



بسم الله الرحمن الرحيم

تقنيات التشفير

في هذا العدد نقدم شرح لأنواع التشفير مع تطبيقات عملية لبرامج مشروحة،
موضوع البحث ينقسم الى جزئين

1- طريقة التشفير المتناظر - Symmetric Encryption

- المقدمة
- شرح لأحد برامج التشفير: 2.0ChaosMash

2- طريقة التشفير الغير متناظر - Asymmetric Encryption :

- مقدمة عامة، البريد الالكتروني المخاطر والحلول
- التشفير الغير متناظر
- التوقيع الرقمي
- الشهادة الرقمية
- شرح لأحد برامج التشفير: WinPT

التشفير المتناظر

Symmetric Encryption

1- المقدمة:

التشفير بشكل عام هو عملية الحفاظ على سرية المعلومات (الثابت منها و المتحرك) باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات الى رموز بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول لهم بذلك لا يستطيعون فهم أي شيء لأن ما يظهر لهم هو خليط من الرموز والأرقام و الحروف الغير مفهومة, يتم تشفير الملف وفك التشفير عن طريق كلمة السر, التي يجب ان تكون معروفة للطرفين (المرسل والمستقبل) وهذا ما يسمى بالتشفير المتناظر, كلمة Decryption تعني فك التشفير.

أشهر طرق التشفير المتناظر

Blowfish, Digital Encryption Standard (DES), Tiny Encryption Algorithm, Triple DES, and International Data Encryption

يقصد بالتشفير المتناظر , اي انه يوجد مفتاح واحد معروف لدى الطرفين لفك التشفير , وهي كلمة السر

قوة التشفير

تعتمد قوة وفعالية التشفير على عاملين أساسيين: الخوارزمية، وطول المفتاح مقدراً بالبت Bit, كل ما زاد البت, زادت نسبة الأمان وصعوبة فك الشيفرة.

الطريقة الصحيحة لتشفير الملف:

1- ضغط الملف

2- ومن ثم تشفيره

2- شرح لأحد برامج التشفير التي تستخدم طريقة التشفير المتناظر:

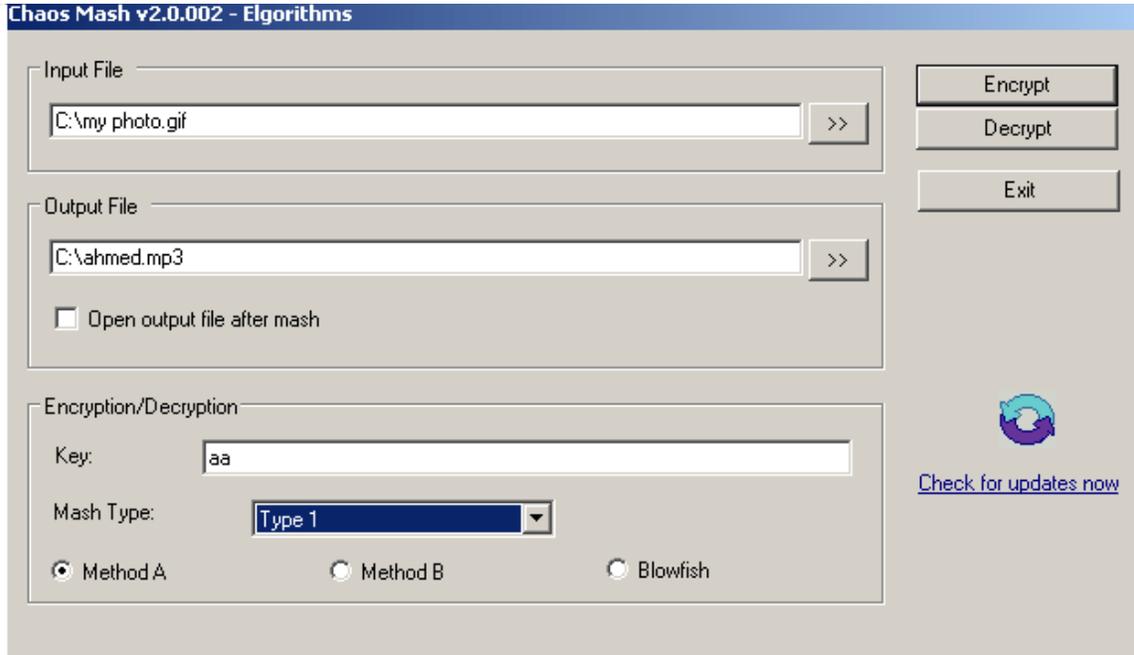
ChaosMash 2.0

برنامج 2.0ChaosMash يُعد من البرامج البسيطة والسريعة في التشفير , من خصائصه:

1- لا يحتاج لتنصيب, ملف واحد فقط

2- يستخدم 15 طريقة للتشفير

لمزيد من التوضيح, استعن بالصورة:



مصطلحات:

1- input file: هو الملف الذي ترد تشفيره.

2- output file: هو الملف المشفر الجديد, يمكن حفظه بأي مكان , ويمكنك اختيار اي امتداد له.

3- key: عبارة عن مفتاح لفك التشفير, هذه الخاصية اختيارية .

4- Mash Type: وهي نوع التشفير الخاصة بالبرنامج, وتزداد قوة التشفير بإزدياد النوع type 1type15.

-5 method A, method B, Blowfish: عبارة عن الخورزميات المستخدمة للتشفير.

-6 encrypt: تشفير الملف, decrypt: فك التشفير.

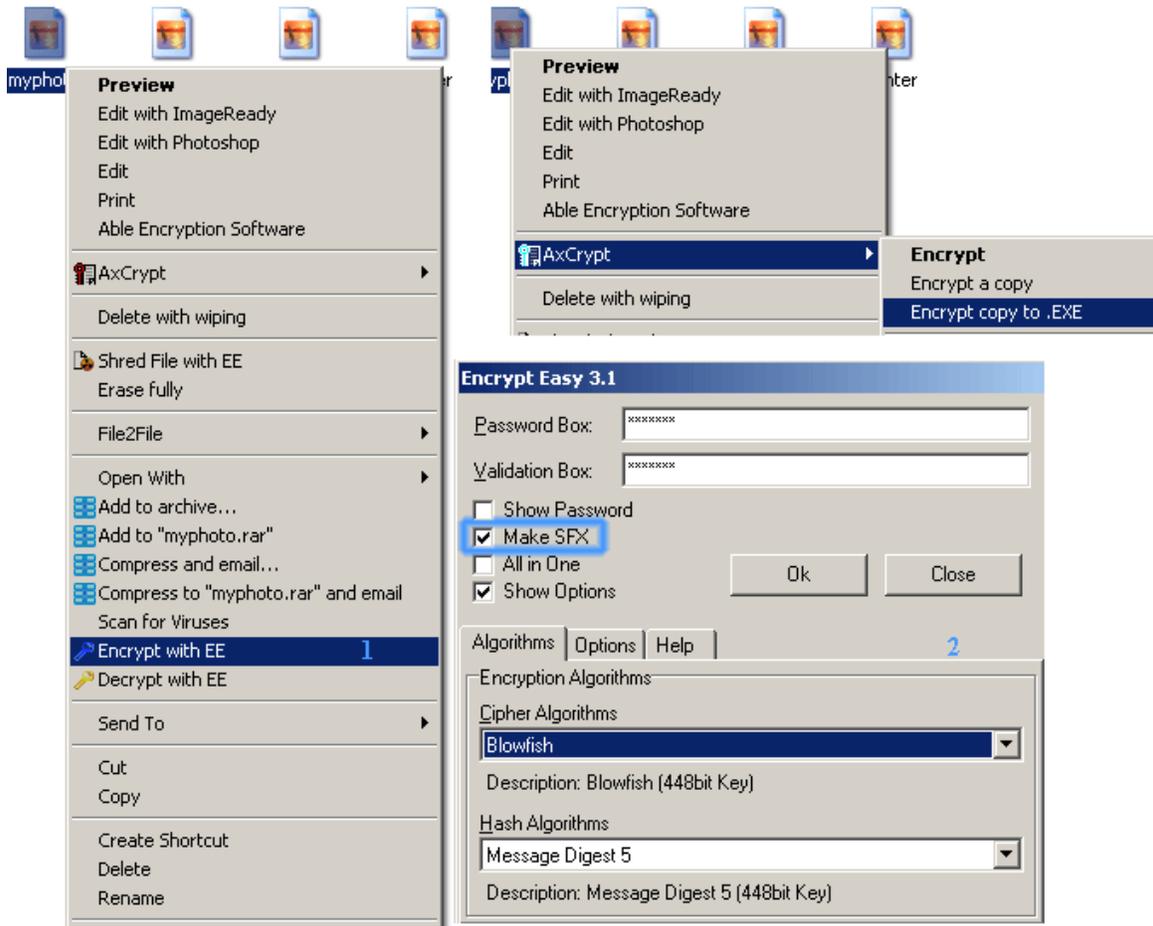
عند استقبال الطرف الآخر للملف المشفر, يجب عليه ان يفك التشفير decrypt بنفس الطريقة التي تم فيها تشفير الملف, اي انه على فرض ان الطرف الأول قام بعمل التالي لتشفير الملف: استخدم method B, type 13, يجب على الطرف الثاني استخدام نفس الطريقة.

عند فك التشفير للملف, في خانة input file تضع الملف المشفر, وفي خانة output الملف بعد فك التشفير, لا تنسى انه يجب عليك معرفة امتداد الملف الحقيقي للملف الذي تم فك تشفيره, حتى تتمكن من فتحه.

وجود كلمة SFX -Self Extrat, في برامج التشفير تعني انه لا يلزم وجود برنامج لفك تشفير الملف عند الطرف المستقبل للملف المشفر, فبوجود هذه الخاصية فإن الملف المشفر يكون عبارة عن ملف تشغيل exe يمكن فك تشفيره عن طريق ادخال كلمة السر فقط.

بعض البرامج التي تدعم هذه الخاصية:

- AxCrypt
- encrypt-easy



التشفير الغير متناظر

Asymmetric Encryption

1- المقدمة:

مع ازدياد الاعتماد على البريد الالكتروني كأحد أهم وسائل الاتصال في قطاع الأعمال يزداد القلق من مخاطر استخدام البريد الالكتروني على سرية المراسلات ومن إساءة استخدامه عن قصد. وخاصة بعد انكشاف منظومات تجسس عملاقة تديرها حكومة الولايات المتحدة الأمريكية وحلفاؤها في بريطانيا وأستراليا. ومؤخرا أقرت الولايات المتحدة قانونا يبيح التجسس على مراسلات الأفراد بدون إذن قانوني، مما يزيد المخاوف من عمليات تجسس مستمرة على المراسلات الشخصية للأفراد والشركات.

هذه المخاوف مشروعة، فالبريد الالكتروني ليس خدمة كاملة وآمنة ومثالية بالحالة العادية، ولكن مع بعض الإجراءات الإضافية يمكن رفع مستوى أمن المراسلات لدرجة تعتبر آمنة.

أهم مخاطر إساءة استخدام البريد الالكتروني:

* الاطلاع على الرسالة: بعض الرسائل قد تكون سرية ولا يرغب المرسل والمستقبل بتسرب محتواها، وخلال سير الرسالة عبر الإنترنت قد يقوم أحد المخدّمات بالتجسس عليها.

للأسف، في الاستخدام العادي للبريد الالكتروني، يستطيع أي مخدم تعبر الرسالة عبره أن يتجسس عليها، بل وأن ينسخ نسخة منها، بمتنها البساطة.

* انتحال الشخصية: يقوم شخص ما بإرسال رسائل منتحلا اسما وبريد الكترونيا خاصين بشخص آخر، وتصل الرسائل إلى الشخص الثالث فيعتقد أنها صادرة من الشخص الثاني ويعاملها على هذا الأساس.

للأسف لا يمكن عمليا أن نمنع أي شخص من إرسال بريد الكتروني باسم أي شخص آخر، مثلا يستطيع أي شخص أن يعدل برنامج البريد الذي يستخدمه لتظهر رسائله كأنها صادرة من الكافر بوش.

* تغيير الرسالة: حتى لو كانت الرسالة صادرة من جهة معروفة، فمن الممكن لمن يعترضها أن يعدل فيها، فمثلا يستطيع أن يغير رقما أو اسما لإحداث تأثير ما لدى المستقبل. وأيضا فهذا التهديد وارد في حالة الاستخدام العادي للبريد الالكتروني.

* إرسال محتوى مؤذي أو مزعج: مثل الفيروسات أو البرامج المؤذية بمختلف أنواعها، أو البريد المزعج الإعلاني أو البريد الممهد لعمليات الخداع عبر الإنترنت.

هل أنت معرض لهذه المخاطر؟

من يدري، فهذه المخاطر جميعها قائمة ولا أحد يدري من سيستغلها ومتى قد يفعل ذلك ولاي دافع. وحتى لو لم يكن لديك أعداء مستعدون لدفع ثمن إيدائك، فربما تقع ضحية مهووس أو غاوي تقليعات يرغب بالتفاخر أنه تجسس على بريدك.

وبسبب طبيعة عمل الإنترنت، لا يمكن في أغلب الأحوال التنبؤ بالمسار الذي تسلكه الرسالة من المرسل إلى المستقبل، ولذلك فمهما كانت احتياطات الأمن التقنية لدى المرسل ولدى المستقبل، ولدى مخدمات البريد التي يستخدمونها، يبقى احتمال تعرض الرسالة لإساءة ما على الطريق أمرا وارد الحدوث في كل لحظة.

مواجهة الأخطار:

عندما اخترع البريد الإلكتروني في سبعينات القرن الماضي، لم يكن مخترعوا الخدمة يحلمون أن تحقق هذا الانتشار، فقد طورت أساساً لتبادل البيانات الرقمية بين المؤسسات العلمية وبين أشخاص يعرفون بعضهم شخصياً. ومع انتشار الخدمة بدأت تظهر المشاكل والأخطار الناتجة عن أن تصميم الخدمة لم يأخذ بعين الاعتبار إمكانية انتشارها جماهيرياً بهذا الشكل.

تبدأ مواجهة هذه الأخطار من إدراكها أولاً، فعندما ترسل رسالة بريد إلكتروني تذكر أن رسالتك قد تتعرض للتجسس، وقد تتعرض للعبث بمحتوياتها. وعندما تستقبل رسالة بريد إلكتروني تذكر أن هذه الرسالة قد تكون مزورة، وقد تكون تعرضت لتدخل ما في مرحلة ما من مراحل انتقالها إليك.

التشفير الغير متناظر -2:

يقصد ب Asymmetric Encryption: التشفير الغير متناظر، أي وجود مفتاحين لإتمام عملية التشفير وفك التشفير، وليس مفتاح واحد كما في التشفير المتناظر (Symmetric Encryption).

يتكون التشفير الغير متناظر من مفتاحين وهما:

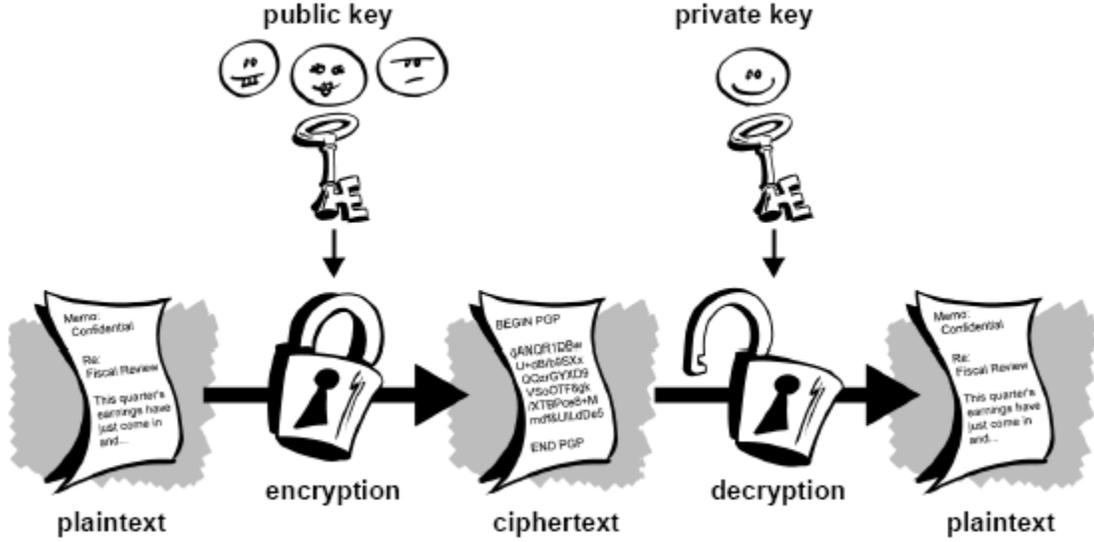
1- public key: المفتاح العام الذي يستخدم لتشفير الرسالة، ويتم إرساله لمن تريد (شخص، مجموعة ..).

2- private key: المفتاح الخاص الذي يستخدم لفك التشفير، تحتفظ به في جهازك الخاص، لا احد يعرف كلمة سر المفتاح الخاص، ولا يمكن فك الشيفرة عن الرسالة الا عن طريق المفتاح الخاص فقط، فإذا ضاع المفتاح الخاص فلا يمكنك فك التشفير عن الرسالة !.

ملاحظة: يطلق على المفتاح الخاص اسم secret key ايضاً، ويمكن اعتباره بمثابة كلمة السر لفك التشفير.

آلية عمل هذه التقنية :

بعد القيام بتكوين المفتاحين، تقوم بإرسال المفتاح العام لمن تريد (شخص، مجموعة ..)، مهمة المفتاح العام هي عمل تشفير للرسالة فقط وليس فك التشفير، الطرف المستقبل يقوم بتشفير الرسالة عن طريق استخدام مفتاحك العام الذي تم إرساله إليه، بعد ذلك يقوم الطرف المستقبل بإرسال الرسالة المشفرة الى المرسل الأصلي الذي قام بإرسال المفتاح العام له، عند استلام المرسل الرسالة المشفرة، فإنه يقوم بفك التشفير عن طريق المفتاح الخاص فقط، هو الوحيد الذي يستطيع فك التشفير عن ذلك الملف .



كما في الصورة:

- 1- plaintext: الرسالة الغير مشفرة.
- 2- encryption: تقوم بعملية التشفير عن طريق المفتاح العام (public key), تلاحظ وجود أكثر من مستخدم.
- 3- ciphertext: الرسالة المشفرة, ويتم ارسالها الى المرسل الأصلي الذي قام بإرسال المفتاح العام للأشخاص .
- 4- decryption: فك التشفير عن طريق المفتاح الخاص (private key).
- 5- plaintext: الرسالة الأصلية بعد فك التشفير.

الهدف من Asymmetric Encryption:

- 1- التخلص من مشكلة تبادل كلمات السر الغير آمنه والتي قد تتعرض للسرقة من خلال طرف اخر ويقوم بكشف المعلومات, كما في التشفير المتناظر (Symmetric Encryption).
- فعن طريق هذه التقنية فإنه يتم تداول المفتاح العام فقط وليس كلمة السر (المفتاح الخاص).
- 2- يمكنك استخدام طريقة التشفير الغير متناظر, لتداول كلمة السر الخاصة بالتشفير المتناظر.

أشهر طرق التشفير الغير متناظر:

Pretty Good Privacy (PGP) and Reinvest,shamir&Aselman (RSA)

3- التوقيع الرقمي – Digital Signatures:

يُستخدَم التوقيع الرقمي للتأكد من أن الرسالة قد جاءت من مصدرها دون تعرضها لأي تغيير أثناء عملية النقل ويمكن للمرسل استخدام المفتاح الخاص لتوقيع الوثيقة إلكترونياً أما في طرف المستقبل، فيتم التحقق من صحة التوقيع عن طريق استخدام المفتاح العام المناسب.

وباستخدام التوقيع الرقمي، يتم تأمين سلامة الرسالة والتحقق من صحتها ومن فوائد هذا التوقيع أيضاً أنه يمنع المرسل من التكرار للمعلومات التي أرسلها.

ومن الممكن اعتماد طريقة أخرى تتلخّص في الدمج بين مفهومي البصمة الإلكترونية للرسالة والمفتاح العام، وهذه الطريقة أكثر أماناً من العملية النموذجية التقليدية ويتم أولاً تمويه الرسالة لإنشاء بصمة إلكترونية لها، ثم تُشفّر البصمة الإلكترونية باستخدام المفتاح الخاص للمالك، ما ينتج عنه توقيع رقمي يُلحَق بالوثيقة المُرسَلة. وللتحقق من صحة التوقيع، يستخدم المستقبل المفتاح العام المناسب لفك شفرة التوقيع، فإن نجحت عملية فك شفرة التوقيع (بإعادتها إلى ناتج اقتران التمويه) فهذا يعني أن المرسل قد وقّع الوثيقة بالفعل، إذ إن أي تغيير يحصل على هذه الوثيقة الموقعة (مهما كان صغيراً)، يتسبب في فشل عملية التحقق. وتقوم برمجيات المستقبل بعد ذلك بتمويه محتوى الوثيقة لينتج عن ذلك بصمة إلكترونية للرسالة، فإن تطابقت القيمة المموّهة للتوقيع الذي فُكّت شفرته مع القيمة المموّهة للوثيقة، فهذا يعني أن الملف سليم ولم يتعرض لأي تغيير أثناء النقل. (مقتبس من لنشرة التجارة و التنمية)

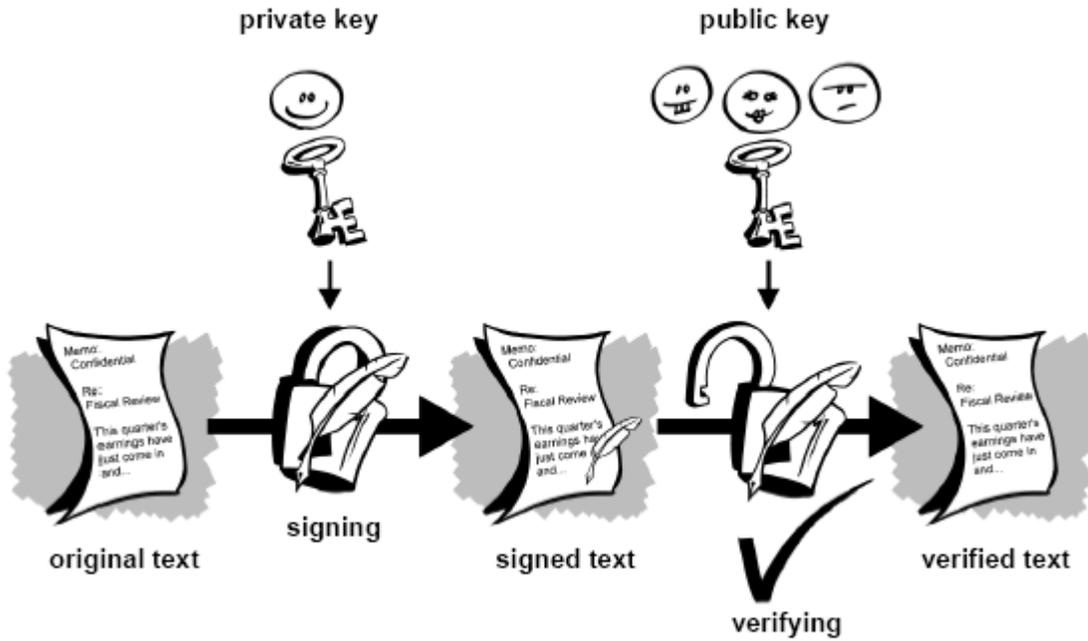
آلية عمل هذه التقنية :

كما ذكرنا سابقاً، ان المفتاح العام يمكن ان يعطى لأكثر من مستخدم، على فرض ان المرسل الأصلي الذي قام بإرسال المفتاح العام ، ارسل رسالة عادية غير مشفرة الى الطرف المستقبل

الذي عنده المفتاح العام ، كيف للطرف المستقبل التأكد من أن الرسالة قد جاءت من مصدرها دون تعرضها لأي تغيير أثناء عملية النقل، في هذه الحالة يقوم الطرف المرسل عند ارسال رسالته

باستخدام التوقيع الرقمي باستخدام المفتاح الخاص يقوم بتشفير التوقيع فقط وليس الرسالة ومن ثم عند الطرف المستقبل ، يستلم التوقيع المشفر بالإضافة الى الرسالة الغير مشفرة

مهمة هذا التوقيعي التأكد من ان الرسالة سليمة ، عن طريق القيام بمقارنة خصائص معينة في الرسالة للتأكد من انها لم تتعرض لأي تغيير أثناء عملية النقل.



كما في الصورة:

1- original text: الرسالة الغير مشفرة , التي سيتم ارسالها بشكل عادي الى الطرف المستقبل.

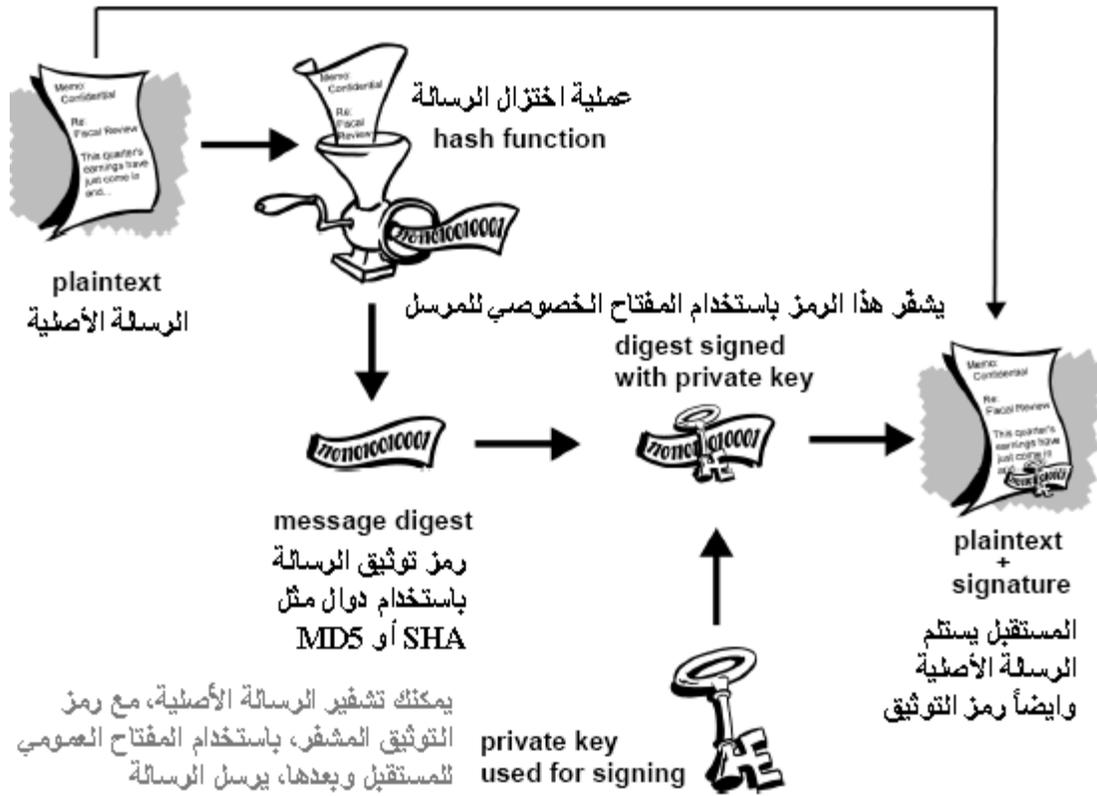
2- signing: التوقيع الرقمي للرسالة عن طريق استخدام المفتاح الخاص ليتم تشفير التوقيع فقط, يمكن ارسال التوقيع الرقمي على شكل ملف مرفق مع الرسالة الأصلية والتي تكون أيضاً على شكل ملف txt مرفق, ومن ثم يقوم الطرف المستقبل بفتح ذلك الملف , ويقوم الملف بالتأكد من الرسالة عن طريق بعض الخطوات البسيطة .

3- signed text: الوقع الرقمي المشفر لتلك الرسالة.

4- verifying: عند الطرف المستقبل , يقوم بفك تشفير التوقيع الرقمي عن طريق استخدام المفتاح العام, وإذا تم التطابق مع الرسالة الأصلية , فستظهر لك رسالة تدل على ذلك.

5- verified text: ظهور رسالة تخبرك ان الرسالة المرسله اليك لم تتعرض لأي تغيير اثناء عملية النقل.

ملاحظة : يعتبر التوقيع الرقمي بمثابة ال hash function , بحيث يؤدي الى نفس الهدف ,
 للتوضيح استعن بالصورة:



4- الشهادة الرقمية – Digital Certificates:

كيف يمكن للمستقبل الذي يقوم بتشفير الرسالة عن طريق استخدام المفتاح العام من التأكد بأن الرسالة المشفرة , تم تشفيرها فعلاً عن طريق استخدام المفتاح العام الحقيقي الذي تم إرساله عن طريق المرسل الأصلي , كيف نضمن ان الرسالة فعلاً يتم فك تشفيرها فقط عن طريق المرسل الأصلي الموثوق به ؟.

في هذه الحالة تستخدم تقنية الشهادة الرقمية " Digital certificates " , التي هي بمثابة جواز السفر الذي به بيانات المرسل الأصلي (إسم المرسل, رقم المرسل, الصورة الشخصية, عنوان البريد, نوع التشفير المستخدم, تاريخ انشاء المفتاح العام, تاريخ انتهاء صلاحية المفتاح العام ..).

الشهادة الرقمية تحتوي على:

1- المفتاح العام "public key".

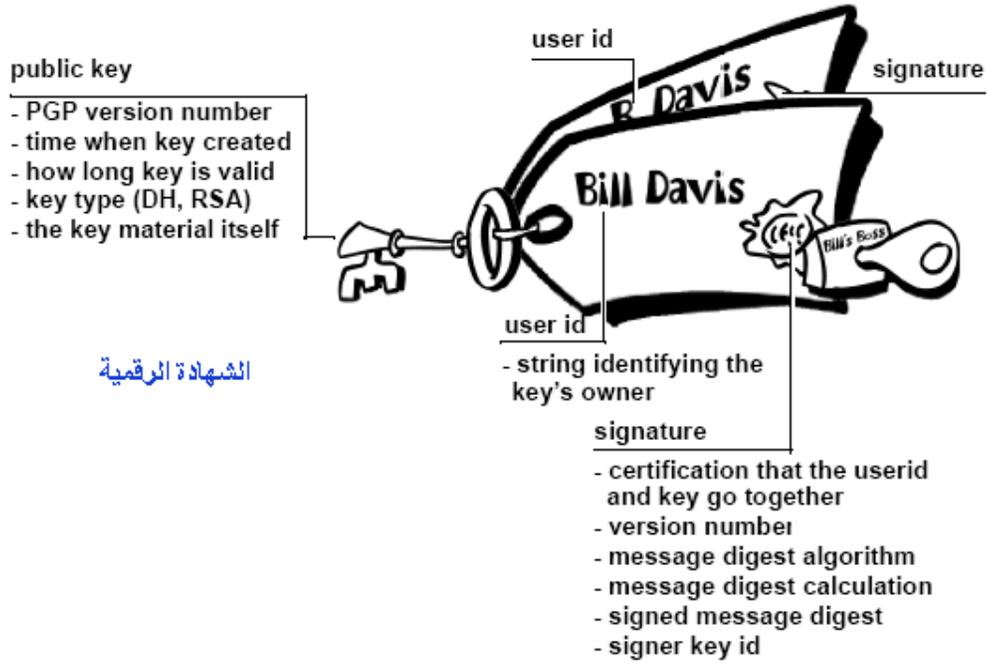
2- معلومات عن المفتاح العام: مثل (إسم المرسل, الكنية, رقم المرسل, عنوان البريد ..).

3- التوقيع الرقمي.

يتم دمج جميع هذه المعلومات في المفتاح العام, ومن ثم يتم إرساله الى الطرف المستقبل, يمكن للطرف المستقبل التأكد من المفتاح العام وخصائصه مثل اسم المرسل .. الخ, كما ذكرنا.

من التطبيقات العملية على موضوع التشفير الغير متناظر, هو برنامج Windows Privacy Tools - WinPT, الذي يعد من اقوى البرامج في التشفير واكثرها اماناً بسبب استخدام

خوارزمية (Pretty Good Privacy - PGP) التي تعد من اقوى الخوارزميات في تشفير الرسائل.



الشهادة الرقمية

5- شرح لأحد برامج التشفير التي تستخدم طريقة التشفير الغير متناظر:

تقدم تقنية PGP امكانية تشفير وتوقيع الرسائل رقميا وقد اثبت هذا البرنامج صموده في وجه جميع محاولات الكسر، وتوضح الحسابات أنه لا يمكن كسر تشفير PGP من قبل أحد في العالم ضمن زمن مقبول، ولذلك فهو يعتبر سرا عسكريا، وتمنع حكومة الولايات المتحدة تصدير برامج PGP إلى بلدنا، ولكن يمكن الحصول عليها من مصادر أخرى.

على الإنترنت عدة برامج مفتوحة المصدر تدعم تشفير PGP، وأهمها GnuPGP الشهير اختصارا ب GPG. ويمكنك إضافة هذا البرنامج الى أغلب برامج البريد الالكتروني لتتمكن من تشفير الرسالة او توقيعها رقميا باستخدامه.

Windows Privacy Tools – WinPT

هذا البرنامج يستخدم خوارزمية (Pretty Good Privacy - PGP) التي تعد من اقوى الخوارزميات في تشفير الرسائل , والتي لم تخترق الى الآن, يمكنك ايضا تشفير الملفات.

ملاحظة: قبل البدء تأكد من خلو الجهاز من ملفات التجسس, حتى لا يسرق المفتاح الخاص.

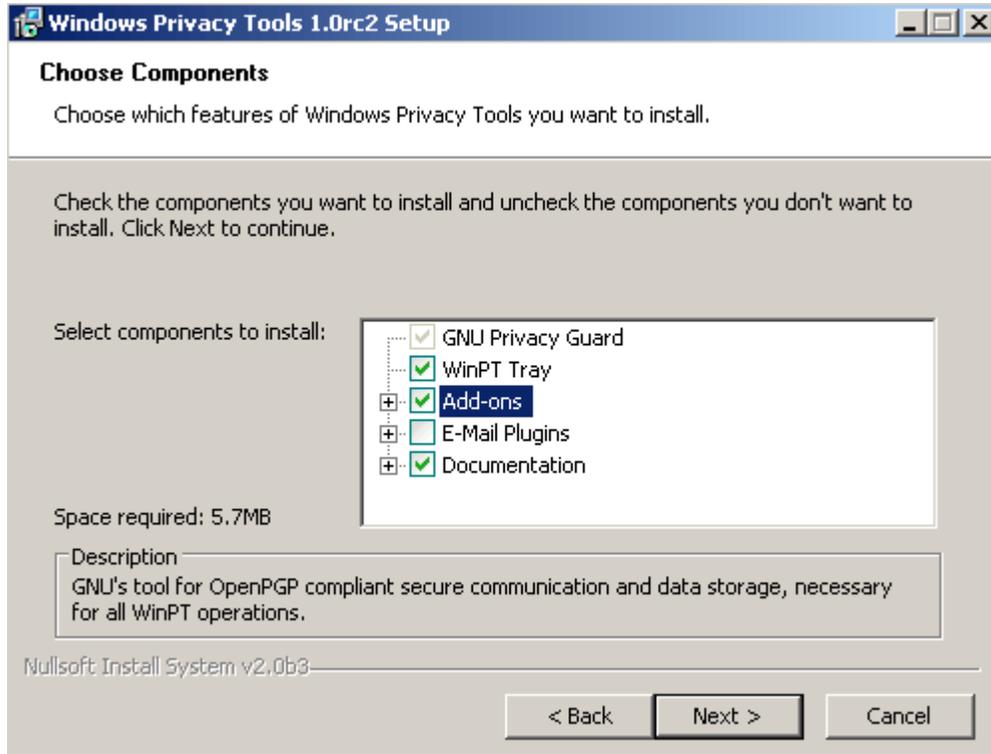
في الخطوات القادمة حتى تصل الصورة اعتبر التالي , وجود طرفين احدهما مرسل والآخر مستقبل

الطرف المرسل	
abu abdalrahman	الإسم
publicKey ID: 0x5F0B907F 2006-02-13 abu abdalrahman <abu_boxii2006@yahoo.com> Primary key fingerprint: 758B 8F52 B651 72F3 55A5 BE16 CDCC A8D0 5F0B 907F	معلومات عن المفتاح
الطرف المستقبل	
Omar alayobi	الإسم
publicKey ID: 0x68F7C804 2006-02-14 Omar alayobi <omar_alayobiii2006_@yahoo.com> Primary key fingerprint: 67AA 9559 87EB 6ABE DDC0 BDBE 5529 1EA0 68F7 C804	معلومات عن المفتاح

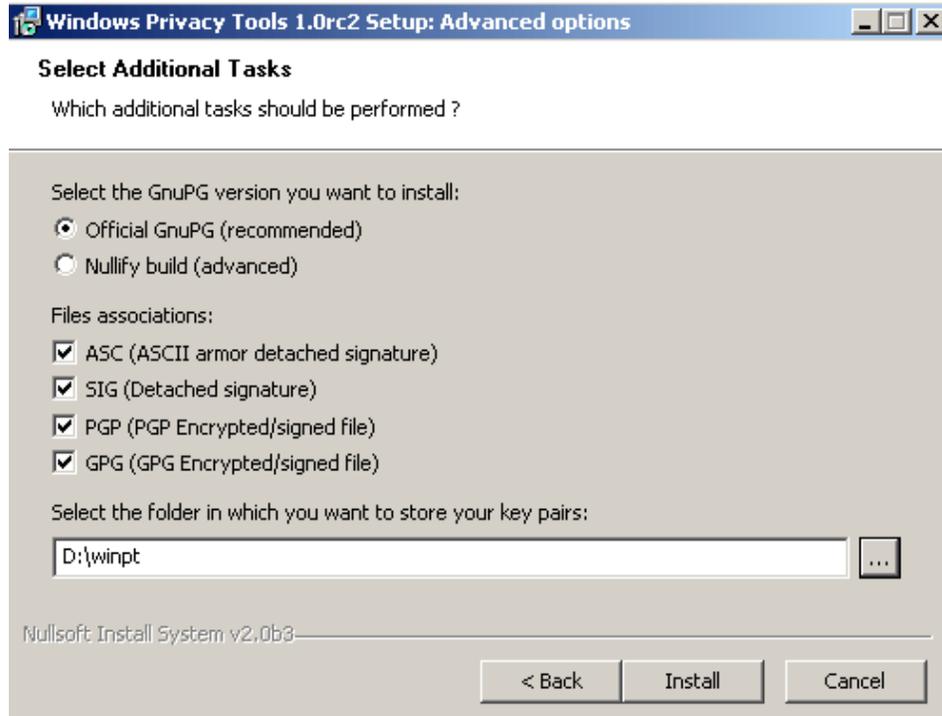
المرحلة الأولى: Asymmetric Encryption

خطوات تنصيب البرنامج : حتى تصل الفكرة لنعتبر الخطوات التالية هي من جانب الطرف المرسل

1- اضغط next ,! يمكنك وضع اشارة صح على E-mail Plugins, اذا اردت ان يتعامل البرنامج مع برنامج outlook.

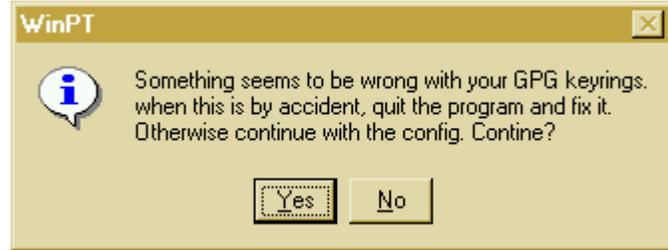


2- اختر مسار المجلد الذي تريد تخزين المفاتيح به, والتي سيتعامل معها البرنامج, مثال: D:\winpt



3- توليد المفتاح العام والخاص (PGP key pair).

بعد الإنتهاء من تنصيب البرنامج, قم بفتحه, ستظهر لك رسالة تخبرك انه عليك توليد المفاتيح اضغط **yes**.



4- OK.



5- توضيح الشاشة التالي:

NOTE: Key generation can be a lengthy process!
Please wait until you get the message that key generation was finished.

Key type: DSA and ELG (default)

Subkey size in bits: 1792 1024-4096

User name: abu abdalrahman

Comment (optional):

Email address: abu_boxii2006@yahoo.com

Key expiration: .. Never

Passphrase: *****

Repeat passphrase: *****

Start Cancel

* key type: نوع الخوارزمية المستخدمة في التشفير. البرنامج يقوم بدمج أكثر من خوارزمية معاً أثناء التشفير كما هو موضح DSA and ELG.

* subkey size in bits: قوة المفتاح كلما زاد البت زادت قوته , الحد الأدنى لحجم المفتاح 1024 bit اي (كلمة السر تتكون من 10 خانات). وهي افضل من ناحية الأمان.

* User name: اسم المستخدم

* Comment: تعليقات اضافية (هذه الخاصية اختيارية).

* عنوان البريد الخاص بك.

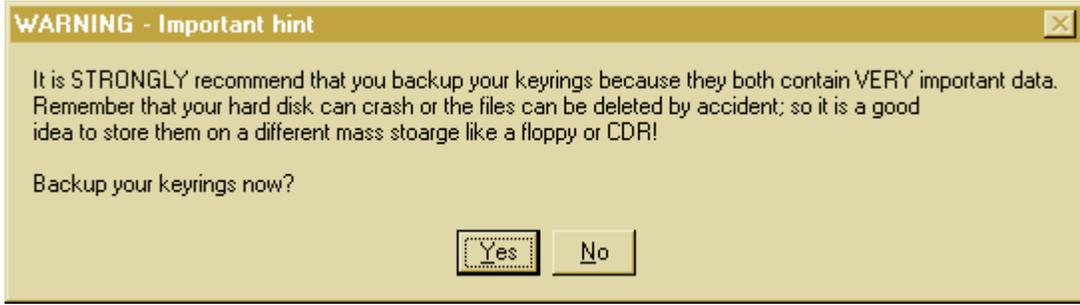
* key expiration: تاريخ انتهاء صلاحية المفتاح, لك الإختيار في ذلك, يمكنك جعل المفتاح غير محدد الزمن Never.

* Passphrase: كلمة السر التي تستخدم للتشفير وفك التشفير.

* Repeat Passphrase: تأكيد كلمة السر.

بعد الإنتهاء من هذه العملية اضغط start ليبدء البرنامج بتوليد المفاتيح (الخاص والعام).

6- هذه الرسالة تقول لك, هل تريد الإحتفاظ بنسخة احتياطية للمفاتيح في حالة ان جهازك تعرض لمشاكل ما , اضغط yes إذا اردت ذلك.



7- اختر اين تريد حفظ المفاتيح, كنسخة احتياطية , لتتمكن من استرجاع المفاتيح فيما بعد, في حالة فقدان المفاتيح الأصلية , او فقدان المعلومات عند عمل فورمات للجهاز او اي عطل اخر.



تم حفظ المفاتيح كما ترى في الشكل:



بعد الإنتهاء من حفظ المفاتيح, تبين لك شاشة ال key manager المفاتيح التي كونتها , يمكنك عمل مفتاح جديد عن طريق الضغط على key-generate.

User ID	Key ID	Type	Size	Cipher	Validity	Creation
abu abdalrahman <abu_boxii2006@yahoo.com>	0x5F0B907F	pub/sec	1024/1792	DSA/ELG	[] Ultimate	2006-02-13

8- بعد الإنتهاء من توليد المفاتيح , الخطوة الحالية هي القيام بتصدير المفتاح العام للطرف الآخر المستقبل, الذي سيقوم بإستخدام المفتاح العام لتشفير الرسائل وإرسالها لك , وانت تقوم بفك التشفير

عن طريق المفتاح الخاص.

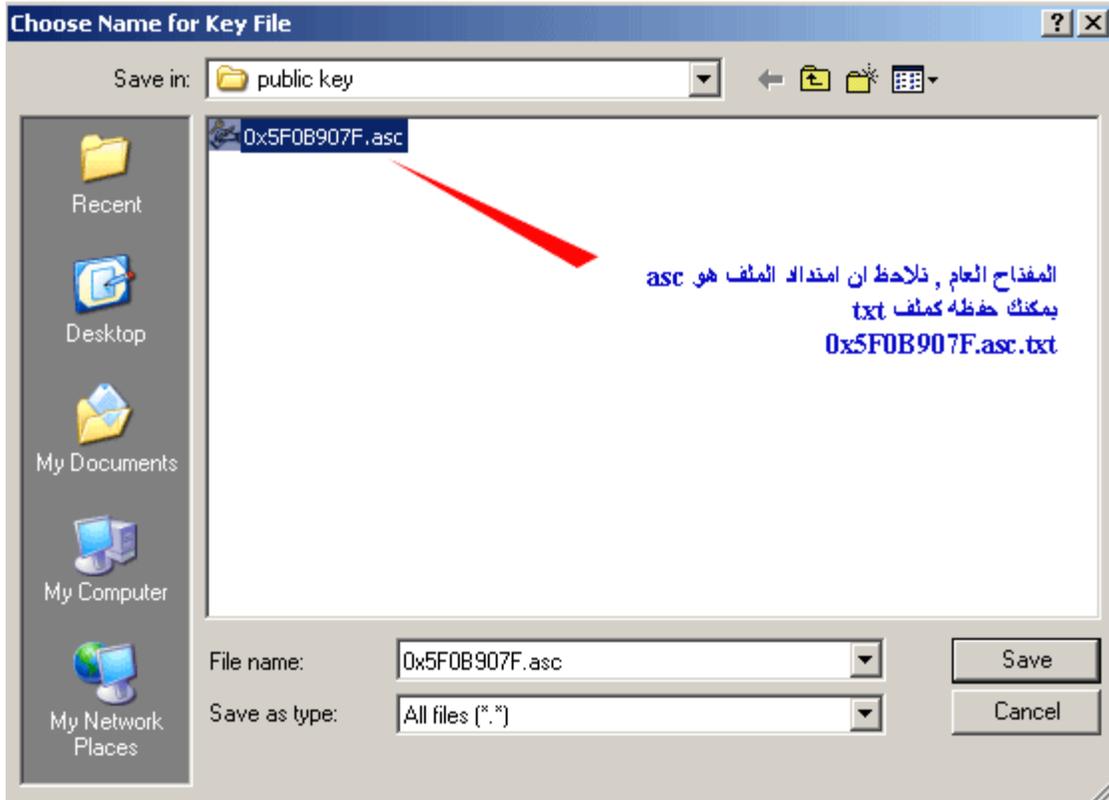
اضغط على Key Manager.



ستظهر لك شاشة المفاتيح , قم بالضغط على المفتاح الموجود في الشاشة, حتى يصبح على شكل مظلل, ومن ثم اضغط -Export key اي تصدير المفتاح العام.

User ID	Key ID	Type	Size	Cipher	Validity	Creation
abu abdalrahman	5F0B907F	pub/sec	1024/1792	DSA/ELG	[] Ultimate	2006-02-13

في هذه الخطوة, قم بتحديد المسار الذي تريد حفظ المفتاح العام به. لاحظ رقم المفتاح العام key ID. أيضاً يمكنك حفظه على شكل ملف مقروء .txt.



بعد ذلك قم بإرسال المفتاح العام للطرف المستقبل, عن طريق البريد الإلكتروني او اي وسيلة تراها مناسبة لك.

توضح الصورة التالية المفتاح العام , يمكنك الحصول على هذه الشاشة عن طريق الضغط بالزر اليمين للماوس ومن ثم open with -notepad .

```

0x5F0B907F - Notepad
File Edit Format View Help
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.2.1 (MingW32)

mQGhBEPwYSURBACdj/cHpjkyJtP8jwHFrKY7y/y2jUmW2RD27O7w0ByYObQIUcS
wLUnLgyUJgqWJpjqQFEWimI3vsCxEd8BXqjcy0U3yB3ZjkoxPe4LRGWLHr+BvNG
r5YhCGOqkq91mbtrjRU2xLhAMfjhZK372NZeaAVYijzMR0C8mRPE8/v+sNwCgtRqQ
y0n7vF+ecb2t2kLQPmkMaNUd/1wLazQq81302FkPqf1OortjwT9rH2hrX2Q+WCF4
BVPwmbGcH75TDou/uuJTTWTZ6hhWSvE3pxxuDx6oZY9/wtj3+ios0/TgQm9KxeXX
9ODN+xYqjZ6u8B9LsB88QwcaD8pDCncgYLwhKh/CPojgRZGrU2CjDG+MR3VCoLFR
FRDTA/9nOcvOgJmJPTJuxkZpwkthgCE8+NUee3SfIWRmuY1o4vftT3Kv8zQxTcP
liyQCRdrHepDJvsdw8UoZbMmyYRP0TONR/iV/kqek3Wgh9cad/2nSdTT0FcNiLgQ
yFHgI8tuffT/2YXCnAAbiLr3LmGjKfOXTj4NVIUixTXyXePL7QpYWJ1IGFiZGFs
cmFobWfuDxhYnVfYm94aWkyMDA2QHlhaG9vLmNvbT6IWQQTEQLAGQUcQ/BhJQQQL
BwMCAXUCAwMWAqECHgECF4AACgkQzcyo0F8LkH91swCcDYyevfib2Ier1VmmRmjN
iPhufVkAnlWSuYJobmZQbimOXVNI/eB6F789uQHNBEPwYTIQBwCv4gCFnRUi2fNv
y3NECAXlg5INAVwWUuV2tdIKQVfan+5Wb4cWfXrNBZBFXJdJnPONDvWC6W/5ZCE
iuxFkad8vNTStCixzZVLhPFUvupKE9mBUf2NCqSgO4C0hH5ZfYhzNNnmQsawXTE6
4WpfrW/NaCj8w6uTO+SVPqMahmjgwZrBdp8EhZGm2hdhnWAZdQYOM0U0WvgGh1Da
xHytxgjjF5zDreWBFJz6Bpe7zQ9hO13COWKhsxdBH8s9Ps2WhmYlu4mKr/HIEoSO
mxxF48pGtAqBhBdEEJKvonyNLmGsDwADBQb+JII+4/8yaEgG0nEb+N8llL6NxbA6
997u4K62eGZCAJhT21sXuP4lJbnie3X/31Dkerk/pl0hMfCVCFcbS3jn4GINDLDg5
Vova7IW5RKXSwROmRkpIszN7Daf+M0K5dxGXCOej5PXHF/Z1Xhmy5HdHqLZPyXM
uifltOnkMnE0iMYR08ML7jIm68hrwIbq6wsNz8vu+TiEMy5afVLSFXKaWPTkOb6Z
BNrYgUg/y40A66BckJ36nmJthR0EttZW1xZDVl03u5BYs7VQNGK4a4Kdnw6hx+k+
QaFLiQUtHWXrJ6KIRgQYEQIABgUCQ/BhMgAKCRDNzKjQXwuQfzORAJ0csJdpivzq
fyAL30KSGOrkLkCgwCfQJpm76RGZl54YDXY1RQsPe/CQAU=
=qYnv
-----END PGP PUBLIC KEY BLOCK-----

```

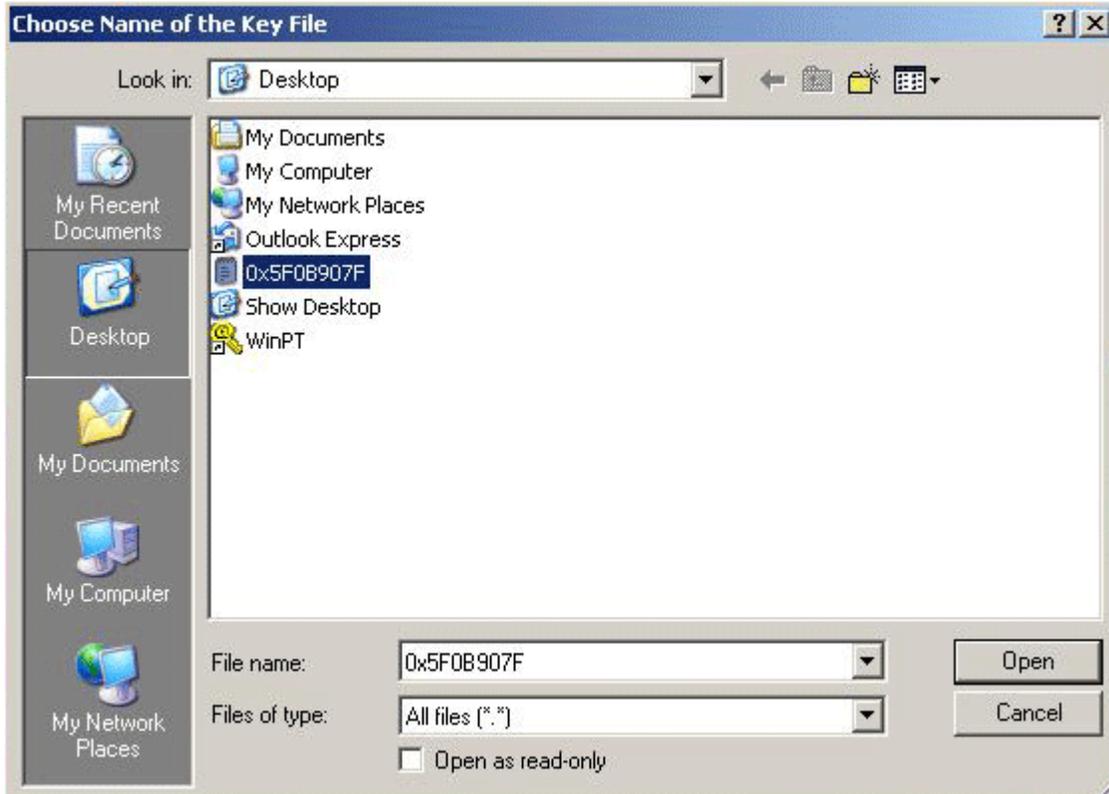
الطرف المستقبل : له مفتاحه الخاص الذي عمله , وهو بإسم Omar , حصل Omar على المفتاح العام من abu abdalrhman .

User ID	Key ID	Type	Size	Cipher	Validity	Creation
Omar alayobi <omar_alayobiiii2006_@yahoo.com>	0x68F7C804	pub/sec	1024/1792	DSA/ELG	[] Ultimate	2006-02-14

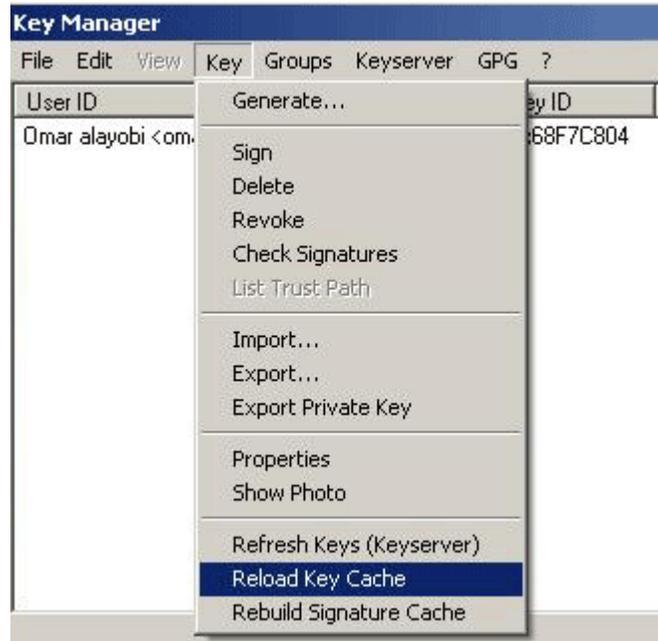
للحصول على المفتاح العام, يقوم Omar بالضغط على key - import كما هو موضح.



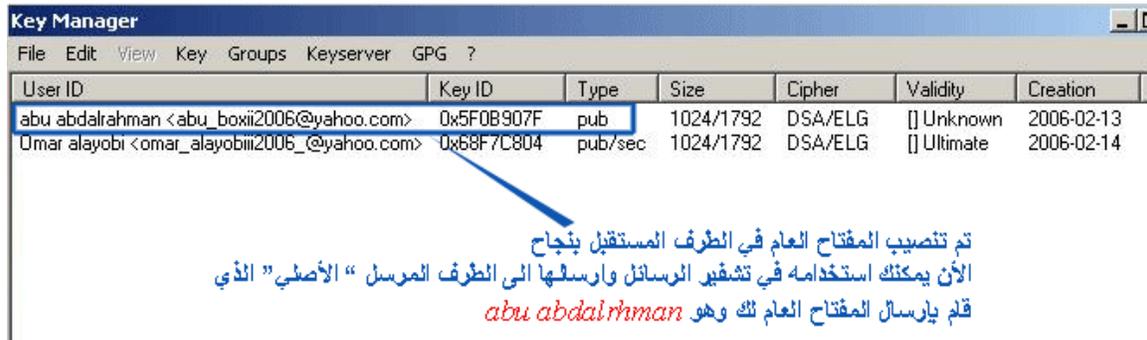
اختر المفتاح بعد ذلك open.



لتفعيل المفتاح يجب عمل refresh كما هو موضح.



المفتاح العام الخاص ب abd abdalrahman



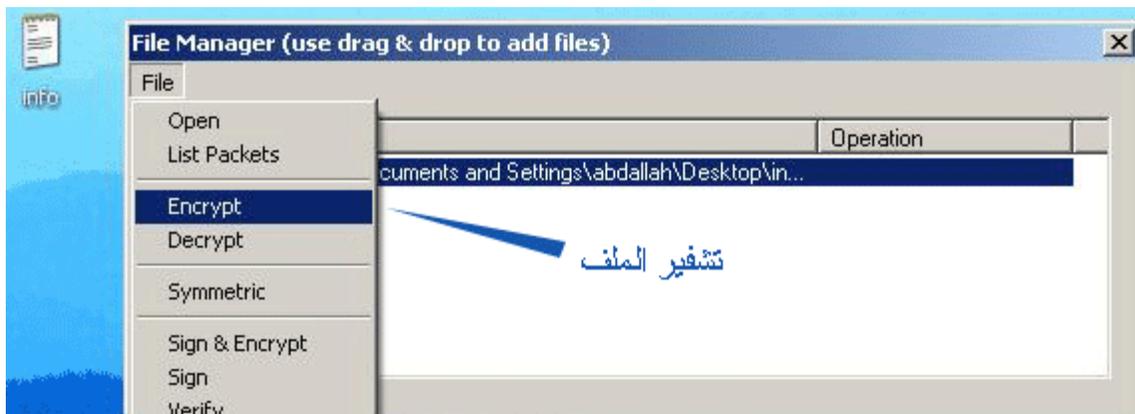
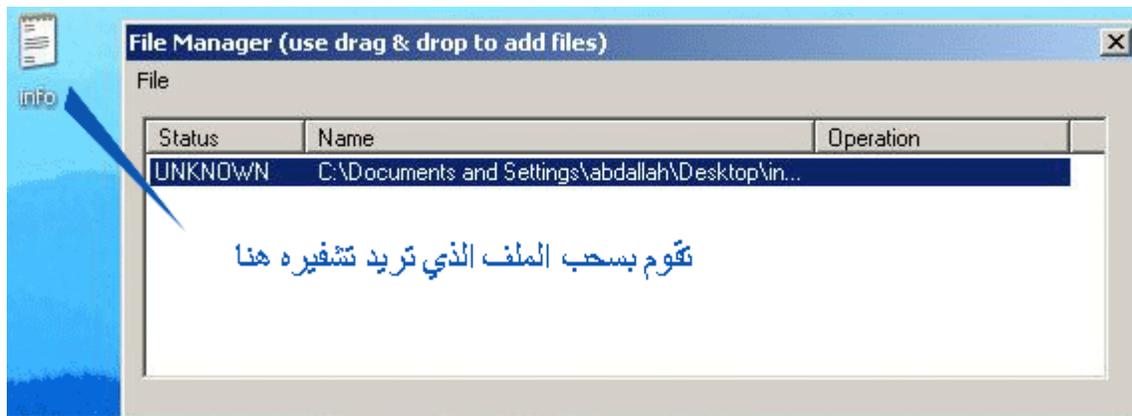
Omar قام بكتابة رسالة الى abu abdalrhman وحفظ هذه الرسالة على شكل info.txt وسيقوم بتشفيرها عن طريق استخدام المفتاح العام الخاص ب abu abdalrahman

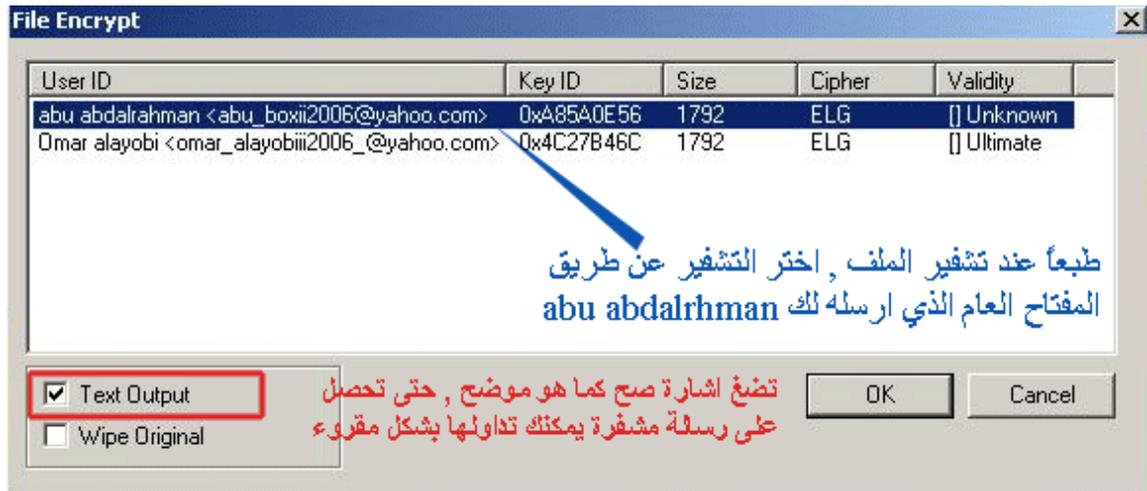


لتشفير الرسالة اذهب الى File Manager

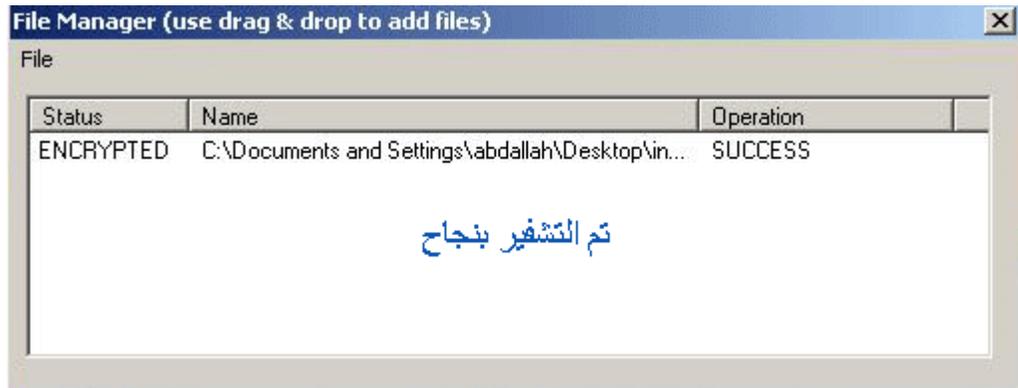
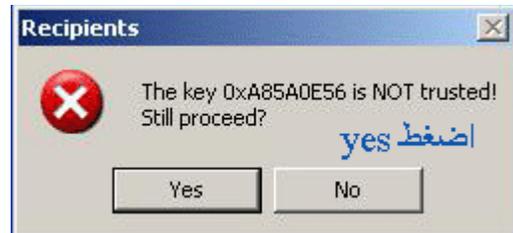


كما هو موضح

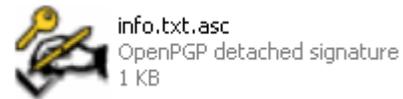




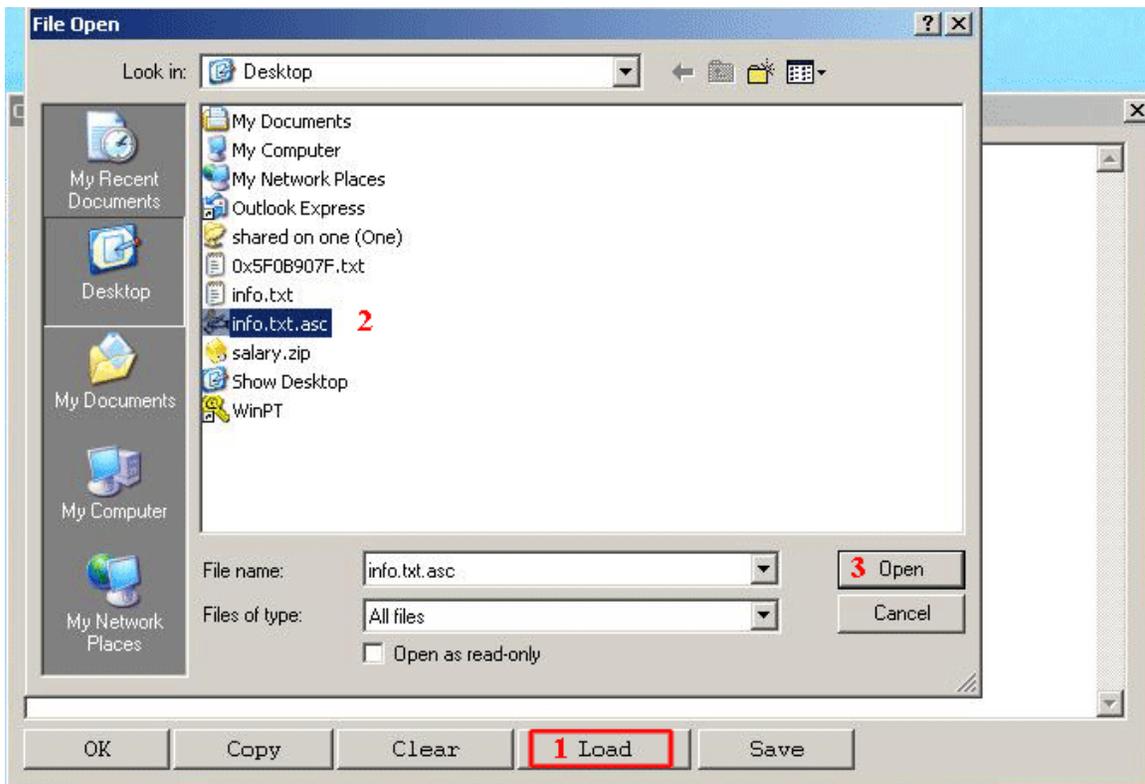
ايضاً عند التشفير, سيطلب منك البرنامج ادخال كلمة السر الخاصة بك, لإتمام عملية التشفير.



يكون شكل الملف المشفر :



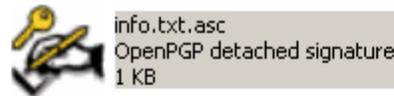
يمكنك فتحه عن طريق ال notepad , او عن طريق الخطوات التالية :





الطرف المرسل "الذي قام بإرسال المفتاح العام :-"

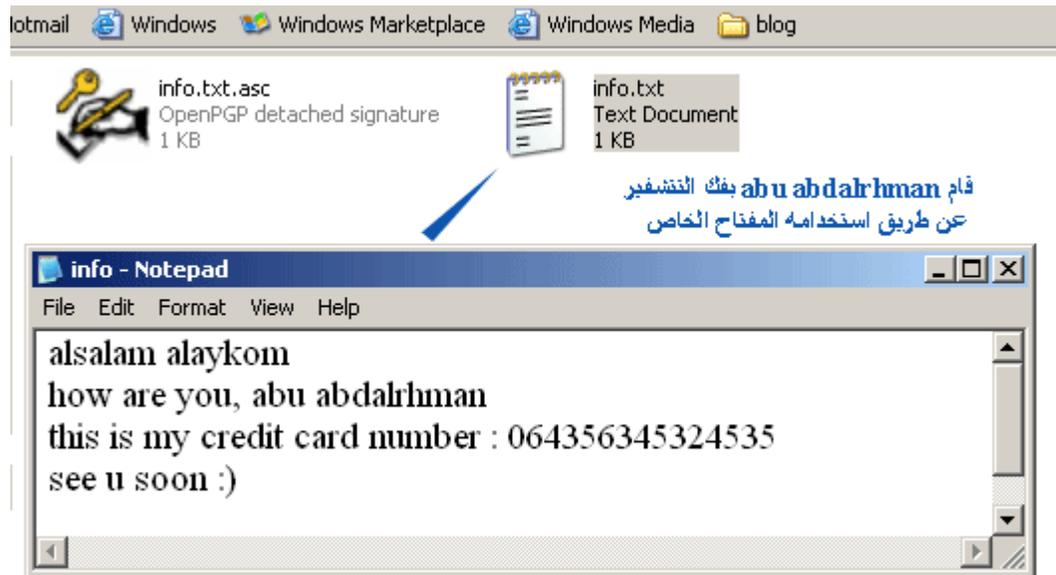
بعد استلام الرسالة المشفرة ...



الملف المشفر
الذي أرسله
omar

يمكنك الضغط على الملف ، ستظهر لك شاشة فك التشفير الخاص ب abu abdalrhman عن طريق ادخال كلمة الأسر (المفتاح الخاص).



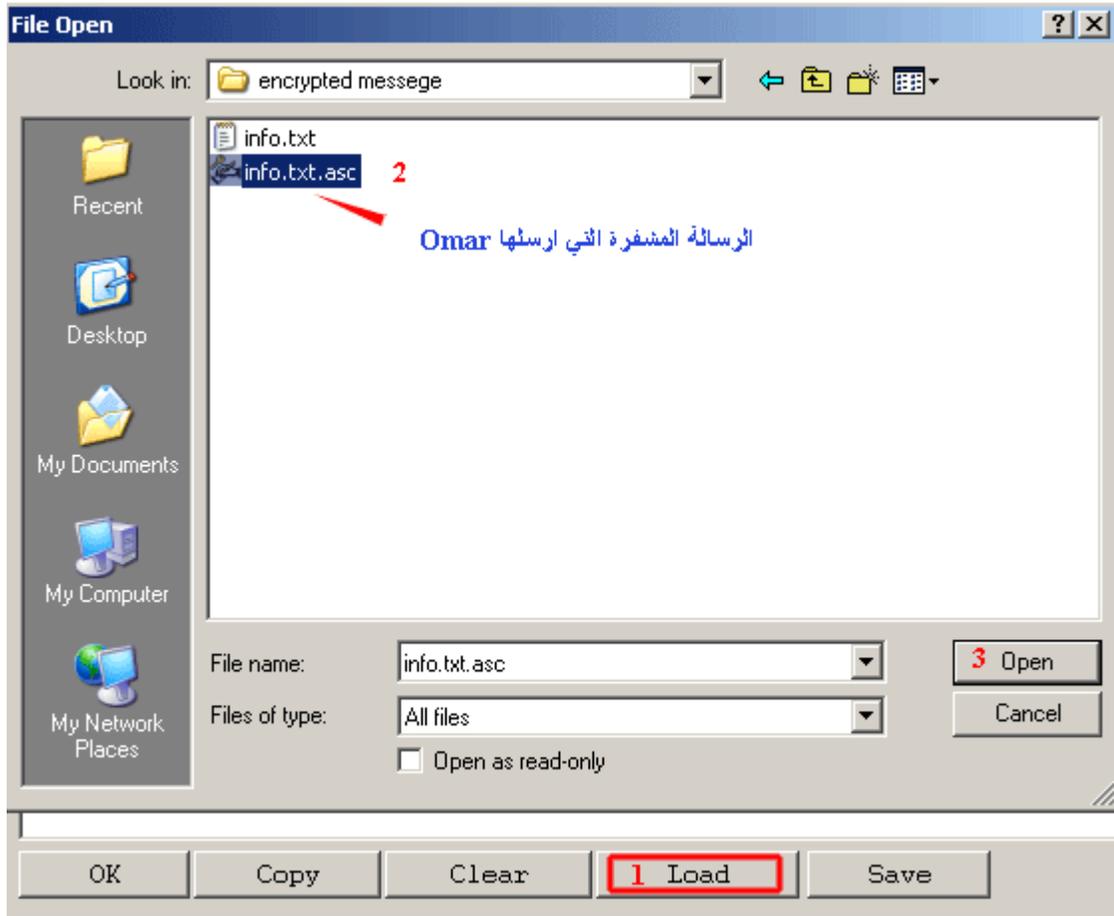


طريقة اخرى لفك التشفير :

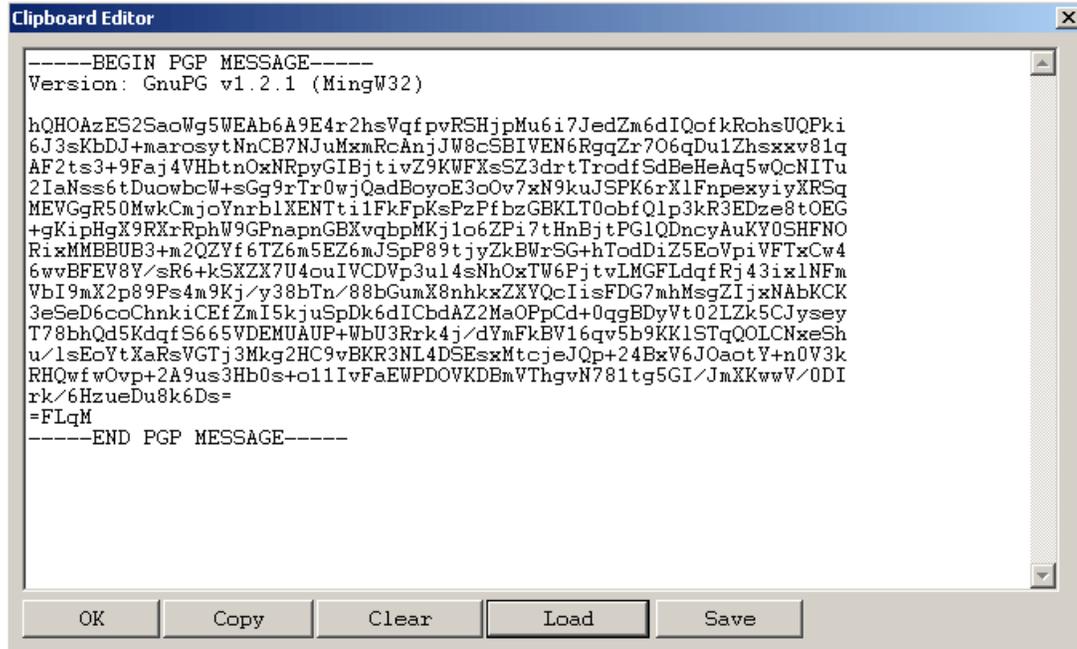
الذهاب الى file manager ومن ثم تقوم بسحب الملف المشفر وبعد ذلك تضغط على .decrypt



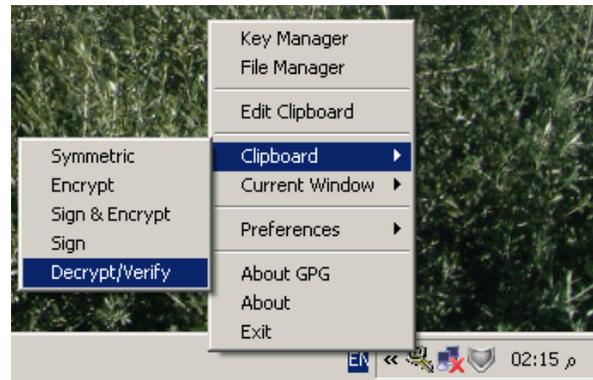
او تذهب الى Edit Clipboard ومن ثم تضغط على load .



ستظهر لك الرسالة المشفرة : بعد ذلك قم بإغلاق المحرر (Clipboard Editor).



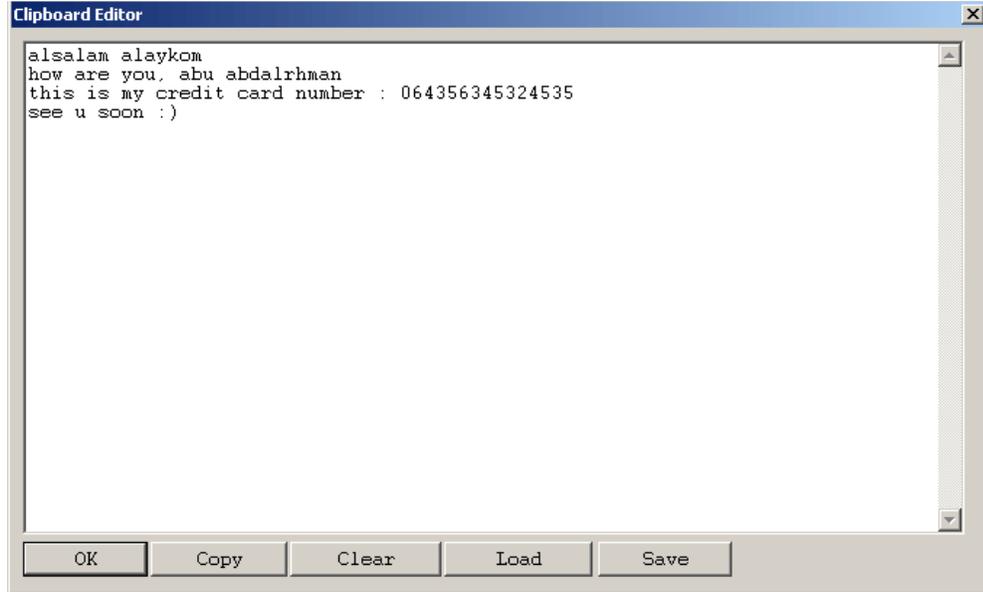
ومن ثم اذهب الى Clipboard ثم Decrypt/Verify ليقوم بعملية فك التشفير للرسالة.



قم بإدخال كلمة السر (المفتاح الخاص).



بعد ذلك اذهب الى Clipboard Editor لترى الرسالة بعد فك التشفير.



هذا بشكل عام ملخص لعملية التداول بالمفتاح العام , توجد اكثر من طريقة لقراءة الملف المشفر وعرضه كما سبق شرحه.

المرحلة الثانية: Digital Signatures

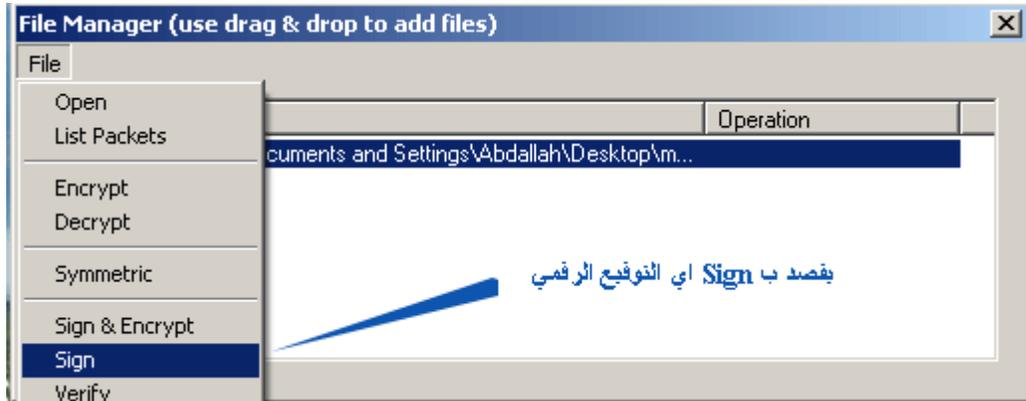
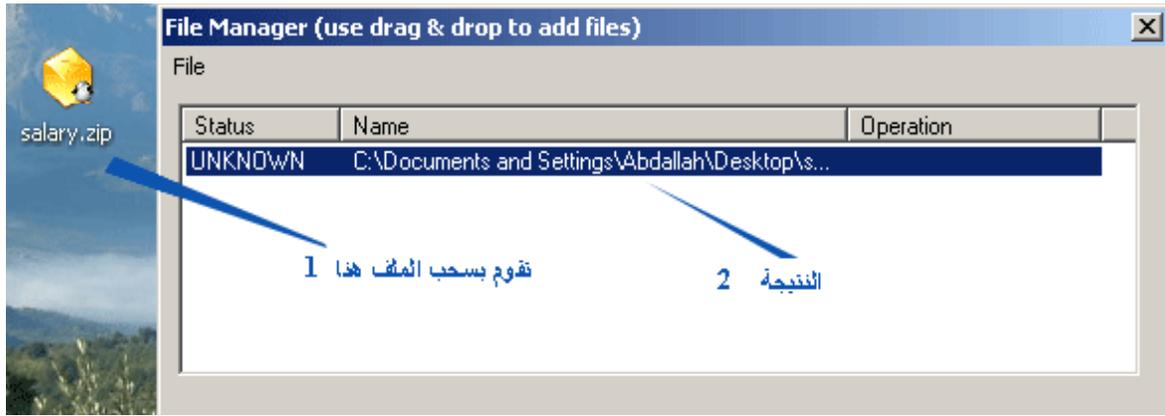
على فرض ان abu abdalrhman قام بإرسال ملف مضغوط الى Omar , كيف ل Omar ان يتأكد من أن الملف قد جاء من مصدره, دون ان يتعرض لأي تغيير أثناء عملية النقل .

هنا يتم استخدام التوقيع الرقمي, الخطوات بسيطة :

الملف الذي سيتم ارسالها الى Omar :



اذهب الى File Manager كما في الصورة:



النتيجة :



الآن تقوم بإرسال الملف المضغوط الى Omar وأيضاً قم بإرسال التوقيع الرقمي الى Omar.

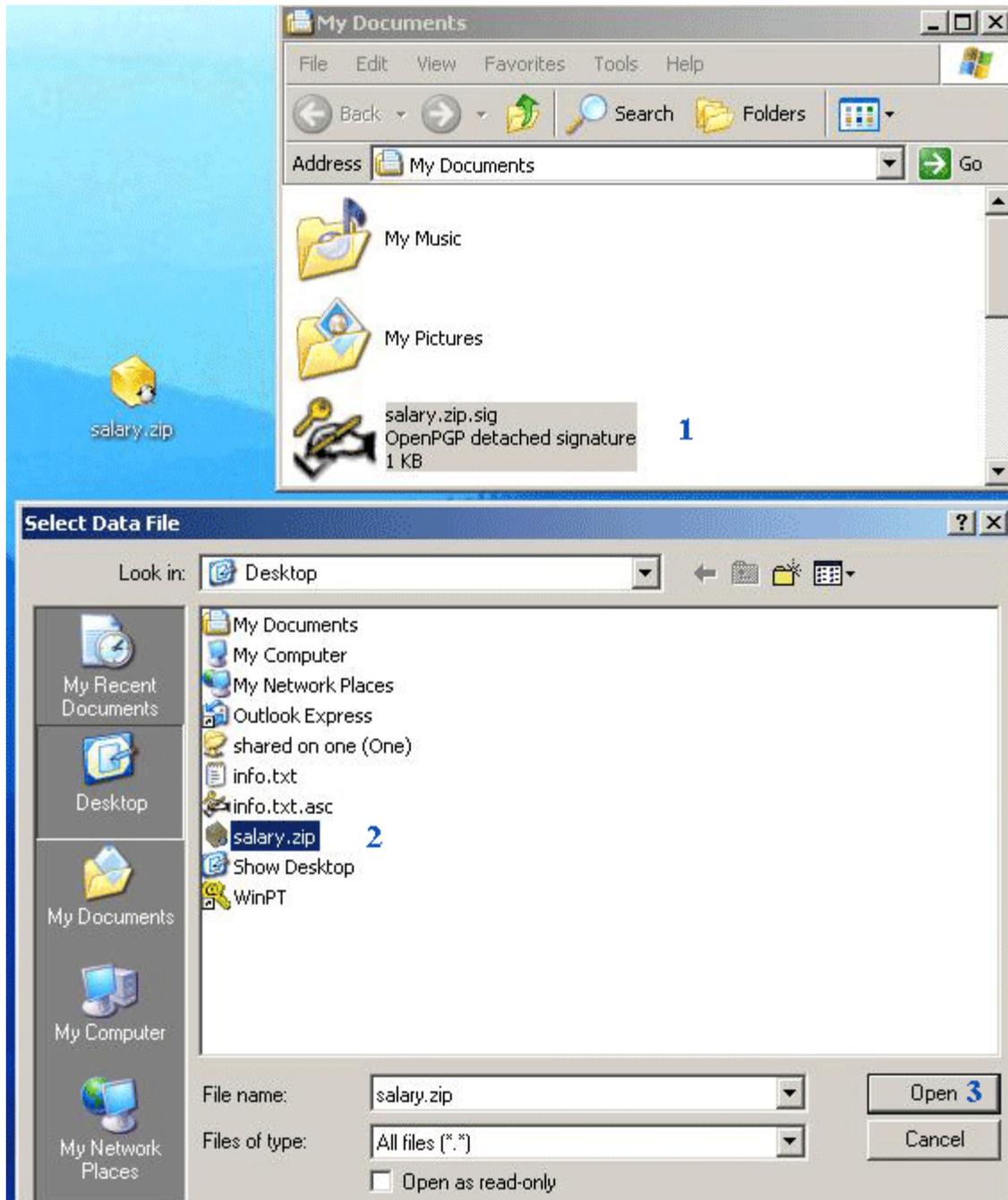
قام Omar بحفظ الملف والتوقيع الرقمي على جهازه, كما يلي :



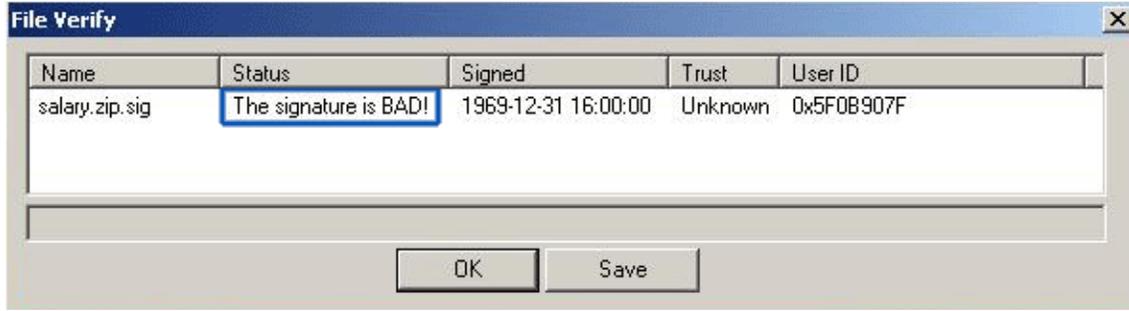
في حالة ان التوقيع الرقمي والملف في نفس المسار , فقط قم بالضغط على salary.zip.sig , اذا كانت الملف هو الملف الحقيقي والذي لم يتعرض لأي تغيير اثناء النقل , فإنه ستظهر لك هذه الرسالة:



في حالة ان الملف والتوقيع في مسارين مختلفين , فإن التوقيع الرقمي يطلب منك تحديد مسار الملف, لكي يقوم بالتأكد من سلامته :



في حالة ان الملف ليس سليم, او تعرض للتغيير اثناء عملية النقل , ستظهر لك هذه الرسالة:



توجد طرق اخرى تعمل كعمل التوقيعي الرقمي وهي ال Hash function مثال على ذلك .MD5

المرحلة الثالثة: Digital Certificates

الشهادة الرقمية: كيف يمكن للمستقبل الذي يقوم بتشفير الرسالة عن طريق استخدام المفتاح العام من التأكد بأن الرسالة المشفرة , تم تشفيرها فعلاً عن طريق استخدام المفتاح العمومي الذي تم ارساله عن طريق المرسل الأصلي (الهدف من الشهادة الرقمية التأكد من سلامة المفتاح العام والمالك الحقيقي له).

الشهادة الرقمية تحتوي على:

- 1- المفتاح العام "public key".
- 2- معلومات عن المفتاح العام: مثل (إسم المرسل, الكنية, رقم المرسل, عنوان البريد ...).
- 3- التوقيع الرقمي الخاص بالمفتاح, وهو سيكون بمثابة البصمة الرقمية (Fingerprint).

الخطوات :

- 1- اضافة User ID

في هذه الخطوة سيتم إضافة رقم مستخدم جديد بالإضافة إلى اسم **abu abdalrhaman** الهدف من هذه العملية إعطاء معلومات إضافية عن **abu abdalrahman** مثلاً: إذا كان عنده بريد إلكتروني آخر يستعمله, أو له كنية معينة, أو تعليق خاص به حتى نتأكد من أن المفتاح العام هو فعلاً من **abu abdarhman** سيتم إضافة كل هذه المعلومات ضمن المفتاح العام الذي سيرسله إلى Omar

Validity	Name	Status
Unknown	abu abdalrahman <abu_boxii2006@yah...	Useable

Buttons: OK, Add, Delete, Revoke

تلاحظ ان **abu abdalrhaman** له لقب اخر وهو **khattab alromi**, ونفس البريد وتعليق خاص به, بعد ان قام بإضافتهم.

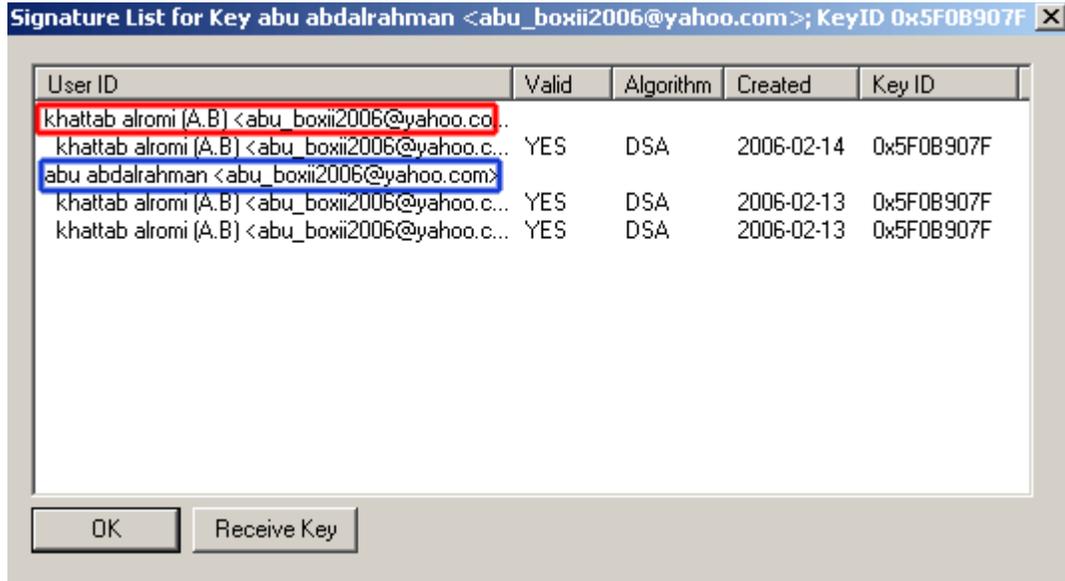
Name: khattab alromi
 Email: abu_boxii2006@yahoc
 Comment: A.B

Buttons: OK, Cancel

بعد الإنتهاء من إضافة الكنية أو الاسم, تضغط على **Check Signatures** لإظهار معلومات التوقيع الخاص بالمفتاح.

النتيجة: طبعاً قم بإرسال المفتاح العام, وعند الطرف المستقبل (Omar) يستطيع التأكد من هذه المعلومات عن طريق الضغط على key - Check Signatures بعد القيام بالضغط على

import للمفتاح العام الذي ارسله abu abdalrahman.



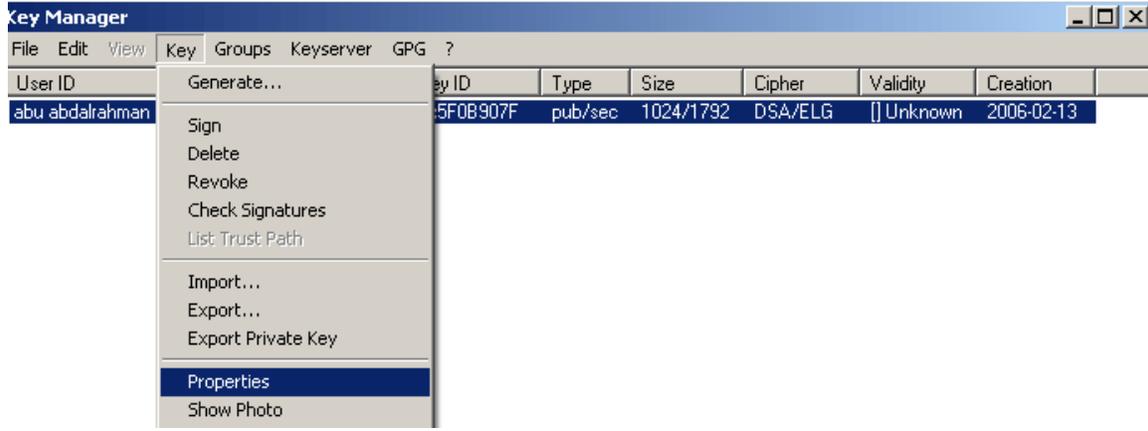
بقيت خطوة اخيره, وهي ارسال البصمة الرقمية لزيادة التثيت من ان المفتاح العام هو المفتاح الحقيقي الذي ارسله abu abdalrahman

بعد ان قمنا بإرسال المفتاح العام ل Omar يجب ان نرسل له البصمة الرقمية بشكل مستقل , إما عن طريق الشات مثلاً او البريد , او اي وسيلة تراهما مناسبة.

للحصول على البصمة الرقمية , هي عبارة عن كود خاص بالمفتاح :

اضغط على Key Manager.

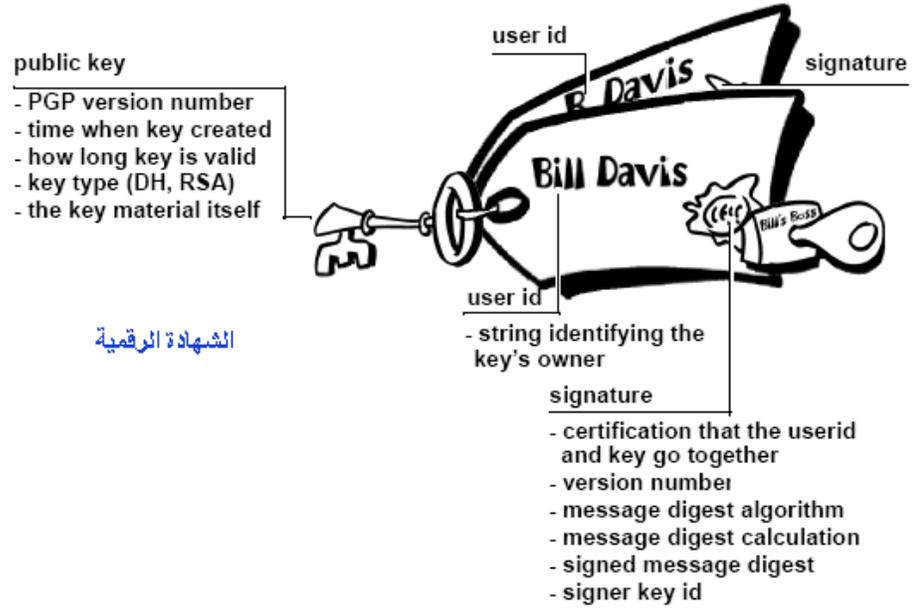




إذا لم تتطابق, هذا يدل على ان المفتاح العام قد تم تغييره , او انه ليس المفتاح الحقيقي الخاص بـ abu abdalrahman

طبعاً, يمكنك ارسال معلومات اخرى مثلًا Algorithm, Created, Key ID لـ Omar لزيادة الثبوت.

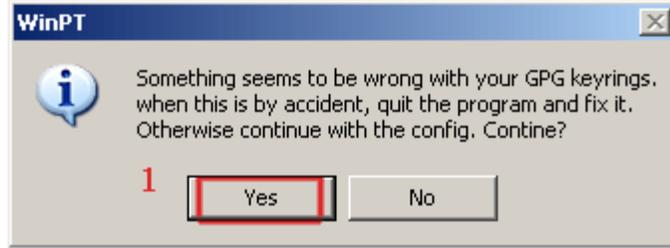
ملخص للمعلومات التي تحتويها الشهادة الرقمية :



إسترجاع النسخ الإحتياطية من المفاتيح:

في حالة عمل فورمات للجهاز او حدوث اية مشاكل, يمكنك بعد تنصيب البرنامج , استرجاع المفاتيح الخاص والعام كما يلي :

1- عندما يطلب منك البرنامج تنصيب المفاتيح, تقوم بإختيار المجلد الذي يحتوي على النسخ الإحتياطية للمفاتيح.

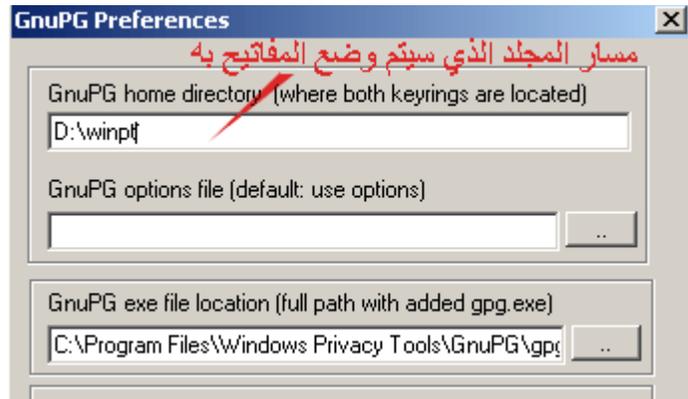


2- يجب استرجاع المفاتيح العام اولاً لأنه يقوم بوضعه في مخزن المفاتيح العام والخاص في مخزن المفاتيح الخاص بالترتيب.



قد تواجهك مشاكل اخرى في حالة استدعاء المفاتيح بطريقة غير صحيحة, لذلك قم بالتأكد من ان مسار تخزين المفاتيح التي سيستخدمها البرنامج صحيحة .

3- مسار المجلد الذي تم تحديده مسبقاً في المرة الأولى عند تنصيب البرنامج, راجع الشرح.



بقيت بعض الأمور :

مثل ال keyserver: وهي عبارة عن سيرفرات تقوم بإستضافة المفاتيح العامة, فيمكن للشخص تحميل المفتاح العام الخاص به على ذلك السيرفر, بحيث ان اي احد يريد الإتصال به يمكنه البحث عن المفتاح العام من تلك السيرفرات, عن طريق ادخال مثلاً عنوان البريد الخاص بالمرسل (صاحب المفتاح العام).

اما بالنسبة لخاصية Revoke: فهي تعني الغاء عمل المفتاح العام, على فرض انك ارسلت المفتاح العام الى اصدقائك او الى السيرفر وتريد الغاء ذلك المفتاح بحيث لا احد يستطيع تشفير اي

رسالة بإستخدامه, يمكنك عمل ذلك عن طريق خاصية Revoke وبعد ذلك تقوم بإرسال المفتاح العام من جديد الى السيرفر والأصدقاء .

مشاكل مستقبلية :

قد تواجهك بعض المشاكل في المفتاح العام او الرسالة المشفرة, عند استقبالك لها من الطرف المرسل عن طريق البريد او رسائل المنتدى مثلاً تحصل هذه المشكلة عندما تقوم بنسخ المفتاح العام وتضعه في ملف txt , بحيث انك عندما تعمل import للمفتاح , تظهر رسالة من البرنامج تخبرك ان المفتاح العام خطأ, او لا يتعرف البرنامج عليه.

ملاحظة: يمكنك وضع الرسالة او المفتاح العام داخل code في حالة التعامل مع المنتديات

1- احرص على وجود مسافة بين المقدمة والرسالة المشفرة او المفتاح العام :

```
New Text Document.txt - Notepad
File Edit Format View Help
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.2.1 (MingW32)
hQHOAzUekRKwtmDREAb/VIAul5tQjxSgT5WMBFo'
KOUgyJvCO1hlieuXzBLG76PLAJFZvL555xurt+thr3354
mMCvBsMzZ0XQpjuUr2lQ69tfiOq80tABjN9dIVfMa4l
746UNc5Xon9rF6D9YNtpsqt0uYjPBjosMcZvSqfKdL
KyZivRFZTVC3q3+QARXBRSX+LzWTI7XngfYXVf
/20Tis1n4hiaeNr7mT46hbDind4QwTIDmrtF7QOm4n
```

احرص على ان تكون
هناك مسافة بين
المقدمة والرسالة

2- عند ارسال المفتاح عن طريق البريد الالكتروني قد يتأثر بكود ال html بحيث انه تصبح هناك مسافات بين الأحرف المشفرة, هذه اغلب المشاكل التي ستواجهها, نفس الشيء للرسالة المشفرة, مثال توضيحي:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.2.1 (MingW32)
mQGibEQXQVcRBACUHQOhTEcL23/sr28RN4NTVmJSIElkBzQREPEFaEAcAKHQ9I
GgXC5TozoLhNxtQeMaSHZEao/bhp17UXu+/Pe8ft/51xvlHtK9LQHDrYIMXmZjm
MgzARiObv6vni6sXfrWiW6ZAEqh0gg5LYSt7ZdL6DbmsZIKwY4 8ar69bYwCg5M5H
+jp1Tx3II+CELkBzQREPEFaEAcAsU4qbjgios9A4OcpKErYHwC mgqqgGLifotRka
UjrH8PNDe1GBarnM2gqhbEeDVcGz/diRwYk3f5lyZjNmVvpZ8R87I7il4kfrf
VyUxhjn2ABM3sSbROARnmC91TRx3wMIMBLFGMsblx+Aw7hmO7Hm BLEi5PTFFpraC
drCEA/0da0GvIU7arcTY9BGDurwsJl5AsqHNesJ5m2gTDbTJRAlOGsZg qB57kVP
iLOOrNgCgELkBzQREPEFaEAcAKqx6MXL4CqWovFk5f2d0t62MbC GCh8h8rPE6mn8c
bYer/Uc3WWaOoKA5GqekX7laEccHf0Y4KVDg1Pq4GWR44HRbOYamF iaGEgPGph
YmhhQGphYmhhLmluZm8+ifkEEeCACABkFAkQ8QVcECwcDagMVAg MDFgIBAh4BAheA
AAoJEFWk6N68YB5D5BdAAoJBeCPK8umTVTu9qNwHsIV8IKLlAJ 9eT1uZNUuUZr/r
h5p9vMBLFGMsblx+Aw7aEAcA8wGUmARFBSICavx1srwYE+ qGaeakV4LlcbUk
XTqtW1kLMPmjuQCv9rHRjgm+qll9iTMP1euWbwqzocb7rimoZg HQ9Ffhs2THA7y7
uJ8+YI93UE1ycvRCwo5epuIo8RFsFEr27JsczSVgln3SDkme/iEuaOgOWI5DKUMh
6AM7DwcOwuLX1dzbbHiBsU5mM+KSUFhQgWSAbVKptq1233b9/6mBazzATpDIws22
zVfzRKJ7qSMQzPlixob4YB/1zBHp4Qq8x17mewFTI1BB1xfuEPP78TPUmMfTc1T
LpqqjdsAAwUHAJwylimfYr+YycAcdv9P18I9D+QmKyua/TwxyE70Skyuf19lg/
/MyiS0MByGcELkBzQREPEFaEAcAKyPKi0eNAMBo6s07LAjs+QWlr hTuOs2SBu/E3t
JLNkMBLFGMsblx+Aw7RC/mr1TKDFbatFjgU7Jks3cKxxiSfk5EwJ6anPBg0y
NkCNusYDSC1onKx0VWZaiSGeCUXsRwVtjzcp1F2BZhh6DCValEvqkvBlxf0Y6BP
7HWY7BKnrKKcocUMaFN3jHQZHC7yoo95Q4Qiwmx6LZXvGkxpl Tmv7TJiEYEGBEC
AAyFMBLFGMsblx+F+Aw7To3rxgHkPlcdQELkBzQREPEFaEAcADTDNIQ akwUEPqrciwF
KYu0ZEI6+a/Fs0pbTEp7/c8w
=MfCz
-----END PGP PUBLIC KEY BLOCK-----
```

تقريباً المسار الموضح توجد فراغات بين الأحرف

GIMF

توجد اكثر من طريقة لحل هذه المشكلة , منها ارسال المفتاح العام او الرسالة المشفرة بملف مرفق, او ازالة الفراغات .

تلاحظ التالي في الرسالة او المفتاح المرسل:



يجب ان تكون الرسالة, او المفتاح العام لا يحتوي على فراغات بين الأحرف المشفرة , لذلك عند ظهور مثل هذه المشكلة , قم بإزالة الفراغات وتأكد من ان جميع الفراغات قد تم ازالتها, يمكن عمل ذلك عن طريق نسخ المفتاح العام او الرسالة المشفرة ووضعها في ال notepad ومن ثم تذهب الى edit >> replace , تقوم بضغط زر مسافة space في خانة find what وتترك خانة replace with فارغة , ومن ثم تضغط على find next حتى تصل للفراغات وتقوم بعمل replace وهكذا. ولكن لا تقوم بإزالة الفراغات الموجودة في مقدمة ونهاية الرسالة او المفتاح العام, اقصد بذلك :

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v1.2.1 MingW32

لا تنسوننا من صالح دعائكم

-----END PGP PUBLIC KEY BLOCK-----

الجهة الإعلامية الإسلامية العالمية

Global Islamic Media Front