . وبعد ذلك على المهاجم كيفية استنتاج المفاتيح الجزئية الغير متكررة والمتولدة من مسجلات التشفير الانسيابي، والتي قمنا بتصميمها لخوارزمية الإخفاء.



الشكل(3) جهاز الجوال(HTC) المستخدم لتنفيذ الخوارزمية المقترحة

الشكل(4) الواجهة الرئيسية لبرنامج الخوارزمية المقترحة المنفذة على جهاز جوال من نوع HTC

الجدول (1) المفاتيح وحجم الرسائل (SMS)النصية التي تم إخفاؤها داخل رسائل وسائط متعددة (MMS)الصوتية

	Key of secret	Size of sms by number of character		Size of mms by byte
		Arabic	English	
1	مكشابتوؤبلاقابلثلات	10	20	19kbyte
2	Ftgresajhuytbvcxzmok	20	40	40kbyte
3	92047581264863869302	30	60	28kbyte
4	FTGHNYUIOQWERFCDGHMP	40	80	78kbyte
5	FTGHNYUIOQWERFCDGHMP	50	70	98kbyte
6	السمكنتلفبقيثبقساغ	60	120	225kbyte
7	VFDGBHYTRESDCVBNHJGF	70	160	150kbyte

الجدول(2) تطبيق مقاييس التشويه العالمية للملفات الصوتية [14]

Mean Absolute Error	$MAE=\frac{1}{N}\sum_{i=0}^{n} wav(i)-Recwav(i)$
Mean Square Error	$MSE=\frac{1}{N}\sum_{i=0}^{n}(wav(i)-\mathrm{Re}\,cwav(i))^2$
Signal to Noise Ratio	$SNR=10\log_{10}\left(\frac{1}{N}\sum_{i=0}^{n} wav(i)^2/(MSE)\right)$

SMS	MMS	MAE	MSE	SNR
10	19kbyte	0.0041118	0.0041118	69.88
20	40kbyte	0.0039062	0.0039062	70.10
30	28kbyte	0.0083705	0.0083705	66.79
40	78kbyte	0.0040064	0.0040064	69.99
50	98kbyte	0.0039859	0.0039859	70.01
60	225kbyte	0.0020833	0.0020833	72.83
70	150kbyte	0.0036458	0.0036458	70.40

المصادر

1- Ying l, Dinglong h, Havivi Z, Rau P., 2008-Users' Perception of Mobile Information Security.

2- Jansen W, Karyglannis T.,– Mobile Agent Security , NIST Special Publication 800-19 National Institute of Standards and Technology.

3-The Government of the Hong Kong Special Administrative Region February 2008 - short message service security. hong kong region .

4-How to Choose an SMS Service Provider (SMS Gateway Provider, SMS Reseller, SMS Broker)- 2006, devlopershom.com .

5-LOON Y., 2006- short message service (sms) security solution for mobile, naval postgraduate school california.

6- How to Create MMS Services, Version 4.0; June 26, 2003.

7-MMS streaming protocol Website http: //sdp. ppona. com .

8-RHEE M., 2003-Inernet security, library of congress .

9-Yi l.,-2006-Applied Stream Ciphers in Mobile Communications,. institute of systems Communications ,chine .

10- Amin M., 2003- Information hiddingusing steganography, university of technology Malaysia .

11- AHMED M. , March 2009 - Threats to Mobile Phone Users' Privacy . Faculty of Engineering & Applied ScienceMemorial University of Newfoundland .

12- Alrababaa M ., 2011-Experimental Validation for Hiding Data Using Audio Watermarking, Australian Journal of Basic and Applied Sciences, 5(7): 135-145,ISSN 1991-8178 .

13- عبد القادر فادي ، 2006- احترف برمجة الشبكات والبروتوكولات بواسطة لغة السي شارب ، عمان- الأردن .

14-Hilal H., 2010-Data Hiding in Audio File by Modulating Amplitude, Eng& Tech. Journal, V0128, N05.

Design of stream cipher for generat partial keys to Hide the Short Message Service(SMS) of Mobile Devices Within the Sound Multimedia Message Service (MMS)

Yahya Najjar[1], Mhammod Shaar[2], Akbal Arab[2], Mashary Aead Asker ALtretheth Al Shammary[2]
[1] *Dept of Computerengineering Electrical and Electroicengineering , Faculty, University of Aleppo*
[2] *Postgraduate Student (PhD)*

Abstract
Mobile devices messages which are sent via the communications networks (SMS) are widely used in practical life. All the messages are sent via the communications networks which are stored inside the mobile devices, are under the threat of attackers or hackers. Mobile devices are being developed very rapidly in response to the user's need, while the protection of the (Messages or Information) is achieved by locking the mobile devices with a special lock. This lock can be unlocked using the opening programs which are existed in the computers. So, these messages need the design of a programmed system for their protection. The purpose of this research is to construct algorithm to hide the short message service (SMS) within the multimedia message service (MMS) with a very high secrecy via the design of a(Stream Cipher) to create a series of partial keys for that algorithm. This design consists of three shift registers. Each one consists of 12 bits where there is a series of zeros and ones series. That creates a series which is the series of the partial keys through which the choice of the bits position is selected from the sound multimedia message service with a very high secrecy which makes it difficult to the enemy to locate those positions. To achieve this, the least significant bits (LSB) which have been used by using a secret key composed of 21 bytes (168 bits).Consequently, the probabilities that maybe taken in the initial state to feed the registers are $(2^{168}-1)$ probabilities. This algorithm has been executed on an htc mobile devices.
Multimedia massage service (MMS),short message service (SMS), Least significant bit(LSB)