



التشفير

الهدف العام من المقرر

يهدف هذا المقرر إلى إكساب المتدرب مهارات التعرف إلى مفاهيم التشفير والتوقيع الرقمي والمصادقة والتراخيص.

الأهداف التفصيلية للمقرر : أن يكون المتدرب قادراً على ان:

- تعلم كيفية حماية البيانات والمعلومات الحيوية باستخدام التشفير.
- فهم مفاهيم التشفير والتوقيع الرقمي والمصادقة والتراخيص.
- فهم مفاهيم أمن الشبكات والأمن في الحوسبة السحابية.
- التعرف على أنواع التشفير والأساليب المستخدمة.
- مقدمة في التشفير والتوقيع الرقمي والمصادقة والتراخيص.
- أنواع التشفير والأساليب المستخدمة فيها.

مقدمة

تعتبر مادة التشفير من الفروع الحيوية في علوم الحاسوب، حيث تهتم بدراسة تقنيات حماية المعلومات وتحويلها إلى صيغ غير قابلة للقراءة للأفراد غير المخولين. يعود تاريخ التشفير إلى فترات قديمة حيث استخدمت لحماية الرسائل السرية. في العصر الحديث، أصبحت هذه المادة أساسية في ضمان أمان البيانات عبر الشبكات والاتصالات. تشمل التقنيات المستخدمة العديد من الخوارزميات والمفاهيم الرياضية، مما يجعلها مجالاً معقداً ومثيراً للاهتمام لمهندسي الحاسوب وأمن المعلومات.

| | |
|----|---|
| 5 | مقدمة في التشفير و التوقيع الرقمي و المصادقة و التراخيص |
| 7 | فهم مفهوم التشفير و أنواعه |
| 9 | فهم مفهوم التوقيع الرقمي و أهميته |
| 11 | فهم مفهوم المصادقة و أنواعه |
| 11 | فهم مفهوم التراخيص و أنواعها |
| 12 | تطبيق تقنيات التشفير و التوقيع الرقمي و المصادقة و التراخيص التوافق مع الفرق المختلفة المعنية بالأمنالسيبراني |
| 20 | أنواع التشفير والأساليب المستخدمة فيها |
| 21 | التعرف على أنواع التشفير |
| 22 | فهم مفهوم المفاتيح و أنواعها |
| 24 | فهم مفهوم الهجمات على التشفير |
| 25 | تطبيق أساليب التشفير |
| 41 | أمن الشبكات و الأمن في الحوسبة السحابية |
| 41 | فهم مفهوم أمن الشبكات |
| 42 | تحليل المخاطر و تقييم الضعف في الشبكات |
| 44 | تطبيق تقنيات الحماية في الشبكات |
| 45 | فهم مفهوم الحوسبة السحابية |
| 48 | تحديد المخاطر الأمنية في الحوسبة السحابية |
| 48 | تطبيق تقنيات الأمان في الحوسبة السحابية |
| 52 | حماية البيانات و المعلومات الحيوية باستخدام التشفير و التوقيع الرقمي |
| 53 | فهم مفهوم حماية البيانات و المعلومات الحيوية |
| 53 | فهم مفهوم التشفير و التوقيع الرقمي |
| 54 | تطبيق تقنيات التشفير و التوقيع الرقمي |
| 58 | فهم مفهوم الهجمات على التشفير و التوقيع الرقمي |
| 59 | تطبيق أساليب حماية البيانات و المعلومات الحيوية |
| 62 | دراسة أمن المعلومات و أساليب الهجوم السيبراني |
| 62 | فهم مفهوم أمن المعلومات |
| 63 | فهم مفهوم الهجوم السيبراني |
| 64 | تحليل المخاطر و التقييم الأمني |
| 66 | تطبيق تقنيات الحماية |
| 67 | تحليل الهجمات السيبرانية |
| 70 | تطبيق أساليب الوقاية و التدريب |
| 73 | الدفاع عن المعلومات و أساليب الحماية السيبرانية |
| 73 | فهم مفهوم الدفاع عن المعلومات |
| 75 | فهم مفهوم الأمان السيبراني |
| 75 | تحليل المخاطر و التقييم الأمني |
| 77 | تطبيق تقنيات الحماية |
| 77 | تطبيق أساليب الوقاية و الاستجابة |
| 78 | تحليل الهجمات السيبرانية |
| 80 | مشروع بحثي يستخدم فيه الطلاب مهارات التشفير و التوقيع الرقمي و الحماية السيبرانية التي تم تعلمها في المقرر |



الوحدة الاولى

مقدمة في التشفير و التوقيع الرقمي و المصادقة و التراخيص.

- فهم مفهوم التشفير و أنواعه.
- فهم مفهوم التوقيع الرقمي و أهميته.
- فهم مفهوم المصادقة و أنواعه.
- فهم مفهوم التراخيص و أنواعها
- تطبيق تقنيات التشفير و التوقيع الرقمي و المصادقة و التراخيص التواصل مع الفرق المختلفة المعنية بالأمن السيبراني.

مقدمة في التشفير و التوقيع الرقمي و المصادقة و التراخيص

• مقدمة في التشفير

يحظى التشفير بمكانة خاصة في علوم أمن المعلومات، فهو قلب أمن المعلومات لما يوفره من سرية لها. فاستخدم التشفير عبر التاريخ لتبادل رسائل لا يمكن قراءتها من قبل أي كان ما عدا الشخص المقصود لتلقي الرسالة.

توسعت تكنولوجيا التشفير الرقمية لتتجاوز الرسائل السرية البسيطة؛ فيمكن استخدام التشفير لأغراض أكثر تعقيداً، مثل التحقق من كاتب الرسائل أو تصفح الإنترنت بشكل مجهول الهوية باستخدام شبكة تور Tor. ففي ظروف معينة، يمكن أن يكون التشفير أوتوماتيكياً وبسيطاً.

• التوقيع الرقمي:

هو طريقة لإضافة توقيع إلكتروني إلى وثيقة إلكترونية للتحقق من صحة الوثيقة ومنع التلاعب بها.

يستخدم التوقيع الرقمي في العديد من التطبيقات، مثل التجارة الإلكترونية والخدمات المصرفية الإلكترونية.

• المصادقة:

هي عملية التحقق من هوية المستخدم قبل السماح له بالوصول إلى نظام أو مورد. تُستخدم المصادقة في العديد من التطبيقات، مثل تسجيل الدخول إلى المواقع الإلكترونية وتطبيقات الهاتف المحمول.

• التراخيص:

هي طريقة لمنح المستخدمين أذونات محددة للوصول إلى نظام أو مورد. تُستخدم التراخيص في العديد من التطبيقات، مثل إدارة الوصول إلى الملفات والبرامج.

• أمن المعلومات:

يعرف بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازمة لتوفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية. المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات.

عناصر أمن المعلومات :

1. السرية Confidentiality

2. التكاملية Integrity

3. التوافر Availability

المخاطر التي تهدد أمن المعلومات

الاختراق Hacking وهو نوعان :

1. Hackers

- الاختراق الأولى
- يخترق دون أن يؤدي الشبكة أو الجاهز أو البيانات.
- فقط يراقب ويطلع على المعلومات.
- تعتبر خطوة أولى نحو الاختراق التدميري.
- ممنوع بموجب القانون.

2. Crackers

- يخترق من أجل التخريب
- على النظام.
- يحدث أثرا على النظام.
- يغير على البيانات أو يعطل الأجهزة
- ممنوع بموجب القانون.

طرق الحماية من المخاطر

- التشفير Encryption
- الحماية بالبرمجيات software control
- الحماية بالأجهزة والمعدات hardware control
- السياسات الأمنية security polices
- الحماية التقليدية (الفيزيائية) physical security
- ومن هنا سوف نتعمق اكثر في التشفير Encryption .

فهم مفهوم التشفير و أنواعه

التشفير Cryptography:

عملية تحويل المعلومات من شكل يمكن قراءته وفهمه إلى شكل مشفر لا يمكن فهمه إلا من قبل الأشخاص الذين يملكون مفتاح فك التشفير. يستخدم التشفير لحماية المعلومات السرية من الوصول غير المصرح به.

فك التشفير:

عملية استخدام المفتاح لإعادة النص المشفر إلى صيغته المقروءة الأصلية.

• علم التشفير Cryptography :

1. (Graphy & Crypto) وتعني الكتابة السرية
2. (Cipher) وتعني تشفير مأخوذة عن العربية (صفر أو تصفير) أي جعل القيمة صفراً أي بال معنى.

كيف يعمل التشفير؟

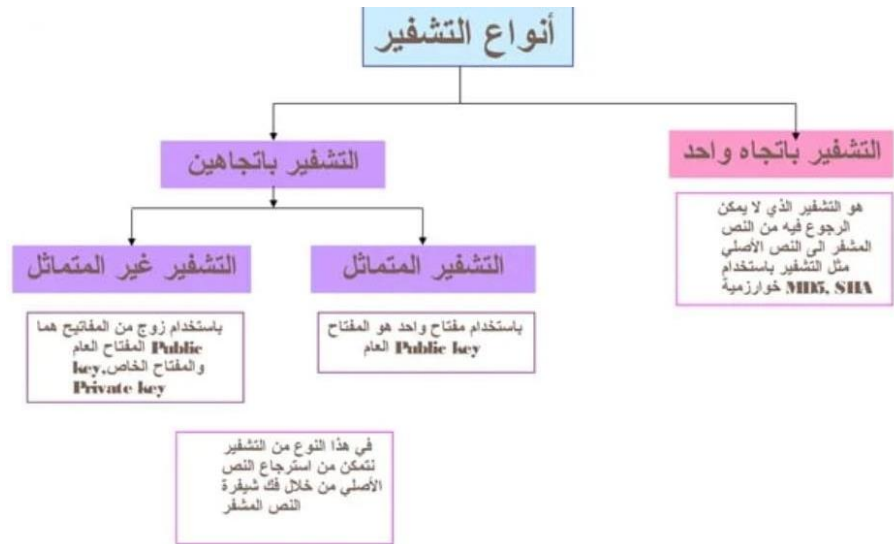
يعتمد التشفير على خوارزمية رياضية لتحويل المعلومات إلى شكل مشفر. تستخدم الخوارزمية مع مفتاح لتشفير المعلومات لا يمكن فك تشفير المعلومات إلا باستخدام نفس المفتاح أو مفتاح فك التشفير المقابل.

ما هي أنواع التشفير؟

التشفير التماثلي: يُستخدم نفس المفتاح لتشفير وفك تشفير المعلومات.
التشفير غير التماثلي: يُستخدم مفتاحان مختلفان، مفتاح تشفير ومفتاح فك تشفير.

ما هي تطبيقات التشفير؟

حماية البيانات: حماية البيانات السرية من الوصول غير المصرح به.
الأمان عبر الإنترنت: تأمين الاتصالات عبر الإنترنت، مثل تصفح الويب والبريد الإلكتروني.
التوقيعات الرقمية: ضمان صحة وسلامة البيانات.
التشفير القابل للبحث: البحث في البيانات المشفرة دون الحاجة إلى فك تشفيرها.



أنواع التشفير:

يمكن تقسيم التشفير إلى ثلاثة أنواع رئيسية:

1. التشفير المتماثل: (Symmetric Encryption)

- يستخدم نفس المفتاح لتشفير وفك تشفير البيانات.
- يتميز بسرعه العاليه وسهولة استخدامه.
- يُستخدم بشكل شائع في تشفير البيانات أثناء نقلها أو تخزينها.
- من أشهر خوارزميات التشفير المتماثل AES و DES و Blowfish.

2. التشفير غير المتماثل: (Asymmetric Encryption)

- يستخدم مفتاحين مختلفين: مفتاح عام ومفتاح خاص.
- يتم استخدام المفتاح العام لتشفير البيانات، بينما يتم استخدام المفتاح الخاص لفك تشفيرها.
- يُستخدم بشكل شائع في التوقيعات الرقمية وتبادل البيانات بشكل آمن.
- من أشهر خوارزميات التشفير غير المتماثل RSA و Elliptic Curve Cryptography (ECC).

3. وظائف التجزئة: (Hash Functions)

- لا تستخدم فيها مفاتيح.
- تُستخدم لحساب قيمة ثابتة تُسمى "التجزئة" من البيانات.
- تُستخدم للتحقق من سلامة البيانات ومنع التلاعب بها.

- من أشهر وظائف التجزئة SHA-1 و SHA-256 و MD5.

أنواع أخرى من التشفير:

- تشفير تيار البيانات (Stream Ciphers): يُستخدم لتشفير البيانات بشكل تدريجي.
- تشفير كتلة البيانات (Block Ciphers): يُستخدم لتشفير البيانات في مجموعات.
- تشفير التشفير (Homomorphic Encryption): يُمكن إجراء العمليات الحسابية على البيانات المشفرة دون الحاجة إلى فك تشفيرها.

اختيار نوع التشفير المناسب:

يعتمد اختيار نوع التشفير المناسب على احتياجاتك ومستوى الأمان المطلوب.

بعض العوامل التي يجب مراعاتها:

- نوع البيانات التي تريد تشفيرها.
- طريقة نقل البيانات أو تخزينها.
- سرعة التشفير وفك التشفير.
- مستوى الأمان المطلوب.

نصائح لاختيار التشفير:

- استخدم خوارزميات تشفير قوية وموثوقة.
 - حافظ على سرية مفاتيح التشفير.
 - استخدم التشفير مع حلول أمان أخرى لضمان أقصى قدر من الحماية.
- ملاحظة: يتطور علم التشفير باستمرار، لذلك من المهم مواكبة أحدث الخوارزميات وأفضل الممارسات.

فهم مفهوم التوقيع الرقمي و أهميته

التوقيع الرقمي Digital Signature ؟

هو آلية تشفير تستخدم للتحقق من صحة وسلامة البيانات الرقمية. قد نعتبرها نسخة رقمية من التواقيع المكتوبة بخط اليد العادية ولكن مع مستويات أعلى من التعقيد والأمان.

بعبارات بسيطة، قد نصف التوقيع الرقمي باعتباره رمزًا مرفقًا برسالة أو مستند. بعد الإنشاء تعمل الشفرة أو الرمز كدليل على أن الرسالة لم يتم العبث بها على طول الطريق من المرسل إلى المتلقي.

أهمية التوقيع الرقمي ومميزاته وصفاته ومكوناته؟

الصفات المميزة للتوقيع الرقمي تشمل:

1. توثيق الموقع: يجب أن يبين أو يشير إلى الشخص الذي قام بتوقيع الوثيقة أو الرسالة أو السجل.
 2. توثيق الوثيقة: يجب أن يعرف عن الطرف الذي قام بتوقيعه بما يجعله غير قابل للتزوير أو التغيير.
 3. الأمان: يضمن التوقيع الرقمي سلامة البيانات ومنع التلاعب بها.
 4. المسؤولية: يمكن ربط التوقيع الرقمي بهوية المرسل، مما يجعله مسؤولاً عن محتوى البيانات.
 5. عدم التكرار: لا يمكن للمرسل إنكار إرسال البيانات بعد التوقيع عليها رقمياً.
 6. الكفاءة: يمكن استخدام التوقيع الرقمي لتسريع العمليات التجارية وتقليل الاعتماد على الوثائق الورقية.
- تعمل تقنية التوقيع الرقمي على تشفير البيانات باستخدام مفاتيح متناظرين، أحدهما سري ويحفظه المستلم، والآخر عمومي. يتم خلق التوقيعات والتثبت من صحتها من خلال التشفير سوف نتعرف أكثر على كل نوع قريباً.

مميزات التوقيع الرقمي؟

1. سهل الاستخدام: يُمكن استخدام التوقيعات الرقمية بسهولة من خلال البرامج والتطبيقات المختلفة.
2. قابل للتطوير: يُمكن استخدام التوقيعات الرقمية مع مختلف أنواع البيانات والوثائق.
3. آمن: يُستخدم التشفير لضمان أمان التوقيعات الرقمية ومنع التلاعب بها.
4. موثوق: يُمكن التحقق من صحة التوقيعات الرقمية بسهولة من قبل أي شخص.

صفات التوقيع الرقمي؟

1. الارتباط: التوقيع مرتبطاً بالبيانات التي تم التوقيع عليها.
2. عدم التكرار: من المستحيل على المرسل إنكار إرسال البيانات بعد التوقيع عليها.
3. التميز: من المستحيل تقليد التوقيع الرقمي لشخص آخر.

مكونات التوقيع الرقمي؟

1. الخوارزمية: هي العملية الحسابية التي يتم استخدامها لتشفير وفك تشفير البيانات.
2. المفتاح الخاص: هو مفتاح سري يستخدم لتشفير البيانات.
3. المفتاح العام: هو مفتاح علني يُستخدم لفك التشفير.

4. الشهادة الرقمية: هي وثيقة إلكترونية تربط المفتاح العام بهوية المرسل.

فهم مفهوم المصادقة وأنواعه

تعريف المصادقة: (Authentication) تُسمى أيضاً "التثبت" و"الاستيقان"، وهو مصطلح شائع في مجال المعلوماتية

المصادقة هي عملية التحقق من هوية المستخدم أو الجهاز للتأكد من أنه مخول بالوصول إلى موارد معينة. تتضمن المصادقة التحقق من البيانات المقدمة، مثل اسم المستخدم وكلمة المرور، أو استخدام تقنيات أخرى مثل البصمة الرقمية أو الرمز الثنائي.

هناك أنواع مختلفة من المصادقة:

1. المصادقة الثنائية: تتطلب اسم مستخدم وكلمة مرور للوصول إلى النظام.
2. المصادقة ذات العوامل المتعددة: تستخدم أكثر من عامل للتحقق، مثل كلمة المرور ورمز الرسالة القصيرة (SMS) أو البصمة.
3. المصادقة الثلاثية العوامل: تستخدم ثلاثة عوامل، مثل كلمة المرور ورمز التطبيق المتنقل والبصمة.
4. المصادقة العمياء: يتم فيها تحديد هوية المستخدم دون الكشف عن تفاصيل محددة، مثل الرصيد أو البيانات الشخصية.

فهم مفهوم التراخيص وأنواعها

التراخيص في مجال التشفير

هي وثائق قانونية تحدد شروط استخدام خوارزميات التشفير وبرامج التشفير. تهدف هذه التراخيص إلى تحقيق التوازن بين ضمان أمن المعلومات وحماية الخصوصية من جهة، ومنع استخدام التشفير لأغراض غير قانونية من جهة أخرى.

أنواع التراخيص في مجال التشفير:

1. التراخيص مفتوحة المصدر: تسمح هذه التراخيص باستخدام خوارزميات وبرامج التشفير بحرية، بما في ذلك التعديل والتوزيع التجاري. من أشهر التراخيص مفتوحة المصدر في مجال التشفير: رخصة GPL ورخصة MIT.
2. التراخيص التجارية: تتطلب هذه التراخيص الحصول على ترخيص من صاحب البرنامج أو الخوارزمية لاستخدامه. تختلف شروط التراخيص التجارية من برنامج إلى آخر، وقد تتضمن رسوماً مالية.
3. التراخيص الحكومية: تضع بعض الحكومات قيوداً على استخدام التشفير، وتتطلب الحصول على ترخيص خاص لاستخدام بعض الخوارزميات وبرامج التشفير.

تطبيق تقنيات التشفير والتوقيع الرقمي والمصادقة والتراخيص التواصل مع الفرق المختلفة المعنية بالأمن السيبراني.

لتطبيق تقنيات التشفير والتوقيع الرقمي والمصادقة والتراخيص القيام ببعض الخطوات :

1. تحديد احتياجاتك ومستوى الأمان المطلوب:

- ما هي البيانات التي تريد حمايتها؟
- ما هو مستوى الأمان الذي تحتاجه؟
- ما هي الميزانية المتاحة لديك؟

2. اختيار التقنيات المناسبة لاحتياجاتك:

- هناك العديد من تقنيات التشفير والتوقيع الرقمي والمصادقة والتراخيص المتاحة.
- يجب عليك اختيار التقنيات التي تلبي احتياجاتك ومستوى الأمان المطلوب.
- 3. تأكد من أن لديك الخبرة اللازمة لتنفيذ هذه التقنيات:

- قد يكون تنفيذ هذه التقنيات معقدًا.

- تأكد من أن لديك الخبرة اللازمة أو استعن بخبير في مجال الأمن السيبراني.

4. التواصل مع الفرق المختلفة المعنية بالأمن السيبراني:

من المهم التواصل مع الفرق المختلفة المعنية بالأمن السيبراني، مثل:

- فريق تكنولوجيا المعلومات: مسؤول عن تنفيذ تقنيات الأمن السيبراني.
- فريق إدارة المخاطر: مسؤول عن تقييم مخاطر الأمن السيبراني.
- فريق الامتثال: مسؤول عن ضمان امتثال المنظمة للقوانين واللوائح المتعلقة بالأمن السيبراني.

أمثلة على تطبيق هذه التقنيات:

- البنوك: تستخدم تقنيات التشفير لحماية البيانات المالية لعملائها.
- المستشفيات: تستخدم تقنيات التشفير لحماية البيانات الطبية للمرضى.
- الحكومات: تستخدم تقنيات التشفير لحماية المعلومات الحساسة.
- الشركات: تستخدم تقنيات التشفير لحماية بياناتها من المنافسين.

فوائد تطبيق هذه التقنيات:

- زيادة مستوى الأمان.

- حماية البيانات والأنظمة من الوصول غير المصرح به.
- ضمان خصوصية المستخدمين.
- تعزيز الثقة في المعاملات الإلكترونية.

عيوب تطبيق هذه التقنيات:

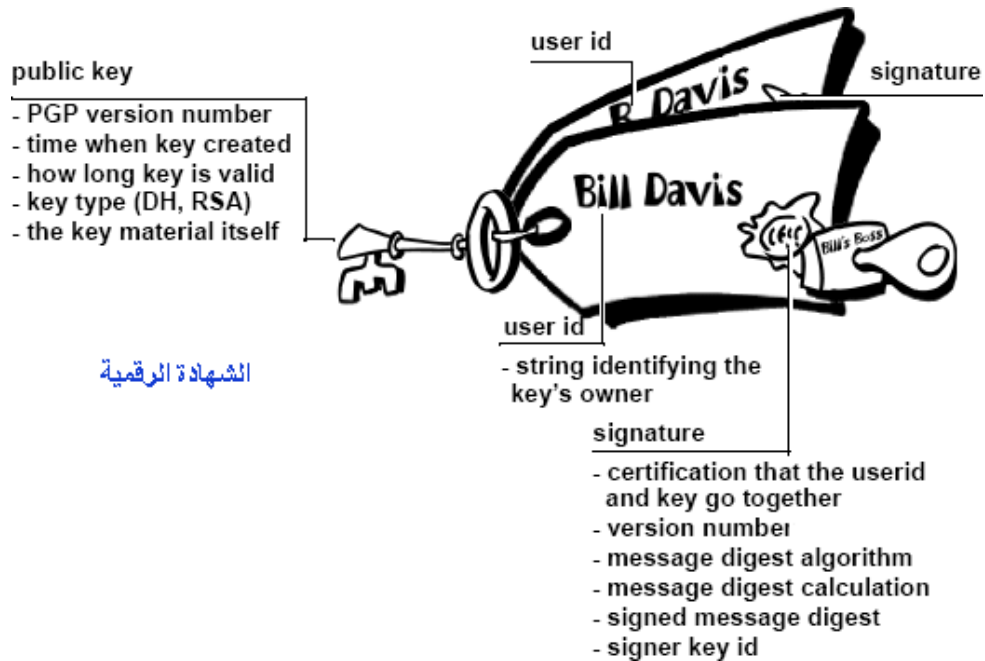
- يمكن أن تكون معقدة للاستخدام.
- يمكن أن تكون عرضة للهجمات.
- يمكن أن تكون مكلفة.

نصائح لتطبيق هذه التقنيات:

- حدد احتياجاتك ومستوى الأمان المطلوب.
- اختر التقنيات المناسبة لاحتياجاتك.
- تأكد من أن لديك الخبرة اللازمة لتنفيذ هذه التقنيات.
- استشر خبيرًا في مجال الأمن السيبراني إذا لم تكن متأكدًا من كيفية تطبيق هذه التقنيات.

الشهادة الرقمية – Digital Certificate

الشهادة الرقمية هي وثيقة إلكترونية تربط بين هوية كيان ما (مثل شخص أو جهاز أو موقع إلكتروني) ومفتاح عام.



مكونات الشهادة الرقمية:

1. المفتاح العام:

هو مفتاح التشفير الذي يمكن استخدامه للتحقق من صحة توقيع الكيان.

2. معلومات عن المفتاح العام:

- اسم المرسل
- الكنية
- رقم المرسل
- عنوان البريد الإلكتروني
- معلومات أخرى

3. التوقيع الرقمي: توقيع رقمي من الجهة المُصدرة للتأكد من صحة الشهادة.

4. معلومات أخرى:

- تاريخ الصلاحية
- الاستخدامات المسموح بها
- معلومات عن الجهة المصدرة

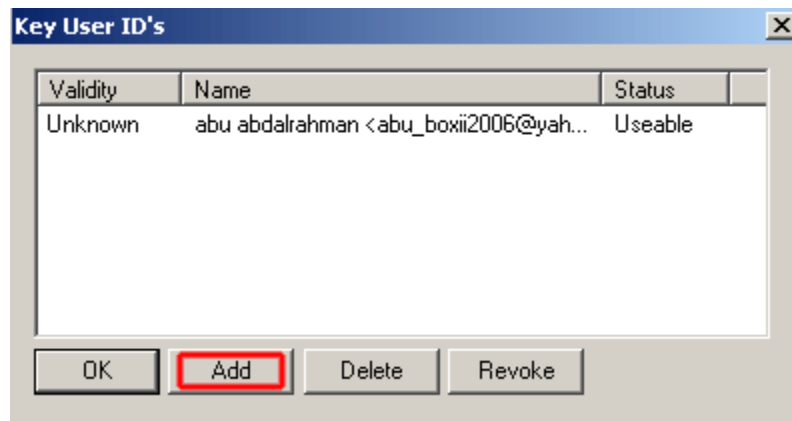
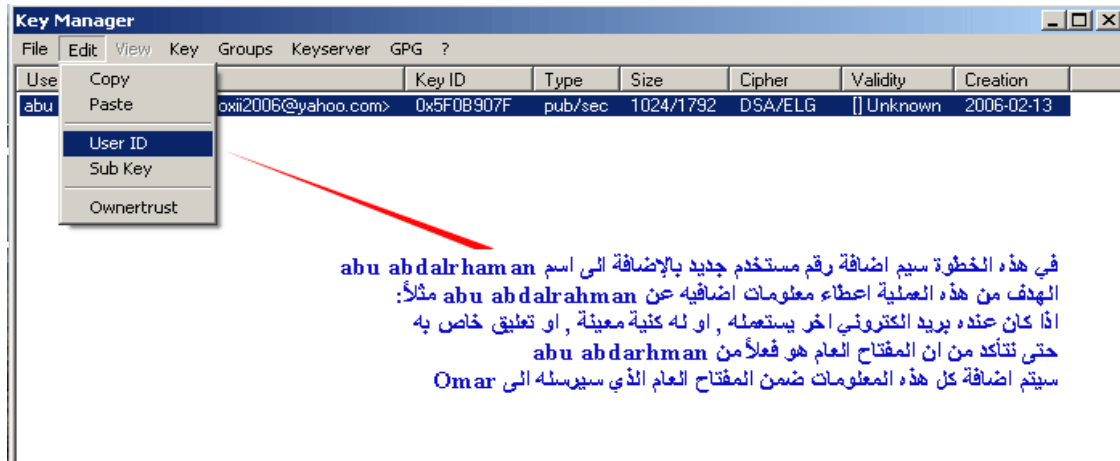
دمج المكونات: يتم دمج جميع هذه المعلومات في ملف واحد، يُعرف باسم الشهادة الرقمية.

استخدام الشهادة الرقمية:

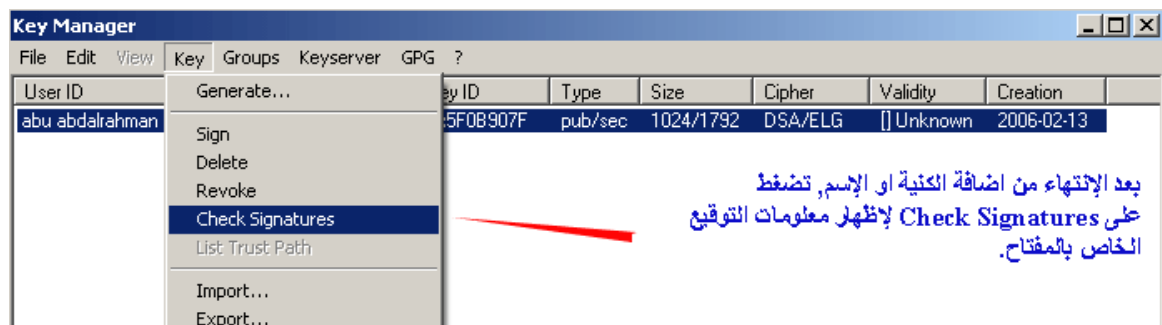
- يتم إرسال الشهادة الرقمية إلى الطرف المستقبل.
- يمكن للطرف المستقبل:
- التأكد من صحة المفتاح العام وخصائصها مثل اسم المرسل.
- فك تشفير البيانات التي تم تشفيرها باستخدام المفتاح العام.
- التحقق من صحة التوقيعات الرقمية التي تم إنشاؤها باستخدام المفتاح الخاص.

حاله عملية :

1- اضافة User ID

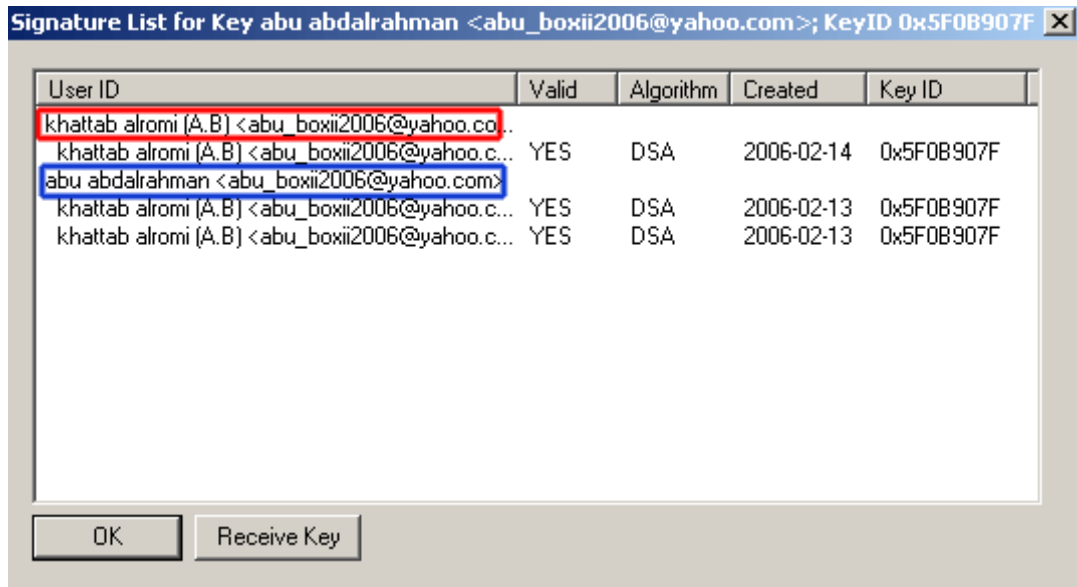


تلاحظ ان abu abdalrhman له لقب اخر وهو khattab alromi، ونفس البريد وتعليق خاص به، بعد ان قام بإضافتهم.



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 أرسله abu abdalrahman.

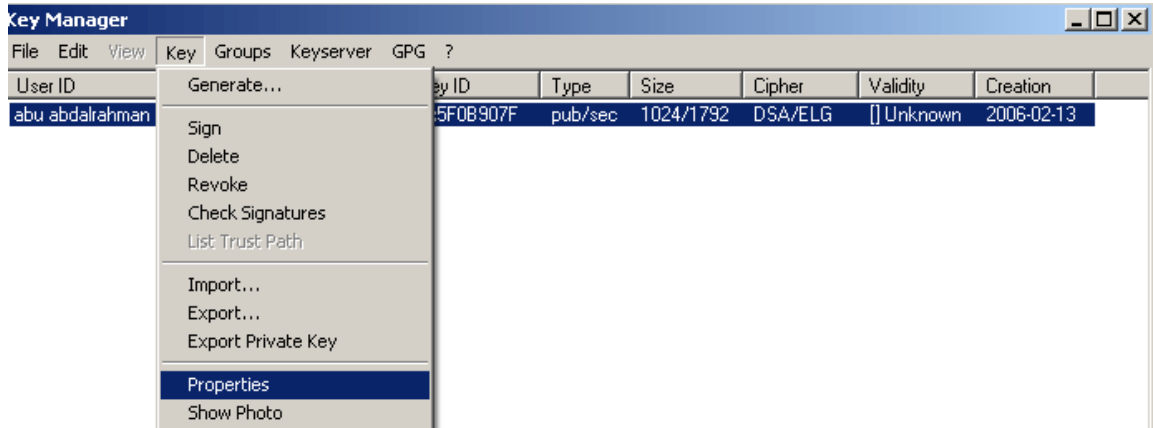


بقيت خطوة اخيره، وهى ارسال البصمة الرقمية لزيادة التثبت من ان المفتاح العام هو المفتاح الحقيقي الذي أرسله abu abdalrahman

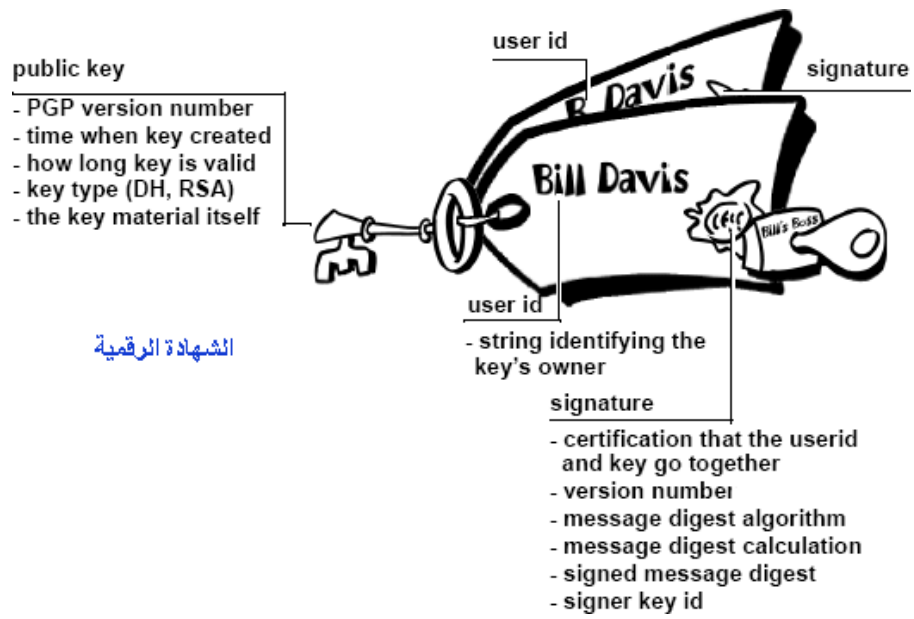
بعد ان قمنا بإرسال المفتاح العام ل Omar يجب ان نرسل له البصمة الرقمية بشكل مستقل ، إما عن طريق الشات مثلا، او البريد ، او اي وسيلة تراها مناسبة.

للحصول على البصمة الرقمية ، مي عبارة عن أود خاص بالمفتاح :اضغط على Manager Key.





إذا لم تتطابق، هذا يدل على أن المفتاح العام قد تم تغييره ، أو أنه ليس المفتاح الحقيقي الخاص بـ abu abdalrahman طبعاً، يمكنك إرسال معلومات أخرى مثلاً Key Algorithm, Created, Omar لزيادة التثبيت. ملخص للمعلومات التي تحتويها الشهادة الرقمية :





الوحدة الثانية

أنواع التشفير والأساليب المستخدمة فيها.

- التعرف على أنواع التشفير.
- فهم مفهوم المفاتيح وأنواعها.
- فهم مفهوم الهجمات على التشفير.
- تطبيق أساليب التشفير.

أنواع التشفير والأساليب المستخدمة فيها

في ظل التزايد المستمر للجرائم الإلكترونية خلال السنوات الأخيرة، باتت حماية أمن الشبكة ضرورة لا غنى عنها للمنظمات التي ترغب في الحفاظ على معلوماتها من الاختراق، وتتعدد التقنيات التي تُستخدم في هذا الغرض، والتي يحددها خبير أمن الإنترنت وفقًا لوضع المنظمة، ومن أبرز تلك التقنيات تشفير البيانات والتي تُعد من أكثر التقنيات أمانًا وفعالية في حماية البيانات، وفي هذا المقال نوضح تعريف تشفير البيانات وأنواعه ومراحله والغرض من استخدامه والتقنيات المُستخدمة في التشفير.

التعرف على أنواع التشفير.

تتعدد أنواع التشفير في الأمن السيبراني، ولكن هناك طريقتين للتشفير هما الأكثر شيوعًا، وذلك على النحو التالي:

1. التشفير المتماثل



التشفير المتماثل Symmetric Encryption والذي يُعرف أيضًا باسم تشفير المفتاح الخاص، هو طريقة تعتمد على استخدام بعض الخوارزميات مفتاحًا خاصًا في عمليات التشفير وفك التشفير، أي أن المفتاح المستخدم للترميز هو نفسه المُستخدم لفك الشفرة، وتتطلب هذه الطريقة وصول المرسل والمستقبل إلى نفس المفتاح، لذلك، يحتاج المستلم إلى المفتاح قبل فك تشفير الرسالة.

وتُعد طريقة التشفير المتماثل هي الطريقة المُفضلة للمستخدمين الأفراد والأنظمة المغلقة، كما أنها أقل أمانًا.

2. التشفير غير المتماثل



التشفير غير المتماثل Asymmetric Encryption والذي يُعرف أيضاً باسم التشفير بالمفتاح العام، ويُستخدم في غالبية بروتوكولات أمن الإنترنت، وفي هذه الطريقة يتم استخدام مفتاحين في عملية التشفير، وهما مفتاح عام وخاص توجد بينهما علاقة رياضية، والاثنين عبارة عن أرقام كبيرة ليست متطابقة ولكنها مقترنة ببعضها البعض، إذ يستخدم المستخدم أحدهما للتشفير والآخر لفك التشفير.

والمفتاح العام في التشفير غير المتماثل متاحاً لأي شخص مجاناً، بينما المفتاح الخاص يمتلكه المستلمين المقصودين فقط، الذين يحتاجون إليه لفك شفرة الرسائل.

وهناك أنواع أخرى من التشفير والتي تختلف باختلاف الغرض من استخدامها، وهي كما يلي:

3. تشفير مستوى الشبكة

وفي هذا النوع تتشفّر طبقة نقل الشبكة من البيانات، وهي الطبقة بين مستوى رابط البيانات ومستوى التطبيق، ويسهل هذا التشفير من الاتصال الخاص عبر الملكية الفكرية عند استخدامه بالاقتران مع أدوات أمن الشبكة.

4. تشفير مستوى الارتباط

في هذا النوع، تتعرض البيانات للتشفير وفك التشفير وإعادة التشفير من قبل النظام عندما يغادر الشبكة المضيفة، وهو ما يساعد على تعزيز الأمان في هذا التشفير، إمكانية استخدام كل رابط مفتاح تشفير مختلف.

5. التشفير من طرف إلى طرف

وهي التقنية المستخدمة في حماية الاتصالات التي تُجرى بين طرفين، مثل محادثات البريد الإلكتروني والرسائل الفورية ومحادثات الفيديو. وتضمن هذه التقنية أنه لن يتمكن أحد من قراءة الرسالة سوى المستقبل المقصود فقط، وبالتالي فهي توفر للمستخدمين أعلى مستوى من الأمان والخصوصية.

6. تشفير مستوى العمود

يشفر هذا النوع الخلايا الموجودة في عمود معين، إذ يحتاج المستخدم إلى إدخال كلمة مرور حتى يصل إلى البيانات في تلك الخلايا.

7. التشفير على المستوى الميداني

وهو تشفير خاص بمواقع الويب، فمن خلاله يتم تشفير مجالات محددة على صفحة الويب، وهي المجالات التي قد تحتوي على معلومات حساسة مثل رقم بطاقة الائتمان.

فهم مفهوم المفاتيح وأنواعها

المفتاح العام Public Key Encryption

يشير إلى أي نظام تشفير يستخدم مفتاحًا عامًا ومفتاحًا خاصًا.

تلعب المفاتيح دورًا أساسيًا في عملية تشفير وفك تشفير المعلومات هي عبارة عن سلاسل من الأرقام أو الحروف التي يتم استخدامها في خوارزميات التشفير لتحويل المعلومات إلى نص مشفر.

أنواع المفاتيح:

1. المفتاح الخاص:

يتم استخدام نفس المفتاح (المفتاح السري) للتشفير وفك التشفير ويكون هذا المفتاح متماثل لأنه المفتاح الوحيد للنسخ أو المشاركة من قبل طرف آخر لفك تشفير نص التشفير ويكون أسرع من تشفير المفتاح العام.

2. تشفير المفتاح العام :

يُعرف تشفير المفتاح العام أيضًا باسم التشفير غير المتماثل. وهو نظام تشفير يستخدم زوجًا من المفاتيح: مفتاحًا عامًا ومفتاحًا خاصًا.

يتم استخدام مفتاحين يستخدم أحدهما للتشفير ومفتاح آخر لفك التشفير ويتم استخدام مفتاح واحد (مفتاح عام) لتشفير النص العادي لتحويله إلى نص مشفر ويستخدم مفتاح آخر (مفتاح خاص) من قبل المتلقي لفك تشفير نص التشفير لقراءة الرسالة.

الجدول التالي يوضح الفرق بينهما:

| الميزة | المفتاح الخاص | المفتاح العام |
|-----------|---|--|
| الوظيفة | فك تشفير المعلومات المشفرة باستخدام المفتاح العام | تشفير المعلومات لكي يتمكن فقط صاحب المفتاح الخاص من فك تشفيرها |
| السرية | يجب أن يكون سرّيًا للغاية ولا يطلع عليه أي شخص غير مصرح له | يمكن مشاركته مع أي شخص |
| الاستخدام | يستخدم لفك تشفير المعلومات، وإنشاء التوقيعات الرقمية، والتحقق من صحة شهادات SSL/TLS | يستخدم لتشفير المعلومات، والتحقق من صحة التوقيعات الرقمية، وإنشاء شهادات SSL/TLS |
| الطول | عادةً ما يكون أطول من المفتاح العام | عادةً ما يكون أقصر من المفتاح الخاص |
| التشبيه | مثل القفل | مثل المفتاح |

أمثلة على استخدام المفتاح الخاص والمفتاح العام:

1. التوقيعات الرقمية:

- يتم استخدام المفتاح الخاص لإنشاء توقيع رقمي على وثيقة.
- يتم استخدام المفتاح العام للتحقق من صحة التوقيع.

2. شهادات: SSL/TLS

- يتم استخدام المفتاح الخاص لإنشاء شهادة SSL/TLS.
- يتم استخدام المفتاح العام للتحقق من صحة الشهادة.

البريد الإلكتروني المشفر:

خوارزمية التوقيع الرقمي Digital Signature Algorithm

هو خوارزمية تستخدم في العديد من التطبيقات، مثل البريد الإلكتروني المشفر.

- يتم استخدام المفتاح العام للمرسل لتشفير الرسالة الإلكترونية.
 - يتم استخدام المفتاح الخاص للمستلم لفك تشفير الرسالة الإلكترونية.
- يُعد كل من المفتاح الخاص والمفتاح العام عنصرًا أساسيًا في علم التشفير، حيث يُستخدمان لضمان سرية المعلومات وحمايتها من الوصول غير المصرح به.
- فهم الفرق بين المفتاح الخاص والمفتاح العام وكيفية عملهما أمر ضروري لضمان أمن المعلومات في العالم الرقمي.

فهم مفهوم الهجمات على التشفير.

الهجمات الأمنية Security Attacks تشير إلى محاولات كسر أنظمة التشفير للوصول إلى المعلومات المشفرة أو تغييرها دون إذن حيث يتعرض الأنظمة والبيانات للتهديد من قبل مختلف الأطراف

هجمات يكمن الهدف من ورائها تعطيل جهاز الكمبيوتر المستهدف أو الغرض منها الوصول الى بيانات جهاز الكمبيوتر المستهدف وربما الحصول على امتيازات المسئول عنه. هناك العديد من أنواع الهجمات، ومنها:

1. هجمات الاختراق: (Hacking) تتضمن محاولات اختراق الأنظمة أو الشبكات بغرض الوصول غير المشروع إلى المعلومات.
 2. هجمات الفيروسات والبرمجيات الضارة: (Malware) تتضمن البرمجيات الخبيثة مثل الفيروسات وبرامج التجسس وأحصنة طروادة، التي تستهدف التلاعب بالأنظمة وسرقة المعلومات.
 3. هجمات الاحتيال الإلكتروني: (Phishing) تستخدم تقنيات احتيال للحصول على معلومات شخصية من الأفراد، مثل كلمات المرور وتفاصيل الحسابات.
 4. هجمات رفض الخدمة (DoS) وتوجيه خدمة: (DDoS) تهدف إلى إعاقة خدمة موقع أو شبكة عبر إرسال كمية كبيرة من الطلبات، مما يتسبب في تعطيلها.
 5. هجمات التصيد: (Spoofing) تتضمن استخدام معلومات مزيفة للتكر والتظاهر بأنها موثوقة، مثل عناوين IP المزيفة.
 6. هجمات التصيد الاجتماعي: (Social Engineering) تعتمد على خداع الأفراد للحصول على معلومات حساسة عبر التلاعب النفسي.
 7. هجمات التشفير: (Cryptographic Attacks) تستهدف نظم التشفير للوصول غير المشروع إلى المعلومات.
 8. حقن هجوم SQL: يستهدف قواعد البيانات من خلال إدخال أو تعديل البيانات بطرق غير مشروعة.
 9. هجمات دون انتظار: (Zero-Day) تستغل ثغرات أمنية لم يتم اكتشافها بعد، وتكون فعالة في الوقت الحالي.
- تحديد نوع الهجوم يساعد في فهم الطرق المحتملة لتفاديه وتعزيز أمان الأنظمة.

تطبيق أساليب التشفير عملي

نقدم شرح لأنواع التشفير مع تطبيقات عملية لبرامج مشروحة، موضوع البحث ينقسم الى جزئين:

طريقة التشفير المتناظر Symmetric Encryption

شرح الأحد برامج التشفير (ChaosMash2.0)

التشفير بشكل عام هو عملية الحفاظ على سرية المعلومات الثابت منها و المتحرك باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى 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 والحروف الغير مفهومة، يتم تشفير الملف وفك التشفير عن طريق كلمة السر التي يجب أن 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 مقدرا بالبت Bit ، كل ما زاد البت زادت نسبة الأمان وصعوبة فك الشيفرة.

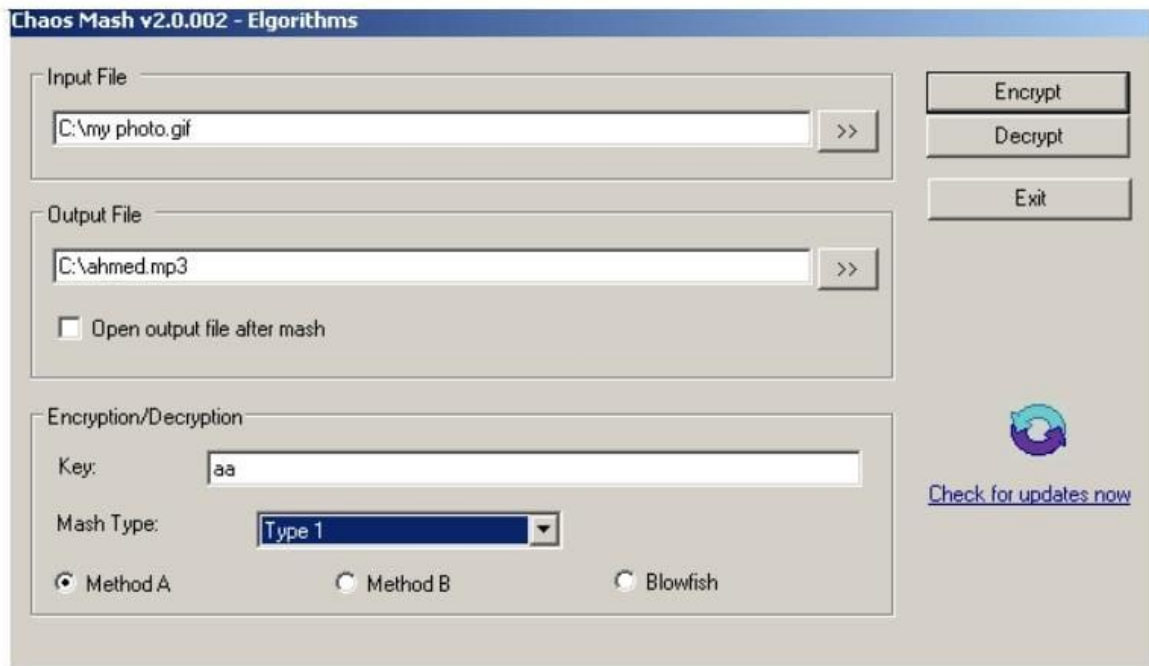
شرح لأحد برامج التشفير التي تستخدم طريقة التشفير المتناظر:

Chaos Mash 2.0

برنامج Chaos Mash2.0 ، يعد من البرامج البسيطة والسريعة في التشفير ، من خصائصه

1- لا يحتاج لتنصيب، ملف واحد فقط

2- يستخدم 15 طريقة للتشفير المزيد من التوضيح، استعن بالصورة

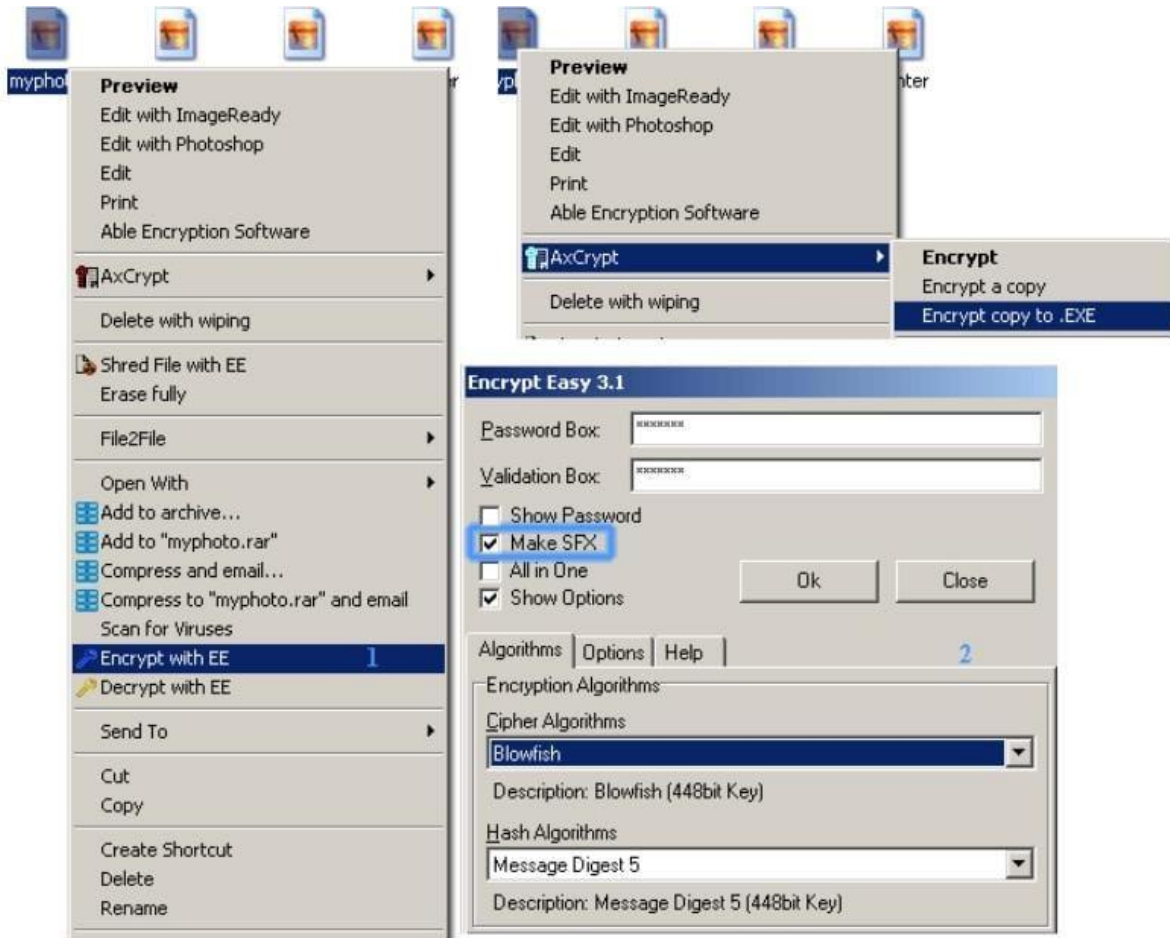


مصطلحات

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 1 type type15.
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 أن يفك التشفير decrypt بنفس الطريقة التي تم فيها تشفير
الملف أي انه على فرض أن الطرف الأول قام بعمل التالي لتشفير الملف: استخدم 13 method B type 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 Self Extra FX 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
- تشفير سهل



طريقة التشفير الغير متناظر - Asymmetric Encryption

- التشفير الغير متناظر

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

الهدف Asymmetric Encryption:

1. التخلص من مشكلة تبادل كلمات السر الغير امنه والتي قد تتعرض للسرقة من خلال طرف آخر 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 Reivest,shamir&Aselman (RSA)

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 أسر 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 بـ GPG. ويمكنك إضافة هذا البرنامج الى أغلب برامج البريد الالكتروني لتتمكن من تشفير الرسالة او توقيعها رقميا باستخدامه.

Windows Privacy Tools – WinPT

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

ملاحظة: قبل البدء التأكد من خلو الجهاز من ملفات التجسس، حتى لا يسرق المفتاح الخاص.

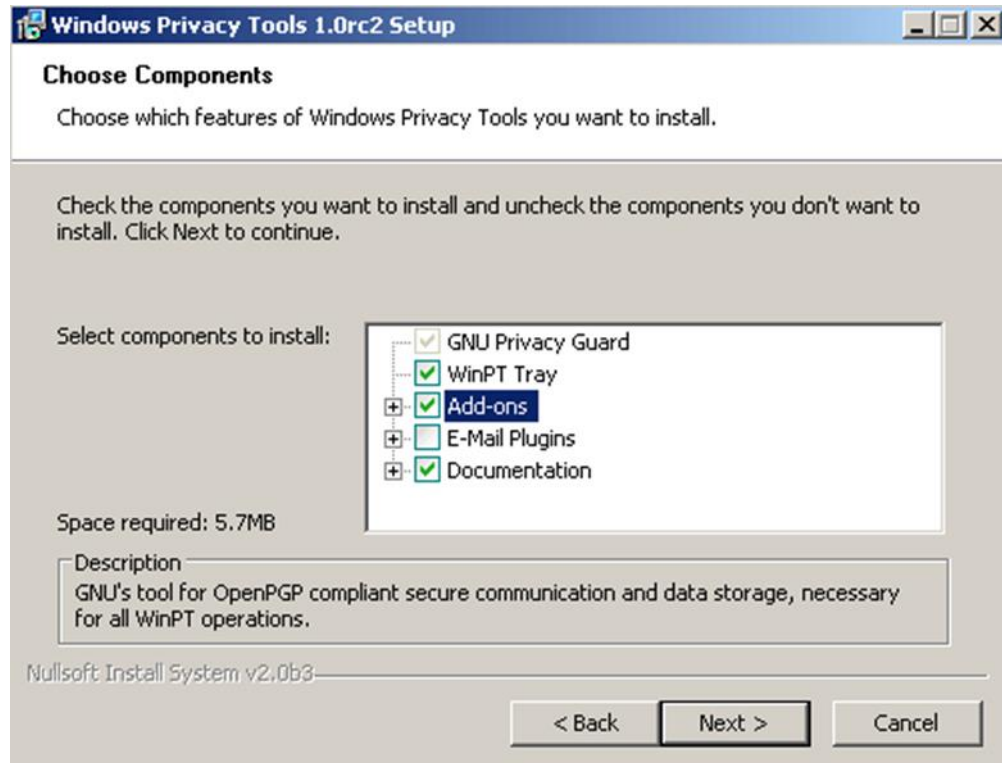
في الخطوات القادمة حتى تصل الصورة اعتبر التالي، وجود طرفين احدهما مرسل والآخر مستقبل

| الطرف المرسل | |
|--------------------|--|
| الاسم | abu abdrahman |
| معلومات عن المفتاح | publicKey ID: 0x5F0B907F 2006-02-13 abu abdrahman <abu_boxii2006@yahoo.com> Primary key fingerprint: 758B 8F52 B651 72F3 55A5 BE16 CDCC A8D0 5F0B 907F |
| الطرف المستقبل | |
| الاسم | Omar alayobi |
| معلومات عن المفتاح | 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 |

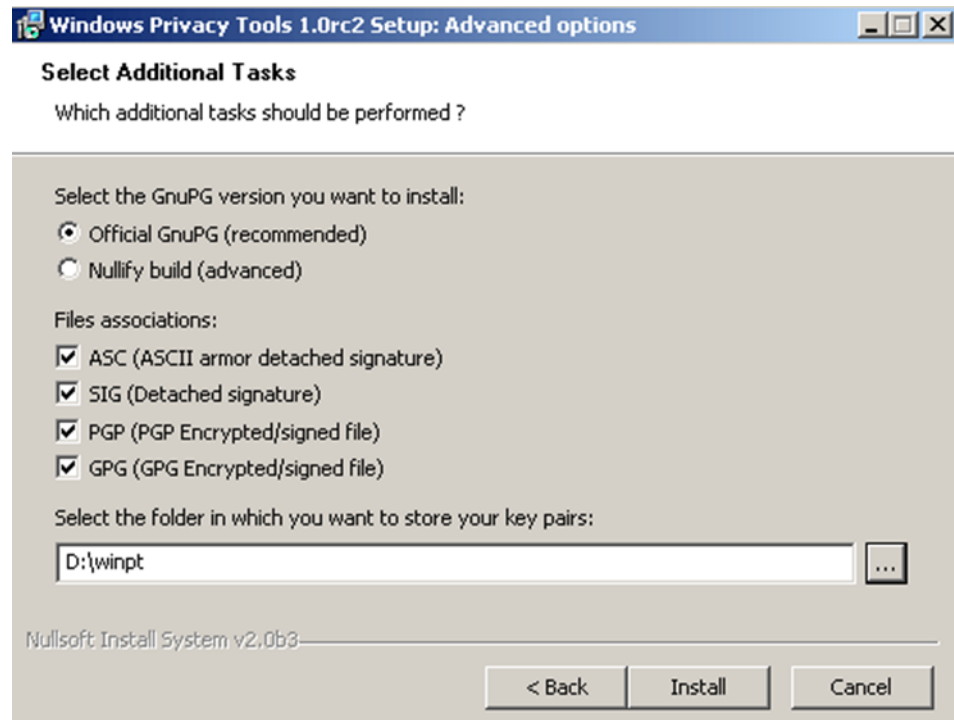
: Asymmetric Encryption

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

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

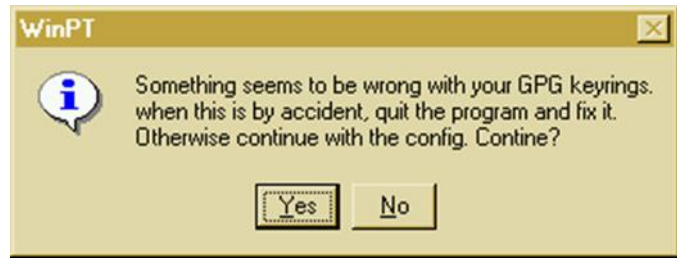


2. اختر مسار المجلد الذي تريد تخزين المفاتيح به، والتي سيتعامل معها البرنامج، مثال: D:\winpt



3. توليد المفتاح العام والخاص (key pair PGP)

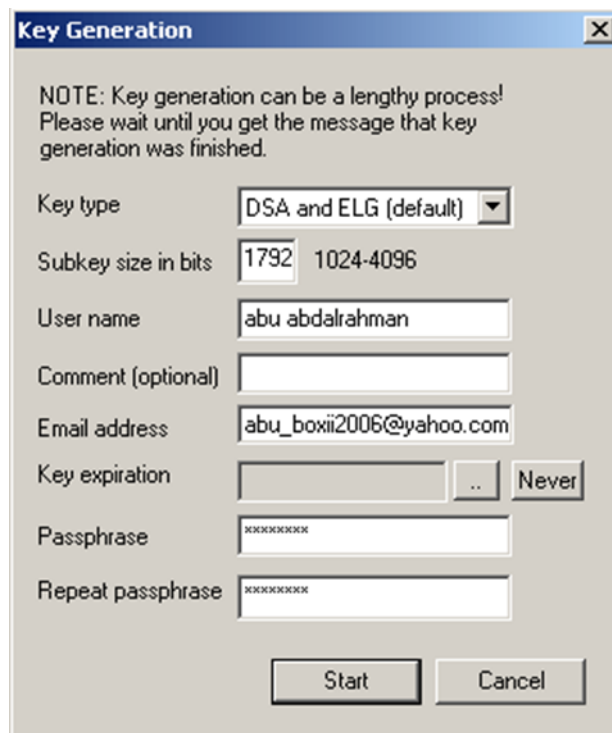
بعد الإنتهاء من تنصيب البرنامج، قم بفتحه، ستظهر لك رسالة تخبرك انه عليك توليد المفاتيح اضغط yes.



OK .4



5. توضح الشاشة التالي:



key type :نوع الخوارزمية المستخدمة في التشفير. البرنامج يقوم بدمج أثر من خوارزمية معاً أثناء التشفير

أما هو موضح DSA and ELG

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

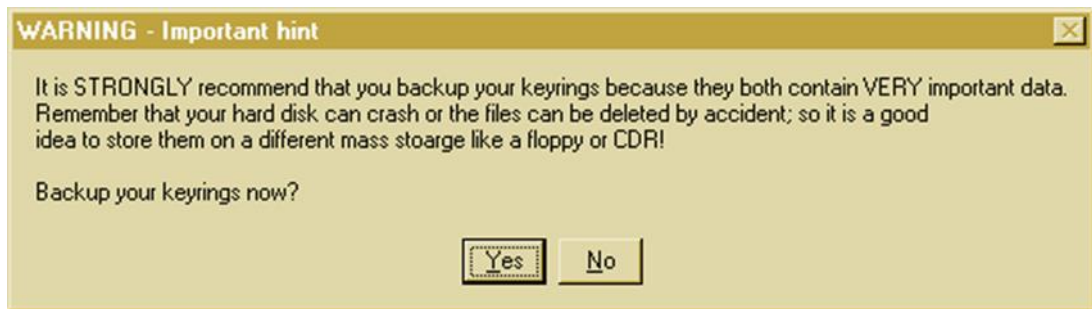
key: expiration *تاريخ انتهاء صلاحية المفتاح، لك الإختيار في ذلك، يمكنك جعل المفتاح غير محدد الزمن

Passphrase: آلمة السر التي تستخدم للتشفير وفك التشفير

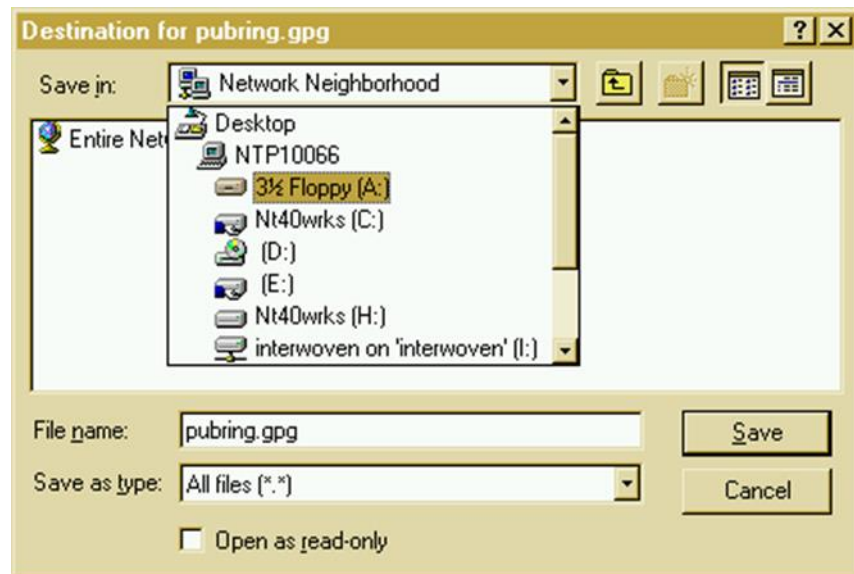
Repeat: Passphrase: تأكيد آلمة السر.

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 اذا اردت ذلك.



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

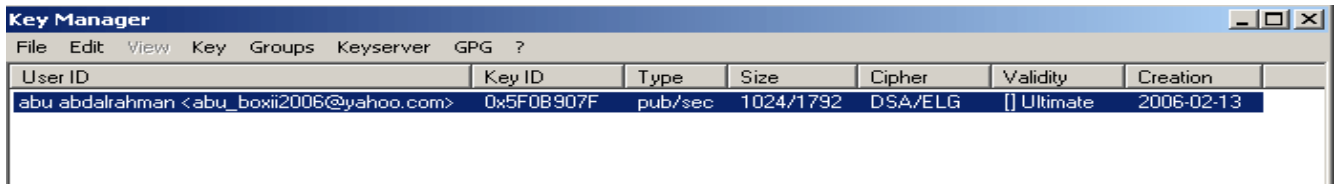


تم حفظ المفاتيح أما ترى في الشكل



بعد الإنتهاء من حفظ المفاتيح، تبين لك شاشة ال key manager التي آونتها ، يمكنك عمل مفتاح جديد

عن طريق الضغط على key- generate

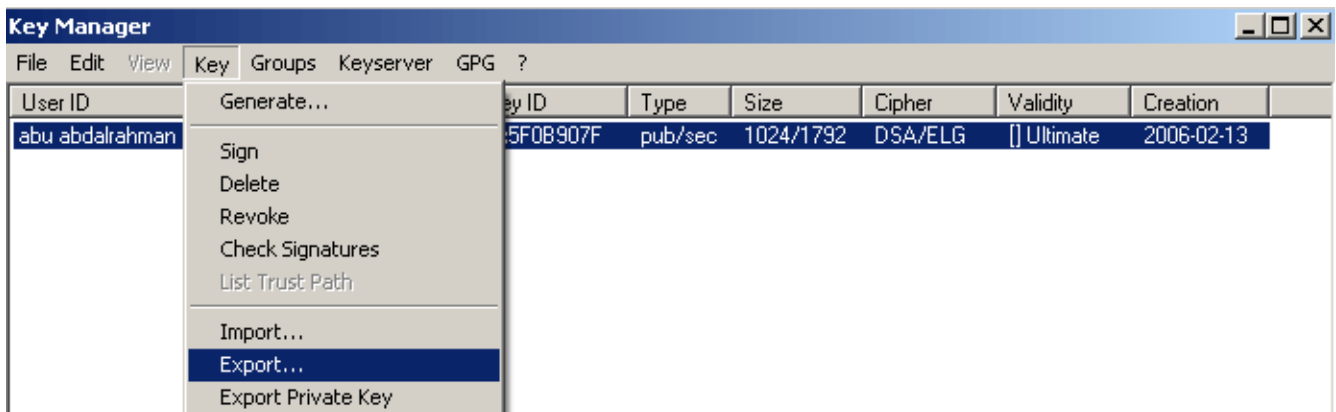


تقوم بفك التشفير

عن طريق المفتاح الخاص اضغط على Key Manager.

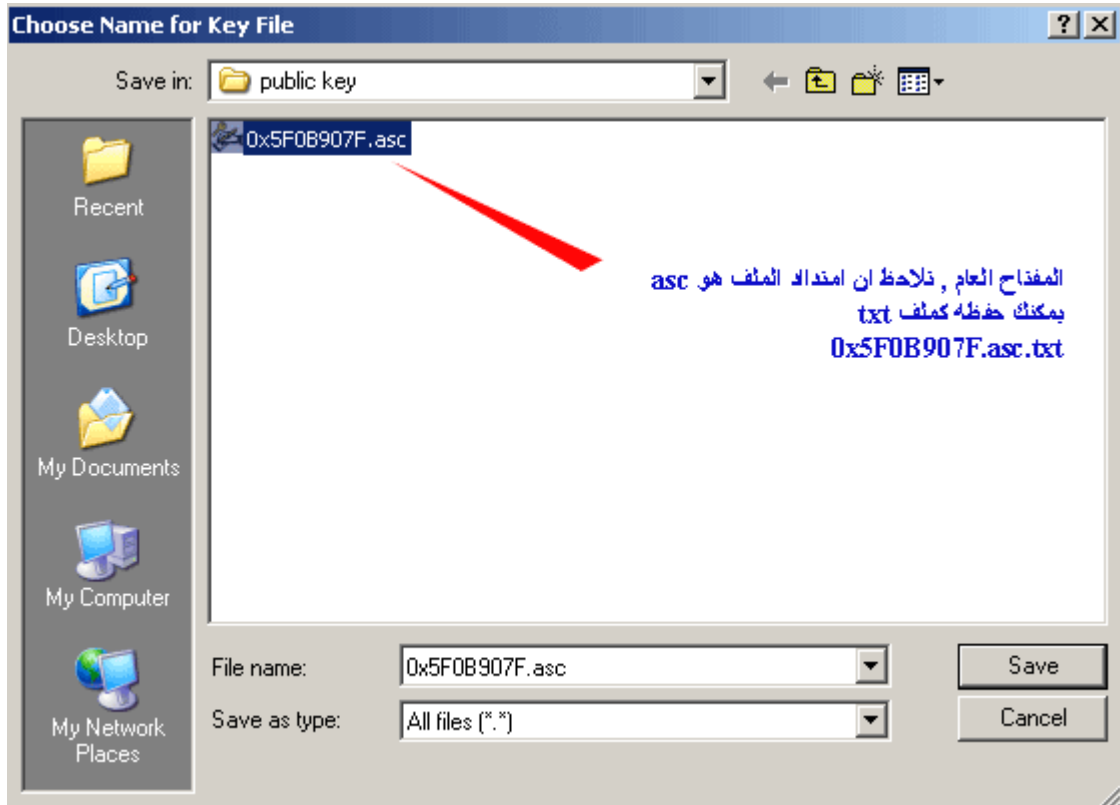


ستظهر لك شاشة المفاتيح ، قم بالضغط على المفتاح الموجود في الشاشة، حتى يصبح على شكل مظل، ومن ثم اضغط key- Export اي تصدير المفتاح العام.



في هذه الخطوة، قم بتحديد المسار الذي تريد حفظ المفتاح العام به. لاحظ رقم المفتاح العام key ID.

ايضاً يمكنك حفظه على شكل ملف مقروء txt.

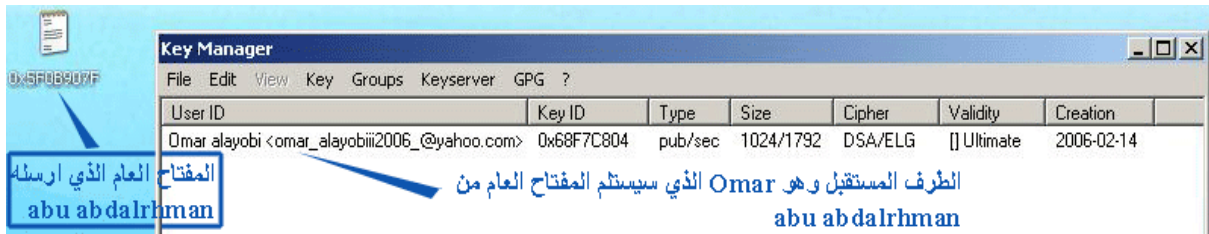


بعد ذلك قم بإرسال المفتاح العام للطرف المستقبل، عن طريق البريد الإلكتروني أو أي وسيلة تراها مناسبة لك.

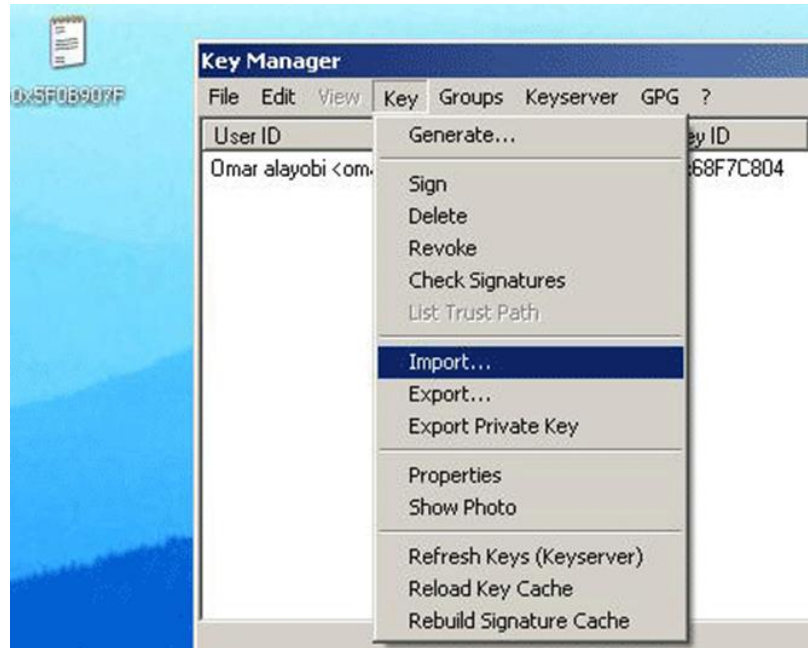
توضح الصورة التالية المفتاح العام ، يمكنك الحصول على هذه الشاشة عن طريق الضغط بالزر اليمين للماوس ومن ثم `open with - notepad`.



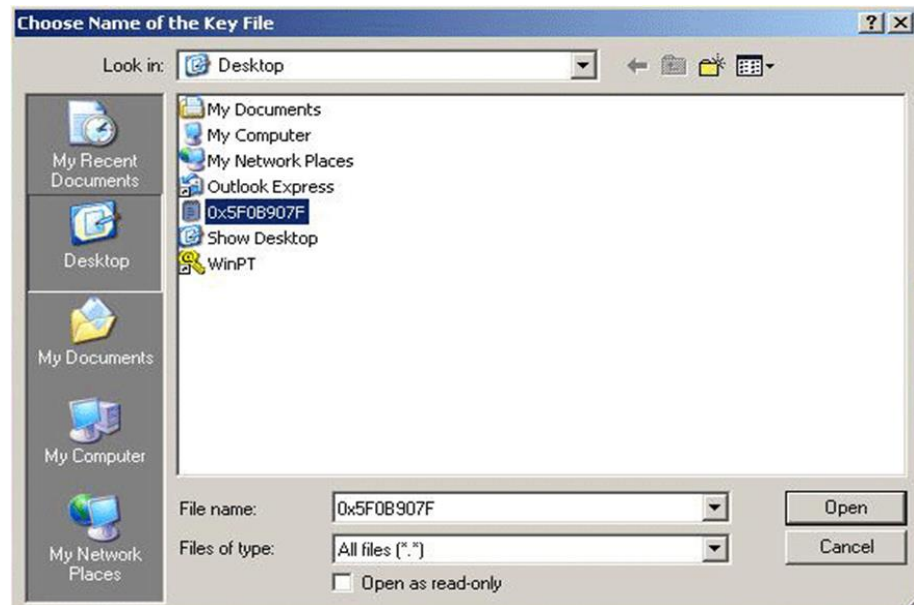
الطرف المستقبل : له مفتاحه الخاص الذي عمله، حصل على المفتاح العام



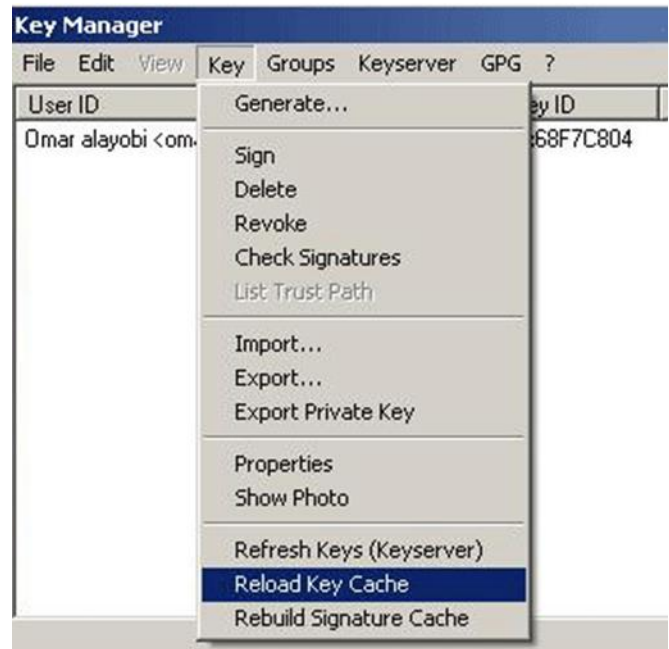
للحصول على المفتاح العام بالضغط على key-import هو موضح .



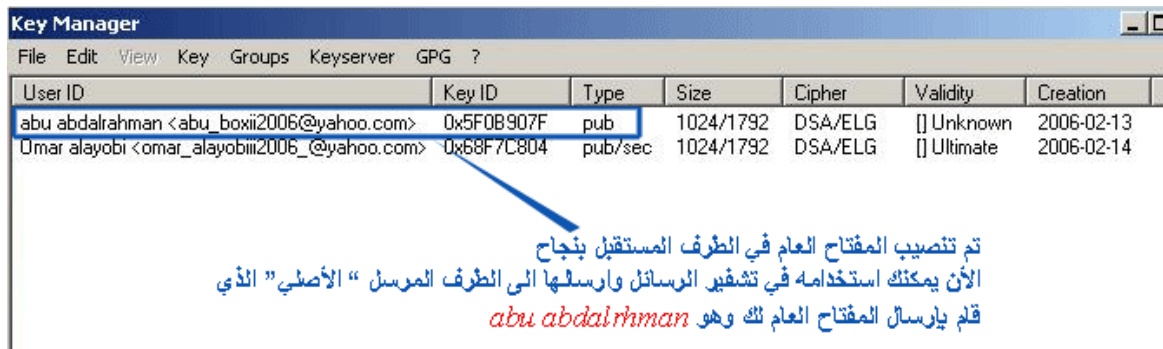
اختر المفتاح بعد ذلك . open.



لتفعيل المفتاح يجب عمل refresh



المفتاح العام الخاص ب abdallahman abd

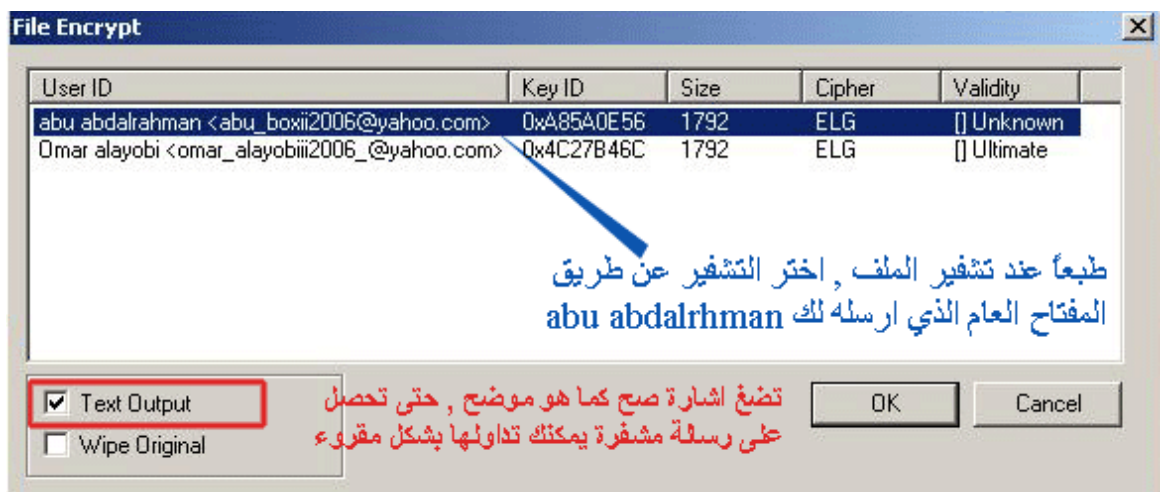
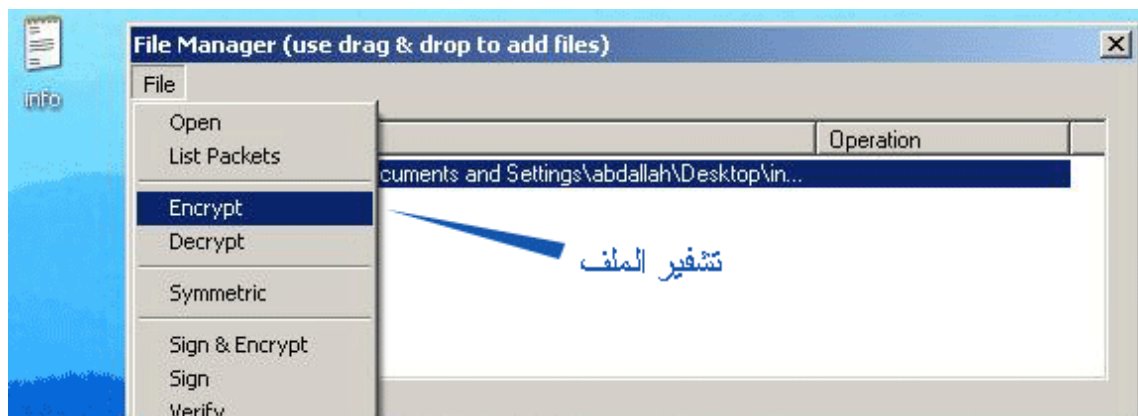
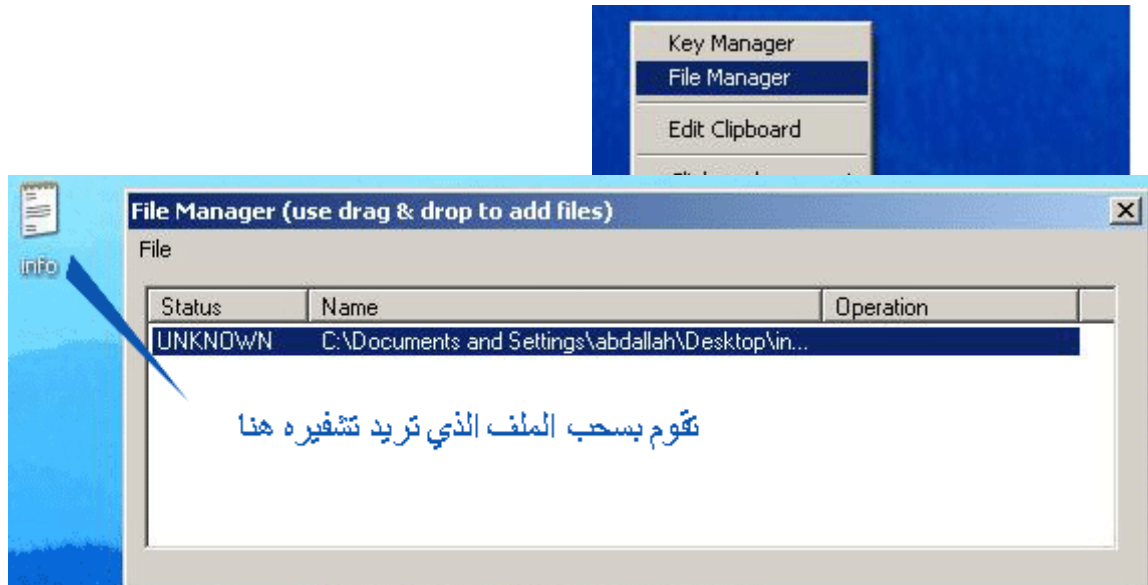


omar قام بكتابة رسالة الى abu abdalrhman وحفظ هذه الرسالة على شكل txt
info عن طريق استخدام المفتاح العام الخاص ب abu abdalrhman



لتشفير الرسالة اذهب الى File Manager

كما هو موضح بالمثال

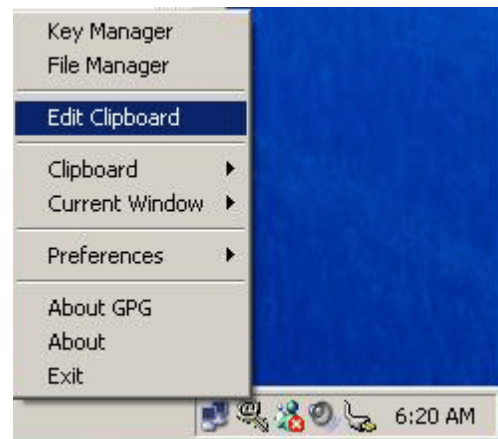


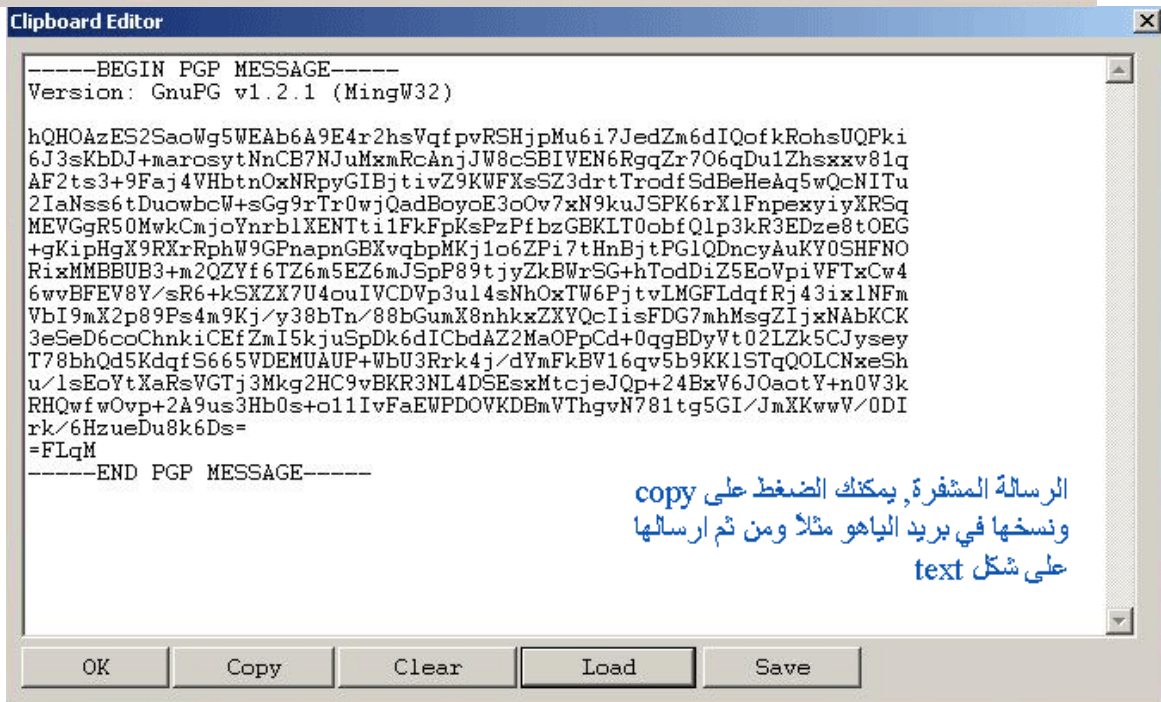
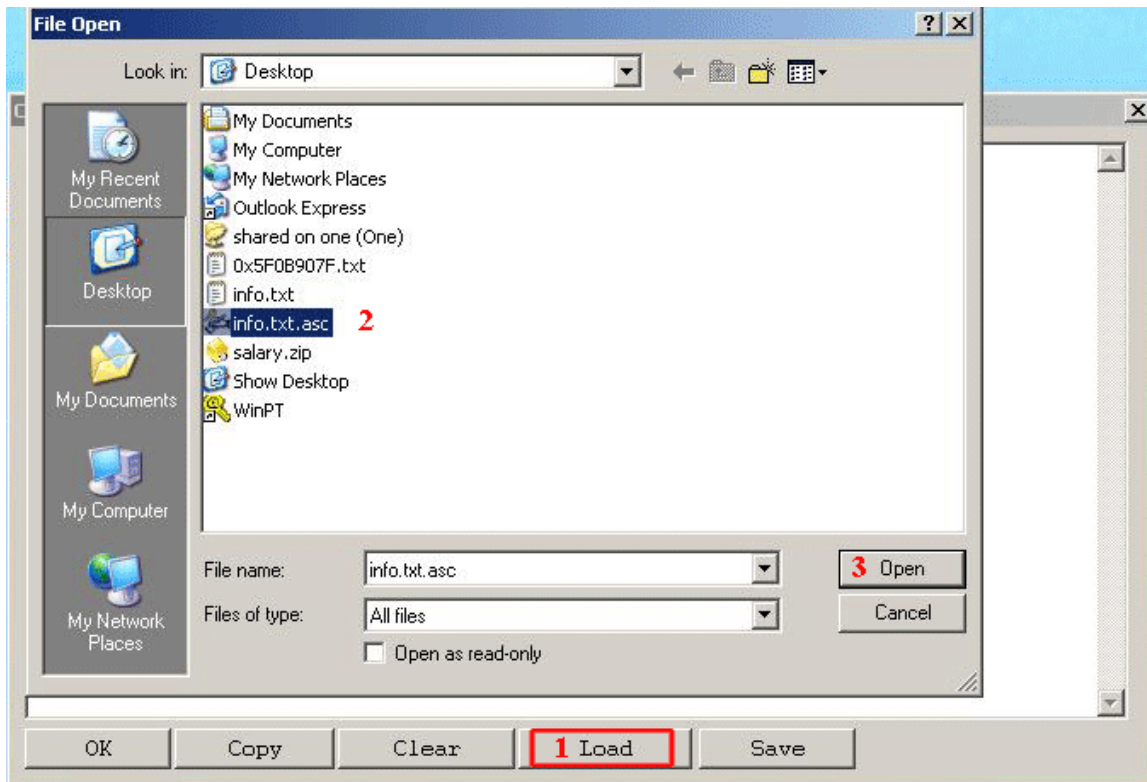
ايضاً عند التشفير، سيطلب منك البرنامج ادخال كلمة السر الخاصة بك، لإتمام عملية التشفير.



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





الوحدة الثالثة

أمن الشبكات والأمن في الحوسبة السحابية.

- فهم مفهوم أمن الشبكات.
- تحليل المخاطر وتقييم الضعف في الشبكات.
- تطبيق تقنيات الحماية في الشبكات.
- فهم مفهوم الحوسبة السحابية.
- تحديد المخاطر الأمنية في الحوسبة السحابية.
- تطبيق تقنيات الأمان في الحوسبة السحابية.

أمن الشبكات والأمن في الحوسبة السحابية.

الأمان السحابي هو فرع من الأمان الإلكتروني يهدف إلى تأمين أنظمة الحوسبة السحابية وحمايتها. ويشمل ذلك الحفاظ على خصوصية البيانات وأمانها على مستوى البنية الأساسية والتطبيقات والأنظمة الأساسية القائمة على الإنترنت. تسهم جهود موفري خدمات السحابة والعملاء الذين يستخدمونها، سواء أكانوا أفرادًا أو شركات صغيرة إلى متوسطة أو مؤسسات، في تأمين هذه الأنظمة وحمايتها.

يقوم موفرو خدمة السحابة باستضافة تلك الخدمات الأمنية على خوادمهم من خلال اتصالات إنترنت دائمة التشغيل. ونظرًا لأن عمل هؤلاء الموفرين يتوقف على ثقة العملاء، فإنهم يستخدمون وسائل الأمان السحابي للحفاظ على خصوصية بيانات العملاء وتخزينها بأمان. ولكن يتحمل العملاء بدورهم جانبًا من مسؤولية الحفاظ على الأمان السحابي. من الضروري هنا فهم كلا جانبي هذه العملية حتى يمكن تطبيق حل ملائم للأمان السحابي.

فهم مفهوم أمن الشبكات.

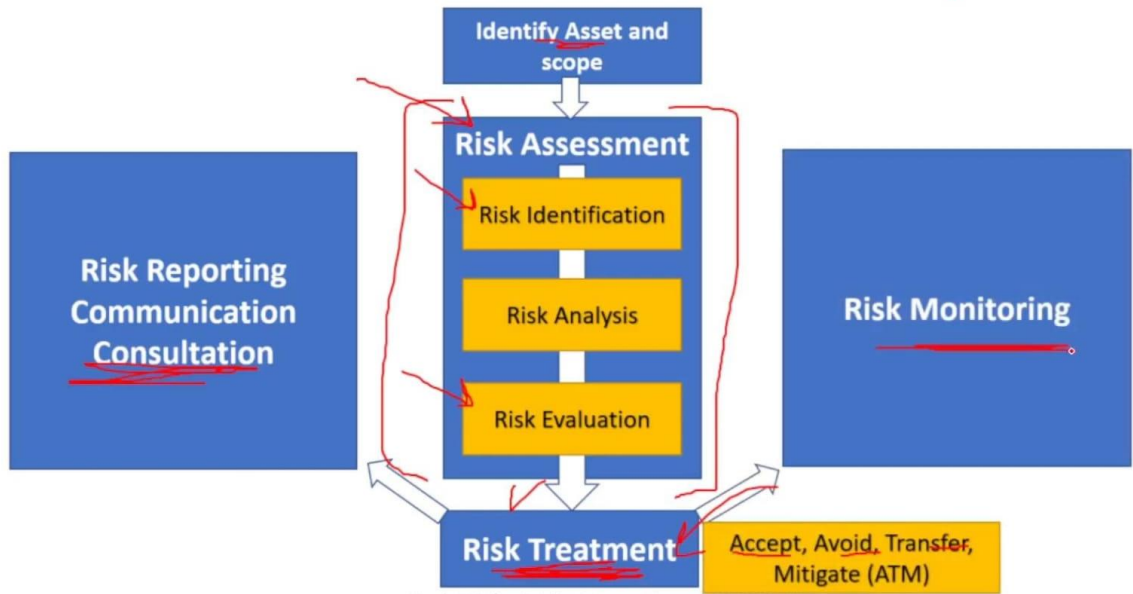
يُعرف تخصص "أمن الشبكات"، والذي يُطلق عليه "Cyber Security"، أو في بعض الأحيان "Network Security"، أنه توفير الحماية القصوى للبيانات والمعلومات في الشبكات بهدف تجنب المخاطر التي قد تلحق بها مثل الاختراق. ومن الجدير بالذكر أن هذه المخاطر قد تكون داخلية، أم خارجية. ولهذا، يوجد وسائل وأدوات لازمة لحمايتها.

يمكن أيضًا تعريف أمن الشبكات أنه حماية جهاز الحاسوب بما فيه من أجزاء ومكونات رئيسية وداخلية، وبرمجيات، بالإضافة إلى البيانات الإلكترونية من التعرض إلى الخراب، أو المخاطر، أو الدمار، أو من وصول السلطات غير المخولة بذلك إليها بطرق غير شرعية.

تحليل المخاطر وتقييم الضعف في الشبكات.

تحليل المخاطر هو عملية لتحديد وتقييم المخاطر التي قد تؤثر على شبكة الكمبيوتر وتقييم الضعف في الشبكات يعدان جزءًا أساسيًا من استراتيجيات الأمان السيبراني.

The Risk Management Process



عند التحدث عن الطوابق الامنية و controls يجب ان تكون متناسبة مع مقدار الخطر الموجود على الاصل ولذلك يجيب النظام الامنى لا يتجاوز قيمة الاصل الذي نحاول تأمينه بالضوابط الامنية

لذلك يجب تقييم ما هو مقدار الحماية الذي يجب تطبيقه يكون نتيجة عن عملية risk assessment و عن طريقه تقييم الخطر يمكنني معرفة ما هي المخاطر التي تحدث في الاصول و من خلال ذلك يمكننا تقدير اعلي المخاطر التي يمكن حدوثها و ما هي اعلي نسبة لتحقيقي ضرر وبالتالي يسهل عمليه اختيار risk management الملائم . نتائج حدوث خطر ما يكون له نتائج ايجابية و اخر سلبية و لكن عملية تقييم الخطر يتطلب الكثير من العمليات

1. في امن الشبكات يتم تقدير نتيجة ع تاثير الضرر الناتج عن طريق تقدير تكلفة الاصل الذي تم الضرر بيه و يمكن تقييم ذلك انه حاصل ضرب احتمالية الحدوث في الضرر الذي حدث impact

عملية ادارة المخاطر تتم من خلال معرفة اهداف لذي نريد ادارة الخطر الموجود في الشبكة بحيث يتم مقارنه المخاطر بأصل موجود و هذه الاصول او العناصر المهمة بالشبكة يجب ان تكون على تحديث مستمر

2. risk assessment هي مرحلة من مراحل risk management يتم فيه اكتشاف المخاطر التي تهدد الشبكة بطريقة غير مباشرة مثال قد يكون يوجد ثغره في ابلكيشن اهاتف و هذه الثغرة تقوم بتسريب بيانات العملاء او تسريب اموال العملاء في البنوك و بالتالي يمكننا قياس مدي الضرر الناتج عن حدوث الثغره

3. risk analysis هنا نتمكن من معرفة مقدار الخطر الناتج و ايضا يمكننا اكتشاف كيف حدث هذا الخطاء و في مرحله التحليل نتوصل الى الخسائر التي قد تحدث و ما مقدارها المالي

4. تقييم المخاطر risk evaluation وهنا نصل الى المشكلة الاساسية التي حدثت وليست مشكلة فرعية ونتمكن من البدء في اعلي شدة الخطر حدثت وهنا نصل الى مرحلة risk treatment نحدد ما هي الخطوات التي يمكننا تنفيذها لتقليل نسبة الخطر بحيث ننفذ بعض الضوابط التي تتحكم في هذا الخطر ل اقلل نسبة ممكنة

5. risk reporting وهنا يتدخل دور الادارة العلي بحيث يجب اخذ القرار الملائم و من هنا نصل الى مرحلة risk monitoring للتأكد من مقدار هذا الخطر قبل تنفيذ خطوات التعامل معه

خطوات تحليل المخاطر:

1. تحديد الأصول: تحديد جميع الأصول الموجودة على الشبكة، مثل أجهزة الكمبيوتر والخوادم وأجهزة التوجيه والمفاتيح والبرامج والبيانات.

2. تحديد التهديدات: تحديد جميع التهديدات المحتملة التي قد تواجهها الشبكة، مثل هجمات المتسللين والبرامج الضارة والكوارث الطبيعية والأخطاء البشرية.

3. تقييم المخاطر: تقييم احتمالية حدوث كل تهديد وتأثيره على كل من الأصول.

4. معالجة المخاطر: تحديد خطوات لمعالجة المخاطر، مثل تنفيذ تدابير الأمان وتطوير خطط الاستجابة للطوارئ.

5. تقييم الضعف: هو عملية لتحديد نقاط الضعف في شبكة الكمبيوتر التي يمكن للمتسللين استغلالها.

6. خطوات تقييم الضعف:

- اكتشاف الأصول:

تحديد جميع الأصول الموجودة على الشبكة، مثل أجهزة الكمبيوتر والخوادم وأجهزة التوجيه والمفاتيح والبرامج والبيانات.

- مسح الأصول:

استخدام أدوات المسح لاكتشاف نقاط الضعف في الأصول.

- تقييم نقاط الضعف:

تقييم خطورة كل نقطة ضعف وتأثيرها على الشبكة.

- إصلاح نقاط الضعف:

تحديد خطوات لإصلاح نقاط الضعف، مثل تطبيق تصحيحات الأمان وتحديث البرامج.

أدوات تحليل المخاطر وتقييم الضعف:

Nessus: أداة قوية لاكتشاف نقاط الضعف في الشبكات.

Nmap: أداة مجانية لاكتشاف الشبكات والمسح.

Metasploit: أداة لاختبار الاختراق.

Wireshark: أداة لتحليل حركة مرور الشبكة.

من خلال تحليل المخاطر وتقييم الضعف، يمكننا تحديد نقاط الضعف في الشبكة واتخاذ خطوات لمعالجتها قبل أن يستغلها المتسللون.

تطبيق تقنيات الحماية في الشبكات.

أمن الشبكات هو مجال مهم لحماية المعلومات والبيانات من التهديدات الإلكترونية. يجب على المؤسسات والأفراد أن يكونوا على دراية بأساسيات حماية الشبكات وتطبيقها للحفاظ على سلامة البيانات. يمكن تقسيم تقنيات الحماية في الشبكات إلى فئات رئيسية:

1. تقنيات منع الاختراق:

جدران الحماية: تمنع الوصول غير المصرح به إلى الشبكة.

أنظمة كشف التطفل (IDS): تراقب الشبكة للكشف عن الأنشطة المشبوهة.

أنظمة منع التطفل (IPS): تمنع الأنشطة المشبوهة على الشبكة.

برامج مكافحة الفيروسات: تمنع انتشار الفيروسات والبرامج الضارة.

2. تقنيات التحكم في الوصول:

التعريف والمصادقة: التحقق من هوية المستخدمين قبل السماح لهم بالوصول إلى الشبكة أو مواردها.

التفويض: تحديد ما يمكن للمستخدمين الوصول إليه على الشبكة.

التحكم في الوصول إلى الشبكة (NAC): التحكم في الوصول إلى الشبكة بناءً على خصائص الجهاز أو المستخدم.

3. تقنيات التشفير:

تشفير البيانات: حماية البيانات من الوصول غير المصرح به.

تشفير الاتصالات: حماية الاتصالات من التجسس والاختراق.

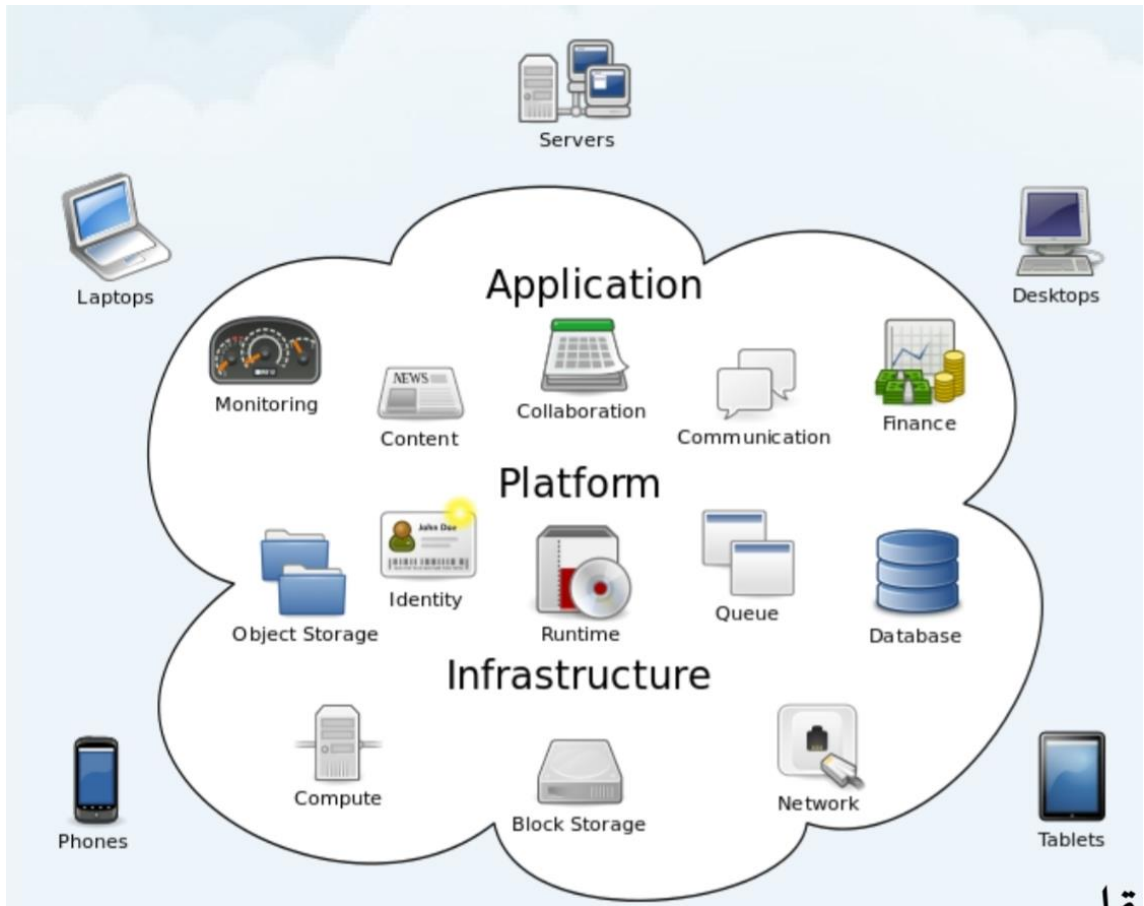
الشبكات الخاصة الافتراضية (VPN): إنشاء شبكة آمنة داخل شبكة عامة.

4. تقنيات الاستجابة للطوارئ:

خطط الاستجابة للطوارئ: تحديد كيفية الاستجابة للأحداث الأمنية.

النسخ الاحتياطي والاسترداد: استعادة البيانات في حالة وقوع كارثة.
مراقبة الأمان: مراقبة الشبكة للكشف عن الأحداث الأمنية.
يعد تطبيق تقنيات الحماية في الشبكات أمرا ضروريا لحماية الشبكة من الهجمات والتهديدات.
من خلال تطبيق تقنيات الحماية يمكنك تقليل مخاطر حدوث خرق أمني وحماية بياناتك وأصولك.

فهم مفهوم الحوسبة السحابية.



أمن الحوسبة السحابية (Cloud computing security) هو مصطلح يشير إلى مجموعة من الإجراءات والتقنيات التي تستخدم لحماية البيانات والتطبيقات والموارد المستضافة في بيئة الحوسبة السحابية. وتعتبر الحوسبة السحابية بيئة مشتركة تشارك فيها الموارد والبيانات عبر شبكة الإنترنت، وهذا يعني أن هناك تحديات أمنية فريدة قد تواجهها.

ويعتبر أمن الحوسبة السحابية يعتبر مسؤولية مشتركة بين مقدمي خدمات الحوسبة السحابية والعملاء. لذا يجب على مقدمي الخدمات توفير بنية أمنية قوية وحماية الأنظمة والبيانات، في حين يجب على العملاء اتخاذ التدابير اللازمة لتأمين حساباتهم وضمان سلامة البيانات التي يتم تخزينها ومعالجتها في الحوسبة السحابية.

المكونات الحوسبة السحابية



1. العميل (المستخدم) : هو الذي سيستفيد من الخدمات بواسطة أي جهاز تقني يملك إمكانيات متوسطة أو تحت المتوسطة يكفي فقط للاتصال بشبكة الانترنت.
2. نظام تشغيل: نظام يمكنه السماح بالاتصال بالإنترنت وهذه الخاصية متاحة تقريبا في كل أنظمة التشغيل الموجودة حاليا.
3. البرنامج (التطبيق): برنامج يحقق الخدمات المقدمة من الحوسبة السحابية و من أشهرها متصفح الإنترنت
4. توفر اتصال بشبكة الإنترنت: من أهم الأدوات التي يجب توفرها للربط بين العميل و بين كل بياناته وكل البرامج التي يستخدمها.
5. مزود الخدمة: و هو مشابه لمزود خدمة استضافة المواقع ولكن بخدمات وخصائص مميزة لكي يسمح لكل من المطورين والمستخدمين من استخدام الموارد المتاحة في الخوادم بكفاءة عالية حيث أن بقاء كل من المستخدمين ومطوري التطبيقات سيكون أكثر على خوادم مزودي خدمات الحوسبة السحابية.

مزايا الحوسبة السحابية

- تقليل التكاليف: لا تحتاج إلى الاستثمار في البنية التحتية لتقنية المعلومات.
- تدفع فقط مقابل الموارد التي تستخدمها.
- زيادة المرونة: يمكنك توسيع أو تقليص مواردك بسهولة حسب الحاجة.
- تحسين الموثوقية: توفر مزودي الخدمات السحابية عادةً ضمانات زمنية عالية.
- تعزيز الأمان: توفر مزودي الخدمات السحابية عادةً ميزات أمان قوية.
- سهولة الوصول: يمكنك الوصول إلى مواردك من أي مكان في العالم عبر الإنترنت.

أنواع الحوسبة السحابية:

- البنية التحتية كخدمة: (IaaS) توفر البنية التحتية الأساسية، مثل أجهزة الكمبيوتر والتخزين والشبكة.
- المنصة كخدمة: (PaaS) توفر منصة لتطوير ونشر التطبيقات.
- البرمجيات كخدمة: (SaaS) توفر تطبيقات جاهزة للاستخدام.
- مزودي الخدمات السحابية:
- Amazon Web Services (AWS): أكبر مزود خدمة سحابية في العالم.
- Microsoft Azure: ثاني أكبر مزود خدمة سحابية في العالم.
- Google Cloud Platform (GCP): ثالث أكبر مزود خدمة سحابية في العالم.

مخاطر الحوسبة السحابية:

- الأمان: قد تكون بياناتك عرضة للخطر إذا لم يكن مزود الخدمة السحابية آمناً.
- الاعتمادية: تعتمد على مزود الخدمة السحابية لتوفير الموارد التي تحتاجها.
- قابلية النقل: قد يكون من الصعب نقل بياناتك من مزود خدمة سحابية إلى آخر.
- خاتمة: الحوسبة السحابية هي نموذج لتقديم تقنية المعلومات كخدمة عبر الإنترنت.
- لها العديد من المزايا، مثل تقليل التكاليف وزيادة المرونة وتحسين الموثوقية وتعزيز الأمان.
- ومع ذلك، هناك أيضاً بعض المخاطر، مثل الأمان والاعتمادية وقابلية النقل.
- من المهم تقييم مزايا وعيوب الحوسبة السحابية قبل اتخاذ قرار بشأن استخدامها.

تحديد المخاطر الأمنية في الحوسبة السحابية.

الأمان السحابي يهدف إلى تأمين أنظمة الحوسبة السحابية وحمايتها. يشمل ذلك الحفاظ على خصوصية البيانات وأمانها على مستوى البنية الأساسية والتطبيقات والأنظمة الأساسية القائمة على الإنترنت. يتضمن الأمان السحابي فئات متعددة مثل:

1. أمان البيانات: يتعلق بتأمين البيانات وتشفيرها.
 2. إدارة الهويات والوصول (IAM): يهدف إلى التحكم في من يمكنه الوصول إلى الموارد السحابية.
 3. الحوكمة*: تشمل السياسات المتبعة لمنع التهديدات والكشف عنها وتقليل مخاطرها.
 4. التخطيط للاحتفاظ بالبيانات (DR) واستمرارية العمل (BC): يهدفان إلى تأمين استمرارية الخدمات في حالة حدوث مشكلة.
 5. الامتثال للقانون: يتعلق بالالتزام بالقوانين واللوائح المتعلقة بالأمان.
- يجب على موفري خدمات السحابة والعملاء الذين يستخدمونها أن يعملوا سوياً لتأمين هذه الأنظمة وحمايتها. يتطلب الأمان السحابي نهجاً مختلفاً عن الأمان التقليدي لتكنولوجيا المعلومات، ويشمل مكونات متعددة مثل الشبكات والبيانات والتطبيقات وأجهزة المستخدم. يجب أن يكون التأمين السحابي استباقياً ومتعدد الجوانب للحفاظ على أمان البيئة السحابية.
- للحفاظ على أمان البيانات في الحوسبة السحابية، يُفضل اتخاذ الإجراءات التالية:
- تشفير المعلومات المخزنة.
 - فصل معلوماتك المخزنة عن بقية المستخدمين.
 - معرفة تصنيف بياناتك وتطبيق الضوابط المناسبة.
 - إجراء نسخ احتياطية دورية للبيانات.
 - تفعيل أدوات الحماية مثل جدار الحماية وتسجيل الدخول الثنائي.

تطبيق تقنيات الأمان في الحوسبة السحابية.

يمكن تقسيم تقنيات الأمان في الحوسبة السحابية إلى فئات رئيسية:

1. تقنيات منع الاختراق:
 - جدران الحماية: تمنع الوصول غير المصرح به إلى الشبكة.
 - أنظمة كشف التطفل (IDS): تراقب الشبكة للكشف عن الأنشطة المشبوهة.
 - أنظمة منع التطفل (IPS): تمنع الأنشطة المشبوهة على الشبكة.
 - برامج مكافحة الفيروسات: تمنع انتشار الفيروسات والبرامج الضارة.

2. تقنيات التحكم في الوصول:

- التعريف والمصادقة: التحقق من هوية المستخدمين قبل السماح لهم بالوصول إلى الشبكة أو مواردها.
- التفويض: تحديد ما يمكن للمستخدمين الوصول إليه على الشبكة.
- التحكم في الوصول إلى الشبكة: (NAC) التحكم في الوصول إلى الشبكة بناءً على خصائص الجهاز أو المستخدم.

3. تقنيات التشفير:

- تشفير البيانات: حماية البيانات من الوصول غير المصرح به.
- تشفير الاتصالات: حماية الاتصالات من التجسس والاختراق.
- الشبكات الخاصة الافتراضية: (VPN) إنشاء شبكة آمنة داخل شبكة عامة

4. تقنيات الاستجابة للطوارئ:

- خطط الاستجابة للطوارئ: تحديد كيفية الاستجابة للأحداث الأمنية.
- النسخ الاحتياطي والاسترداد: استعادة البيانات في حالة وقوع كارثة.
- مراقبة الأمان: مراقبة الشبكة للكشف عن الأحداث الأمنية.

أدوات لتطبيق تقنيات الأمان في الحوسبة السحابية:

Cloud Security Posture Management (CSPM): أداة لتقييم وضع أمان البنية التحتية السحابية.

Cloud Access Security Broker (CASB): أداة للتحكم في الوصول إلى التطبيقات والبيانات السحابية.

Data Loss Prevention (DLP): أداة لمنع فقدان البيانات أو سرقتها.

Security Information and Event Management (SIEM): أداة لجمع وتحليل أحداث الأمان.

نصائح لتطبيق تقنيات الأمان في الحوسبة السحابية:

- نستخدم نهجًا متعدد الطبقات للحماية.
- تحديث برامج الأمان بانتظام.
- تثقيف المستخدمين حول مخاطر الأمن السيبراني.
- إجراء اختبارات اختراق منتظمة.

- نوثق جميع إجراءات الأمان الخاصة بك.

ما هي المجالات الأربعة للأمن السحابي؟

يتعلق مجال الأمن السحابي بتوفير الحماية والأمان للبيانات والتطبيقات والبنية التحتية في بيئة الحوسبة السحابية. لتكون المجالات الرئيسية الأربعة للأمن السحابي كما يلي:

1. أمن الوصول والتحقق يتعلق بضمان الوصول المناسب للمستخدمين المصرح لهم والتحقق من هويتهم. ويشمل ذلك إدارة الهوية والوصول، وتوفير آليات التحقق مثل كلمات المرور والعوامل الثنائية والتعرف على الصوت أو البصمة، وتحديد مستويات الوصول للمستخدمين وفقًا لصلاحياتهم.
2. أمن البيانات والخصوصية يركز على حماية البيانات المخزنة والمرسلة في البيئة السحابية. ويشمل على تشفير البيانات، وإدارة المفاتيح، وتطبيق سياسات الحماية، والاستجابة لانتهاكات البيانات، وضمان الامتثال للتشريعات والمعايير المتعلقة بالخصوصية.
3. أمن الشبكة والاتصالات يتعلق بحماية الشبكة السحابية والاتصالات بين المستخدمين والموارد السحابية. يشمل على تأمين الاتصالات بواسطة تشفير البيانات المرسلة واستخدام بروتوكولات أمنية، وكشف ومنع الاختراقات والهجمات السيبرانية، وتأمين البنية التحتية للشبكة والحوافز النارية.
4. أمن التطبيقات والخدمات يشير إلى حماية التطبيقات والخدمات السحابية من الهجمات والثغرات الأمنية. ويتضمن ذلك اختبار الأمان والتدقيق للتطبيقات، وتطبيق مبادئ تطوير آمن للبرمجيات، ورصد الأمان والتحقق من سلامة التطبيقات وتحديثها بانتظام.



الوحدة الرابعة

حماية البيانات والمعلومات الحيوية باستخدام التشفير والتوقيع الرقمي.

- فهم مفهوم حماية البيانات والمعلومات الحيوية.
- فهم مفهوم التشفير والتوقيع الرقمي.
- تطبيق تقنيات التشفير والتوقيع الرقمي.
- فهم مفهوم الهجمات على التشفير والتوقيع الرقمي.
- تطبيق أساليب حماية البيانات والمعلومات الحيوية.

حماية البيانات والمعلومات الحيوية باستخدام التشفير والتوقيع الرقمي.

يلعب التشفير دورًا حيويًا في حماية البيانات الحساسة بحث يعتبر التشفير أداة أساسية لحماية البيانات التي يتم تخزينها ومعالجتها على الخوادم البعيدة. يساعد استخدام التشفير في هذا السياق على ضمان سرية المعلومات وحمايتها من التهديدات السيبرانية المتقدمة. . على سبيل المثال، يعتمد تشفير البريد الإلكتروني على بروتوكولات مثل PGP لتأمين محتوى الرسائل ومرفقاتها. في المجال التجاري، يستخدم الشركات التشفير لحماية بيانات العملاء والمعاملات المالية، مما يزيد من مستوى الثقة بين الأطراف المتعاملة.

دعونا نغم بالتوسع أكثر في موضوع التشفير واستخداماته المتنوعة في العالم الرقمي.

في سياق تطبيقات الشبكات اللاسلكية والاتصالات الهاتفية، يعتبر التشفير أحد العناصر الأساسية لضمان أمان المحادثات وبيانات المستخدمين. فمن خلال تقنيات التشفير، يتم تشفير المكالمات الصوتية والرسائل النصية على شبكات الهواتف المحمولة، مما يحمي هذه المعلومات من الاعتراض غير المصرح به.

تأتي تقنيات التشفير أيضًا على الطاولة في ميدان الصحة الرقمية، حيث يتم تخزين السجلات الطبية الإلكترونية وتبادل المعلومات الطبية بين المؤسسات الصحية باستخدام الشفرات القوية. هذا يساهم في ضمان سرية وسلامة المعلومات الصحية الحساسة.

دور التشفير في حماية البيانات الرقمية:

التشفير يعكس تطورًا حيويًا في كيفية تعاملنا مع المعلومات وكيفية حمايتها.

يفهم التشفير على أنه عملية تحويل البيانات من حالتها الطبيعية إلى شكل يصعب فهمه أو فك شفرته بدون وجود مفتاح خاص.

يستخدم في الاتصالات الرقمية لحماية الخصوصية وضمان سرية المعلومات.

على سبيل المثال، يُستخدم بروتوكولات التشفير مثل SSL/TLS لتأمين المعلومات المرسلة عبر الإنترنت.

تطبيقات التشفير:

البريد الإلكتروني: يعتمد تشفير البريد الإلكتروني على بروتوكولات مثل PGP لتأمين محتوى الرسائل ومرفقاتها.

الأعمال والمؤسسات: يستخدم في حماية بيانات العملاء والمعاملات المالية.

العملات الرقمية: يُستخدم لتأمين المعاملات المالية في بيئة البلوكشين.

التحديات والنقاشات:

قد تثير قضايا الخصوصية والأمان تحديات في تحقيق التوازن بين الأمان وحقوق الفرد.

يمثل التشفير ركيزة أساسية في العالم الرقمي، حيث يساهم في تعزيز الأمان وحماية الخصوصية.

فهم مفهوم حماية البيانات والمعلومات الحيوية.

مفهوم حماية البيانات والمعلومات الحيوية بشكل موجز:

حماية البيانات: تشير إلى الإجراءات والتقنيات التي تهدف إلى الحفاظ على سرية وسلامة البيانات. يتضمن ذلك حماية البيانات من الوصول غير المصرح به، والتلاعب، والتدمير.

المعلومات الحيوية: تشمل المعلومات الحيوية البيانات الحساسة والمهمة، مثل المعلومات الطبية، والبيولوجية، والوراثية. تحمل هذه المعلومات قيمة كبيرة وتحتاج إلى حماية خاصة.

التشفير والتوقيع الرقمي: هما أدوات أساسية لحماية البيانات والمعلومات الحيوية:

التشفير: يحول البيانات إلى شكل غير قابل للقراءة دون وجود مفتاح. يستخدم في البريد الإلكتروني، والمعاملات المالية، والاتصالات الرقمية.

التوقيع الرقمي: يثبت هوية المرسل ويضمن سلامة البيانات. يستخدم في المعاملات الرقمية والمستندات الرسمية.

فهم هذه المفاهيم يساعد في الحفاظ على أمان معلوماتنا والمساهمة في بناء عالم رقمي آمن.

فهم مفهوم التشفير والتوقيع الرقمي.

التشفير:

- هو عملية تحويل البيانات إلى شكل غير قابل للقراءة إلا من قبل الأشخاص الذين يملكون مفتاح فك التشفير.
- يُستخدم التشفير لحماية البيانات من الوصول غير المصرح به، مثل سرقة البيانات أو التجسس.
- هناك العديد من خوارزميات التشفير المختلفة، ولكل منها نقاط قوتها وضعفها.
- من المهم اختيار خوارزمية التشفير المناسبة لنوع البيانات واحتياجاتك الأمنية.

التوقيع الرقمي:

- هو عملية ربط توقيع رقمي ببيانات إلكترونية للتحقق من صحتها ومنع التزوير.
- يستخدم التوقيع الرقمي للتأكد من أن البيانات لم يتم تغييرها منذ توقيعها، وللتأكد من هوية الشخص الذي وقع عليها.
- يستخدم التوقيع الرقمي في العديد من التطبيقات، مثل التجارة الإلكترونية والبريد الإلكتروني.

مزايا استخدام التشفير والتوقيع الرقمي:

- حماية البيانات من الوصول غير المصرح به.
- منع التزوير والتلاعب بالبيانات.
- ضمان سلامة البيانات وسرية المعلومات الحيوية.
- تعزيز الثقة في المعاملات الإلكترونية.

تطبيق تقنيات التشفير والتوقيع الرقمي.

تطبيقات التشفير:

1. حماية كلمات المرور: استخدام خوارزميات التشفير القوية لتشفير كلمات المرور المخزنة على أجهزة الكمبيوتر أو المواقع الإلكترونية.
2. تأمين البيانات على الأجهزة المحمولة: استخدام برامج التشفير لتشفير البيانات الموجودة على الهواتف الذكية والأجهزة اللوحية.
3. حماية الاتصالات عبر الإنترنت: استخدام بروتوكولات التشفير مثل TLS و HTTPS لتشفير الاتصالات عبر الإنترنت، مثل البريد الإلكتروني أو مكالمات الفيديو.
4. حماية البيانات الحساسة: استخدام التشفير لحماية البيانات الحساسة، مثل المعلومات المالية أو الطبية.

تطبيقات التوقيع الرقمي:

1. التوقيع على المستندات الإلكترونية: استخدام التوقيعات الرقمية للتوقيع على العقود والوثائق الأخرى إلكترونياً.
2. التحقق من صحة البرامج: استخدام التوقيعات الرقمية للتحقق من صحة البرامج قبل تثبيتها على جهاز الكمبيوتر.
3. التصديق على المعاملات الإلكترونية: استخدام التوقيعات الرقمية للتحقق من هوية الأشخاص الذين يقومون بإجراء المعاملات عبر الإنترنت.
4. ضمان سلامة وسرية البيانات: استخدام التوقيعات الرقمية للتأكد من أن البيانات لم يتم تغييرها منذ توقيعها وللتأكد من هوية الشخص الذي وقع عليها.

أمثلة على الأدوات المستخدمة في التشفير والتوقيع الرقمي:

1. GnuPG:

أداة مجانية ومفتوحة المصدر للتشفير والتوقيع الرقمي.

2. OpenSSL:

أداة مجانية ومفتوحة المصدر لمكتبة التشفير.

3. Microsoft CryptoAPI:

أداة مدمجة في نظام التشغيل Windows للتشفير والتوقيع الرقمي.

4. Adobe Acrobat:

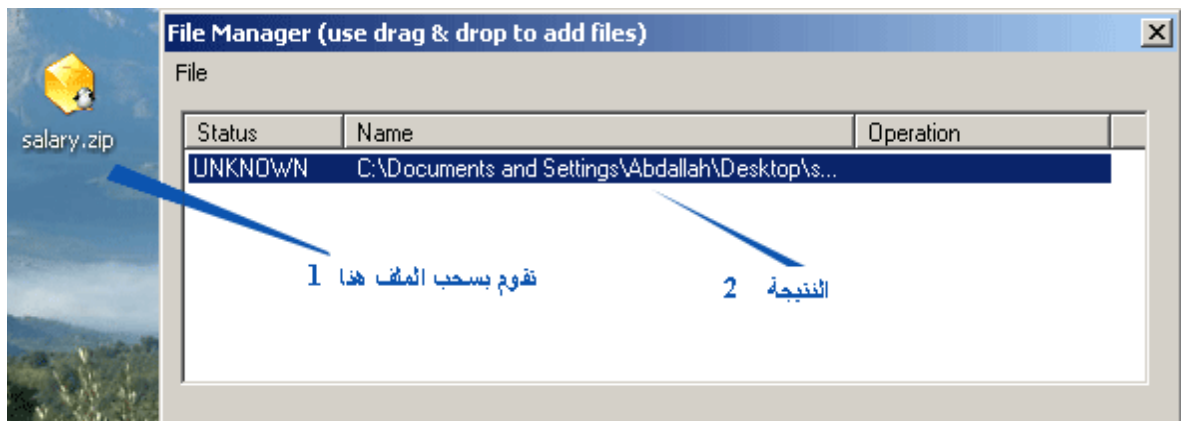
برنامج يستخدم على نطاق واسع للتوقيع على المستندات إلكترونياً.

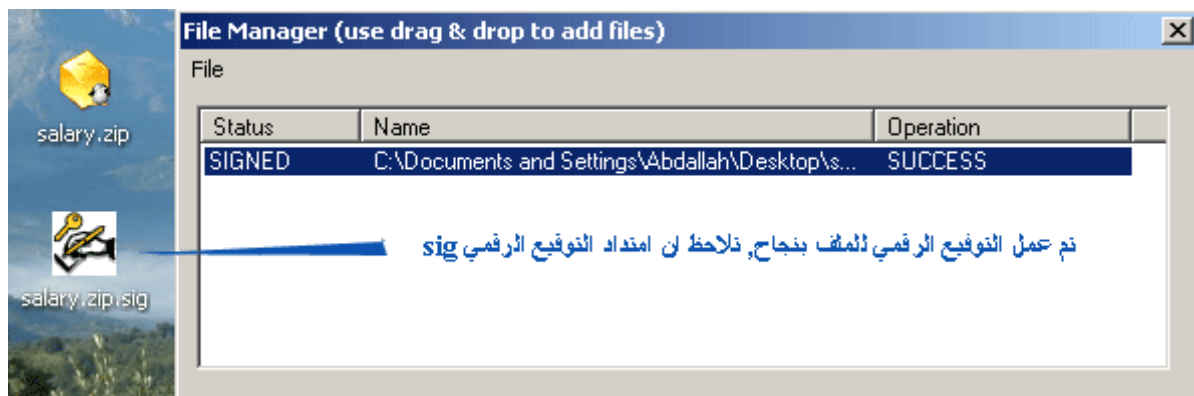
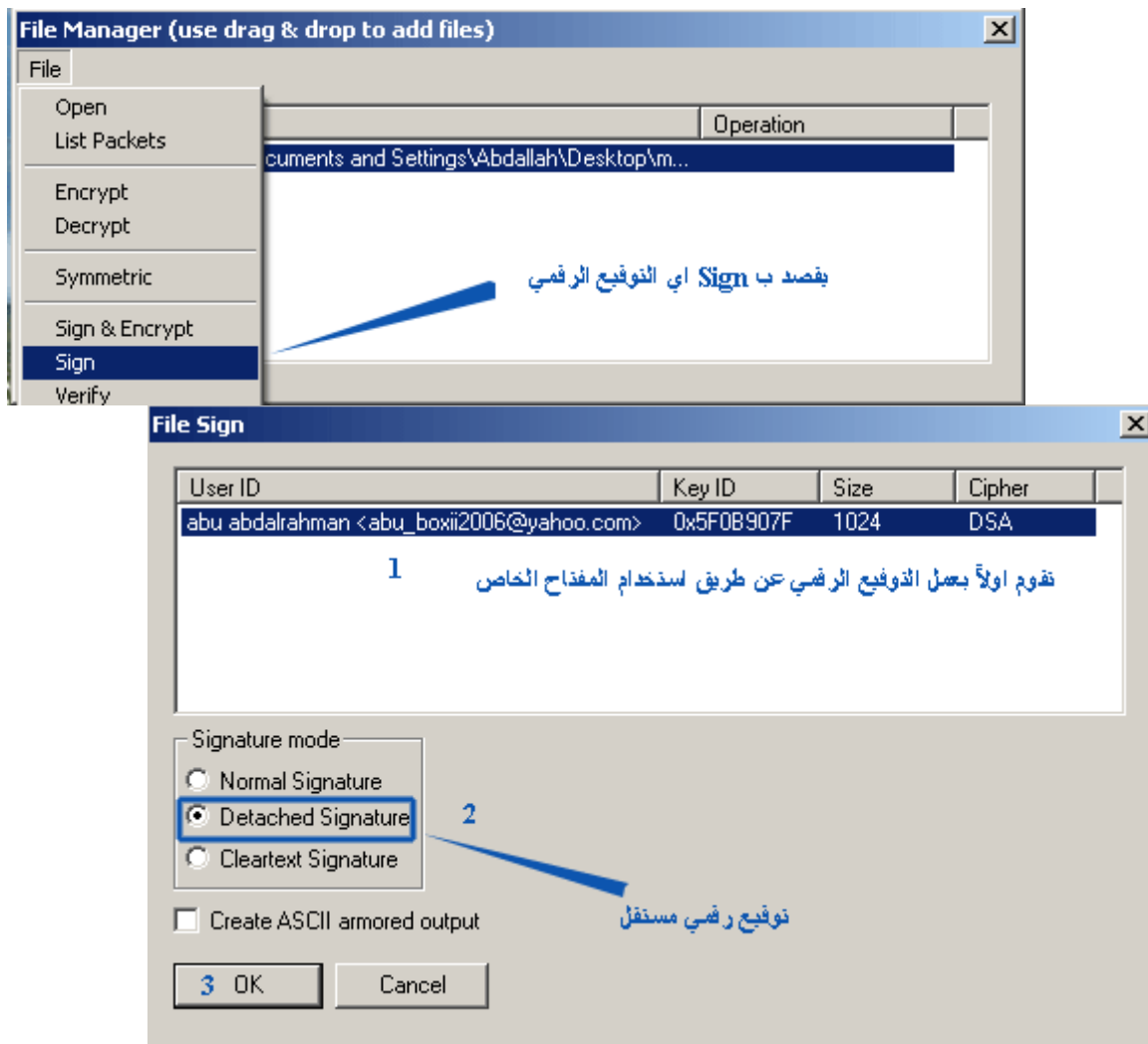
5. DocuSign

: منصة للتوقيع الإلكتروني على المستندات.

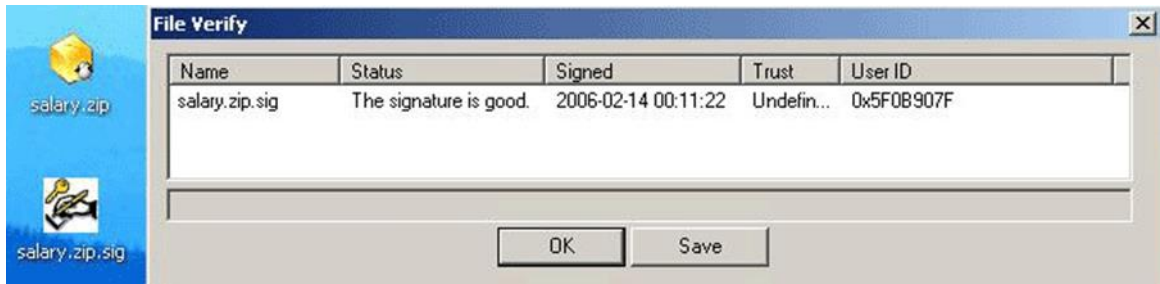
تطبيق عملي التوقيع الرقمي Digital Signatures

مثال عملي على فرض ان abdalrhman قام بإرسال ملف مضغوط إلى Omar و يريد التأكد من انه يقوم استخدم التوقيع الرقمي ، اذهب الى كما هو موضح بfilmmanager الخطوات التالية

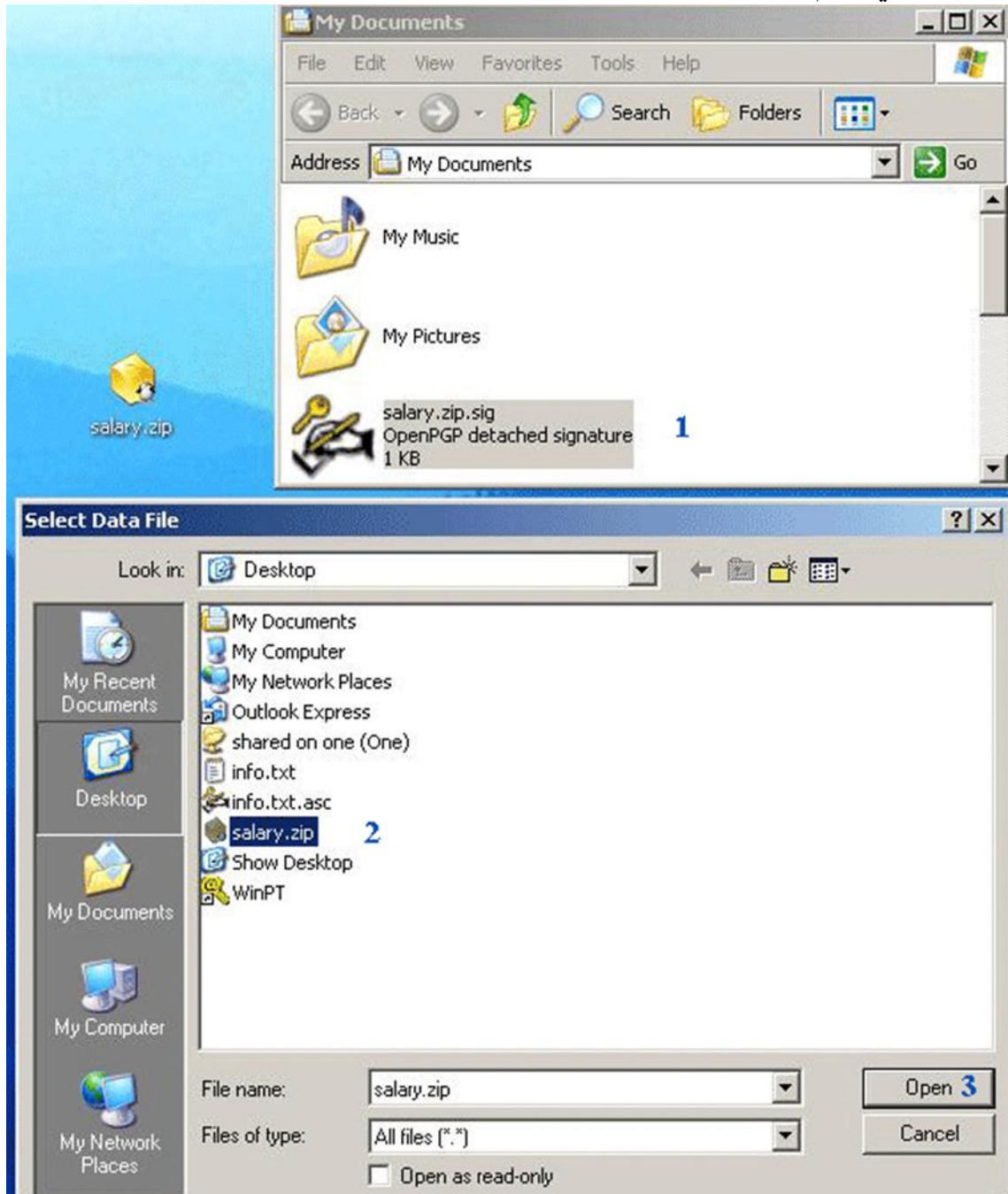




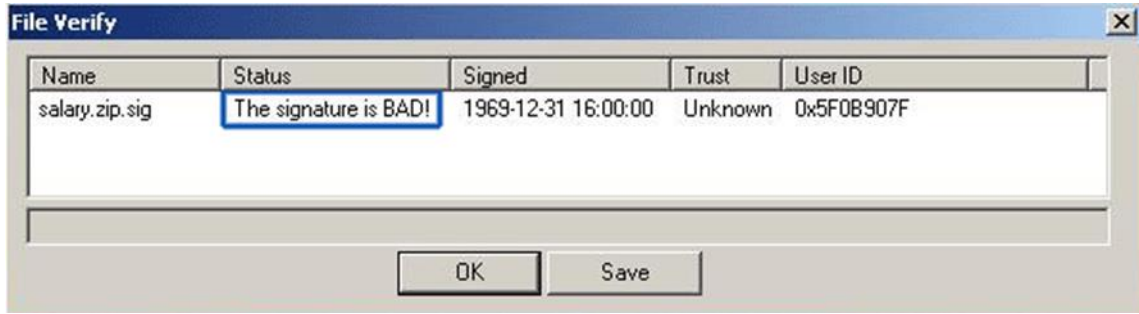
الآن نقوم بإرسال الملف المضغوط الى omar وأيضاً قم بإرسال التوقيع الرقمي في حالة ان التوقيع الرقمي والملف في نفس المسار فقط قم بالضغط على salary.zip.sig اذا كان الملف هو الملف الحقيقي والذي لم يتعرض لأي تغيير اثناء النقل ، فإنه ستظهر لك هذه الرسالة:



في حالة ان الملف والتوقيع في مسارين مختلفين ، فإن التوقيع الرقمي يطلب منك تحديد مسار الملف، لكي يقوم بالتا



التأكد من سلامته الملف في حالة ان الملف ليس سليم، او تعرض للتغيير اثناء عملية النقل ، ستظهر لك هذه الرسالة:



فهم مفهوم الهجمات على التشفير والتوقيع الرقمي. الهجمات على التشفير:

1. الهجوم بالفيروسات: يتم تضمين برنامج خبيث في ملفات قابلة للتنفيذ يستهدف أجهزة الكمبيوتر. يهدف هذا النوع من الهجمات إلى التسلل إلى النظام وتدمير الملفات أو سرقة المعلومات الحساسة. يتم استدراج الضحايا إلى تشغيل هذه البرامج الخبيثة عبر الضغط على مرفقات البريد الإلكتروني أو زيارة مواقع ويب مشبوهة.
2. الهجوم بواسطة البرمجيات الخبيثة: يتم تضمين برمجيات ضارة في تطبيقات قد تكون غير آمنة. يستهدف هذا النوع من الهجمات ثغرات في النظام أو البرامج للوصول إلى المعلومات أو تعطيل الخدمات.

الهجمات على التوقيع الرقمي:

1. التصيد الاحتيالي: يستخدم تقنيات اجتماعية لخداع الأفراد لتقديم معلومات حساسة مثل اسم المستخدم وكلمة المرور. يعتمد هذا النوع من الهجمات على اختراق عقلية الفرد، مستفيدين من الأمانة الشخصية والثقة المفرطة.
2. هجمات الحجب الخدمي: يتم تعطيل الخدمات عبر الإنترنت باستخدام تقنيات مثل توجيه حركة المرور الزائفة أو تنفيذ هجمات تكنولوجيا التوجيه (DDoS) يتم زيادة حجم حركة المرور المتجهة نحو الخدمة المستهدفة بشكل كبير، مما يتسبب في تعطيل الخدمة للمستخدمين الشرعيين.

طرق حماية التشفير والتوقيع الرقمي من الهجمات:

- استخدام خوارزميات التشفير والتوقيع الرقمي القوية.
- استخدام مفاتيح التشفير والتوقيع الرقمي الطويلة.
- تخزين مفاتيح التشفير والتوقيع الرقمي في مكان آمن.
- استخدام بروتوكولات التشفير الآمنة.
- تحديث برامج التشفير والتوقيع الرقمي بانتظام.
- تثقيف المستخدمين حول مخاطر الأمن السيبراني وكيفية حماية البيانات والمعلومات الحيوية.

فهم هذه الهجمات يساعد في تطوير استراتيجيات الحماية والتصدي لها. يجب على الأفراد والمؤسسات اتخاذ إجراءات وقائية فعالة لا يوجد نظام تشفير أو توقيع رقمي آمن تمامًا ومع ذلك يمكن تقليل مخاطر التعرض للهجوم بشكل كبير من خلال اتباع أفضل الممارسات.

تطبيق أساليب حماية البيانات والمعلومات الحيوية.

حماية البيانات هي عملية حماية البيانات المهمة. طريقة حماية البيانات الهامة من سرقة البيانات والفساد وسوء الاستخدام وأنواع التلف الأخرى. تعد خصوصية البيانات جزءًا من إدارة البيانات. ويسمى أيضًا خصوصية البيانات. تضمن خصوصية البيانات أمان البيانات التي يتلقاها العملاء ، وتخزين البيانات واستخدامها للغرض المقصود. تتحكم خصوصية البيانات في كيفية جمع البيانات التي تم الحصول عليها ومشاركتها واستخدامها. ضمان كل هذه الأشياء هو المهمة الرئيسية لخصوصية البيانات.

يمكن تقسيم أساليب حماية البيانات والمعلومات الحيوية إلى ثلاث فئات رئيسية:

1. أساليب الفنى و تقنية:

- التشفير: تحويل البيانات إلى شكل غير قابل للقراءة إلا من قبل الأشخاص الذين يملكون مفتاح فك التشفير.
- التوقيع الرقمي: ربط توقيع رقمي ببيانات إلكترونية للتحقق من صحتها ومنع التزوير.
- التحكم في الوصول: تحديد من يمكنه الوصول إلى البيانات والمعلومات الحيوية.
- النسخ الاحتياطي: إنشاء نسخ احتياطية من البيانات والمعلومات الحيوية في مكان آمن.
- مراقبة الأمان: مراقبة الأنظمة والشبكات للكشف عن أي نشاط مشبوه.

2. أساليب إدارية:

- وضع سياسة أمان شاملة: تحديد قواعد وإجراءات لحماية البيانات والمعلومات الحيوية.
- تثقيف المستخدمين حول مخاطر الأمن السيبراني: تعليم المستخدمين كيفية حماية البيانات والمعلومات الحيوية.
- إجراء اختبارات اختراق منتظمة: اختبار أنظمة وأمن الشبكات للكشف عن نقاط الضعف.
- وضع خطة استجابة للطوارئ: تحديد كيفية التعامل مع الأحداث الأمنية.

3. أساليب قانونية:

- سن قوانين لحماية البيانات والمعلومات الحيوية: ضمان حماية البيانات والمعلومات الحيوية بموجب القانون.
- ملاحقة المتسللين: اتخاذ الإجراءات القانونية ضد المتسللين الذين ينتهكون أمن البيانات والمعلومات الحيوية.

أمثلة على تطبيق أساليب حماية البيانات والمعلومات الحيوية:

1. حماية كلمات المرور: استخدام خوارزميات التشفير القوية لتشفير كلمات المرور المخزنة على أجهزة الكمبيوتر أو المواقع الإلكترونية.
2. تأمين البيانات على الأجهزة المحمولة: استخدام برامج التشفير لتشفير البيانات الموجودة على الهواتف الذكية والأجهزة اللوحية.
3. حماية الاتصالات عبر الإنترنت: استخدام بروتوكولات التشفير مثل TLS و HTTPS لتشفير الاتصالات عبر الإنترنت، مثل البريد الإلكتروني أو مكالمات الفيديو.
4. التوقيع على المستندات إلكترونياً: استخدام التوقيعات الرقمية للتوقيع على العقود والوثائق الأخرى إلكترونياً.
5. التحقق من صحة البرامج: استخدام التوقيعات الرقمية للتحقق من صحة البرامج قبل تثبيتها على جهاز الكمبيوتر.
6. ضمان سلامة وسرية البيانات: استخدام التوقيعات الرقمية للتأكد من أن البيانات لم يتم تغييرها منذ توقيعها وللتأكد من هوية الشخص الذي وقع عليها.


خصائص وثيقة السياسة الأمنية العامة

1. تكون منظمة ومرتبطة ومبوبة تكون مكتوبة بلغة فقا لمهام المنشأة واضحة سهلة الفهم والتطبيق.
2. تحدد فيها المسؤوليات والصلاحيات بكل دقة تبع تحديد.
3. تبع تحديد الإجراءات التي يجب أن تكون بكل دقة عند ظهور أي مشكلة.



الوحدة الخامسة

دراسة أمن المعلومات وأساليب الهجوم السيبراني.

- فهم مفهوم أمن المعلومات.
 - فهم مفهوم الهجوم السيبراني.
 - تحليل المخاطر والتقييم الأمني.
 - تطبيق تقنيات الحماية.
 - تحليل الهجمات السيبرانية.
 - تطبيق أساليب الوقاية والتدريب.
- 

دراسة أمن المعلومات وأساليب الهجوم السيبراني.

في عصرنا الرقمي، أصبحت المعلومات هي العملة الجديدة، وأمنها يمثل أولوية قصوى للأفراد والمؤسسات على حد سواء.

لذلك، ازدادت أهمية دراسة أمن المعلومات وأساليب الهجوم السيبراني لفهم كيفية حماية البيانات والأنظمة من المخاطر المتزايدة.

أهمية دراسة أمن المعلومات وأساليب الهجوم السيبراني:

1. فهم المخاطر: تساعد دراسة أمن المعلومات على فهم المخاطر التي تواجهها البيانات والأنظمة، مثل البرامج الضارة، والهجمات الإلكترونية، والهندسة الاجتماعية.
2. تطوير استراتيجيات الحماية: يمكن تحليل أساليب الهجوم السيبراني لتطوير استراتيجيات فعالة لحماية البيانات والأنظمة.
3. بناء الوعي: تزيد دراسة أمن المعلومات من وعي المستخدمين بالمخاطر وأفضل الممارسات لحماية أنفسهم.
4. تلبية متطلبات العمل: تتطلب العديد من الوظائف مهارات في أمن المعلومات، مثل تحليل المخاطر واختبار الاختراق.

فهم مفهوم أمن المعلومات.

ما هو أمن المعلومات: هو مجموعة من الممارسات والحلول التي تهدف إلى حماية المعلومات من التهديدات الداخلية والخارجية. يشمل ذلك ضمان سرية المعلومات وسلامتها وتوافرها للمستخدمين المخولين فقط.

أهمية أمن المعلومات:

1. حماية البيانات الحساسة: تهدف المعلومات الحساسة إلى حماية البيانات الحساسة، مثل المعلومات الشخصية، والمعلومات المالية، والملكية الفكرية.
2. تقليل المخاطر: يساعد أمن المعلومات على تقليل المخاطر التي تواجهها المنظمات، مثل المخاطر المالية، والسمعة، والتشغيلية.
3. الامتثال للقوانين: تتطلب العديد من القوانين، مثل قانون حماية البيانات، تطبيق ممارسات أمن المعلومات.
4. تعزيز الثقة: يساعد أمن المعلومات على تعزيز ثقة العملاء والمستثمرين في المنظمة.

عناصر أمن المعلومات:

1. السرية: ضمان عدم الوصول إلى المعلومات إلا من قبل المستخدمين المخولين.

2. النزاهة: ضمان دقة المعلومات واكتمالها.
3. التوافر: ضمان توفر المعلومات للمستخدمين المخولين عند الحاجة إليها.
4. اللا إنكار: ضمان قدرة المنظمة على إثبات صحة المعلومات ورفض أي إنكار لها.

فهم مفهوم الهجوم السيبراني.

ما هو الهجوم السيبراني:

هو أي عمل متعمد يهدف إلى الوصول غير المصرح به إلى المعلومات أو الأنظمة أو تعطيلها أو تدميرها. يمكن أن ينفذ من قبل قراصنة أو مجرمين إلكترونيين أو جهات حكومية أو حتى موظفين داخل المنظمة.

أنواع الهجمات السيبرانية:

1. البرامج الضارة: برامج ضارة تُستخدم لسرقة البيانات أو تعطيل الأنظمة.
2. هجمات التصيد الاحتيالي: رسائل بريد إلكتروني أو رسائل نصية خادعة تهدف إلى خداع المستخدمين للكشف عن معلوماتهم الشخصية.
3. هجمات رفض الخدمة: هجمات تهدف إلى إغراق خادم أو شبكة بالطلبات، مما يجعلها غير متاحة للمستخدمين الشرعيين.
4. هجمات الهندسة الاجتماعية: تقنيات تعتمد على التلاعب النفسي لخداع المستخدمين للكشف عن معلوماتهم أو تنفيذ إجراءات ضارة.

خطوات لمنع الهجمات السيبرانية:

1. تطبيق سياسة أمن المعلومات: يجب أن يكون لدى المنظمة سياسة أمن معلومات تحدد متطلبات الأمن.
2. التوعية بأمن المعلومات: يجب أن يكون جميع المستخدمين على دراية بمخاطر أمن المعلومات وأفضل الممارسات لحماية أنفسهم.
3. التحكم في الوصول: يجب أن يكون الوصول إلى المعلومات محدودًا بالمستخدمين الذين يحتاجون إليها لأداء وظائفهم.
4. استخدام حلول الأمن: يجب استخدام حلول الأمن، مثل جدران الحماية، وبرامج مكافحة الفيروسات، وأنظمة الكشف عن الاختراق.
5. التدقيق والتقييم: يجب مراجعة ممارسات أمن المعلومات بشكل دوري لتقييم فعاليتها.

أهداف الهجمات السيبرانية:

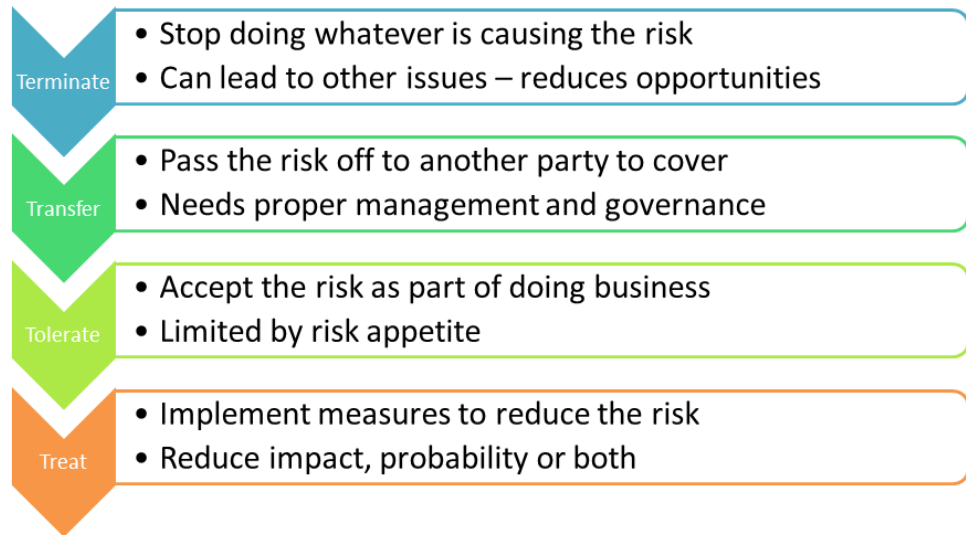
1. سرقة البيانات: سرقة المعلومات الحساسة، مثل المعلومات الشخصية، والمعلومات المالية، والملكية الفكرية.

2. تعطيل الأنظمة: تعطيل الأنظمة الحاسوبية أو الشبكات، مما يؤدي إلى انقطاع الخدمة أو فقدان البيانات.
3. تدمير البيانات: تدمير البيانات أو إتلافها، مما قد يؤدي إلى خسائر مالية أو تشغيلية كبيرة.
4. التجسس: جمع المعلومات الاستخبارية عن المنظمة أو الأفراد.
5. التشهير: الإضرار بسمعة المنظمة أو الفرد.

تحليل المخاطر والتقييم الأمني.

تحليل مخاطر الأمان (SRA) هو عملية تحديد وتقييم وتخفيف مخاطر الأمان المحتملة. إنه جزء أساسي من إدارة المخاطر، وخطوة أساسية في أي جهود للمنظمات لحماية بياناتها وأصولها هي عملية وليست منتجاً. لا ينطوي الأمر ببساطة على حساب عدد الحوادث الأمنية أو حساب القيمة الدولارية للبيانات المفقودة أو المسروقة. بدلاً من ذلك، يتعلق SRA بفهم النطاق الكامل للمخاطر من التهديدات منخفضة المستوى إلى الهجمات المدمرة وتحديد تلك التي تشكل أكبر تهديد لأمن مؤسستك.

Security Risk Response Options



من المهم فهم المفاهيم التالية:

1. المخاطرة: العواقب المحتملة لحدث أو ضعف أو تهديد.
2. الثغرات الأمنية: أوجه القصور في تصميم النظام أو التطبيق أو التطبيق الذي يسمح للمهاجم باستغلالها.

3. الحوادث: الأحداث التي يمكن أن تؤدي إلى استغلال الضعف.

4. التأثير: عواقب حادث أو ضعف أو تهديد.

هناك ثلاث مراحل أساسية في SRA تحديد المخاطر، وتقييم المخاطر، وتخفيف المخاطر.

1. **تحديد المخاطر هو الخطوة الأولى في SRA.** يتضمن تحديد المخاطر الأمنية المحتملة

على الصعيدين الداخلي والخارجي لمؤسستك وتقييم مدى خطورتها. يتضمن ذلك فهم طبيعة التهديد (على سبيل المثال، الجريمة الإلكترونية، وسرقة البيانات، والتهديدات الداخلية)، والأضرار المحتملة التي يمكن أن تحدث، واحتمال حدوثها.

2. **تقييم المخاطر هو الخطوة الثانية في SRA.** إنه يحدد أي مخاطر أمنية هي الأكثر تهديداً

لمؤسستك ويحدد أفضل السبل للتخفيف منها. يتضمن ذلك حساب احتمالية الحدوث، والأضرار المحتملة التي يمكن أن تحدث، وتكلفة منع هذا الضرر.

3. **التخفيف من المخاطر هو الخطوة الأخيرة في SRA.** إنه ينطوي على تنفيذ تدابير لمنع أو

تقليل الضرر المحتمل الناجم عن المخاطر الأمنية المحددة. قد يشمل ذلك تنفيذ إجراءات أمنية جديدة، أو تدريب الموظفين على كيفية استخدام هذه الإجراءات، أو إصدار تنبيهات وتحذيرات حول التهديدات المحتملة

الخطوات المتضمنة في تحليل المخاطر الأمنية

تحليل المخاطر الأمنية هو عملية تحديد وتقييم المخاطر الأمنية المحتملة المرتبطة بنظام أو أصل معين. الهدف من هذه العملية هو ضمان بقاء النظام أو الأصل آمناً وأمناً من الهجمات المحتملة.

هناك عدد من الخطوات المتضمنة في إجراء تحليل المخاطر الأمنية. فيما يلي قائمة بالخطوات الرئيسية:

1. **التعريف:** تتمثل الخطوة الأولى في تحليل المخاطر الأمنية في تحديد النظام أو الأصل قيد

المراجعة. يمكن القيام بذلك من خلال المقابلات مع أصحاب المصلحة أو تحليل البيانات.

2. **التقييم:** بمجرد تحديد النظام أو الأصل، فإن الخطوة التالية هي تقييم المخاطر التي تشكلها

هذه التهديدات. يتضمن ذلك تقييم شدة التهديد، وتحديد ما إذا كان قد تم استغلاله مسبقاً، وحساب احتمالية حدوثه مرة أخرى.

3. **تحديد الأولويات:** بمجرد تقييم المخاطر، يجب ترتيبها حسب الأولوية. يتضمن ذلك تحديد

التهديدات التي تشكل أكبر تهديد للنظام أو الأصل وترتيبها حسب الأهمية.

4. **الوقاية:** بمجرد ترتيب المخاطر حسب الأولوية، من المهم وضع تدابير لمنع حدوثها.

يتضمن ذلك تنفيذ سياسات الأمان وتثبيت تحديثات وتصحيحات البرامج وتدريب

الموظفين على كيفية استخدام النظام بأمان.

يعد تحليل المخاطر الأمنية عملية أساسية لأي مؤسسة تريد الحفاظ على أنظمتها وأصولها في مأمن من الهجمات المحتملة. باتباع هذه الخطوات، يمكن للمنظمات ضمان أن أنظمتها آمنة من الأذى وتظل عاملة طوال أي موقف غير متوقع.

تطبيق تقنيات الحماية.

تقنيات الحماية هي مجموعة من الأدوات والعمليات التي تُستخدم لحماية المعلومات والأنظمة من المخاطر الداخلية والخارجية.

تشمل تقنيات الحماية:

- التحكم في الوصول: تحديد المستخدمين الذين يمكنهم الوصول إلى المعلومات والأنظمة.
- التشفير: تحويل المعلومات إلى نص مشفر لا يمكن قراءته إلا من قبل المستخدمين المخولين.
- جدران الحماية: منع الوصول غير المصرح به إلى الشبكات والأجهزة.
- برامج مكافحة الفيروسات: اكتشاف وإزالة البرامج الضارة من الأجهزة.
- أنظمة الكشف عن الاختراق: اكتشاف الأنشطة المشبوهة التي قد تشير إلى هجوم إلكتروني.
- التوعية بأمن المعلومات: توعية المستخدمين بمخاطر أمن المعلومات وأفضل الممارسات لحماية أنفسهم.

أهمية تطبيق تقنيات الحماية:

1. حماية المعلومات الحساسة: تهدف تقنيات الحماية إلى حماية المعلومات الحساسة، مثل المعلومات الشخصية، والمعلومات المالية، والملكية الفكرية.
2. تقليل المخاطر: تساعد تقنيات الحماية على تقليل المخاطر التي تواجهها المنظمات، مثل المخاطر المالية، والسمعة، والتشغيلية.
3. الامتثال للقوانين: تتطلب العديد من القوانين، مثل قانون حماية البيانات، تطبيق تقنيات الحماية.
4. تعزيز الثقة: يساعد تطبيق تقنيات الحماية على تعزيز ثقة العملاء والمستثمرين في المنظمة.

خطوات لتطبيق تقنيات الحماية:

1. تحديد المخاطر: يجب تحديد المخاطر التي تواجهها المنظمة لتحديد تقنيات الحماية المناسبة.
2. تقييم تقنيات الحماية: يجب تقييم تقنيات الحماية المختلفة لتحديد تقنية الحماية التي تلبي احتياجات المنظمة.

3. تنفيذ تقنيات الحماية: يجب تنفيذ تقنيات الحماية بشكل صحيح لضمان فعاليتها.
4. إدارة تقنيات الحماية: يجب إدارة تقنيات الحماية بشكل مستمر لضمان مواكبة التهديدات المتغيرة.

نصائح لتطبيق تقنيات الحماية:

- ابدأ من الصفر: تأكد من أن لديك أساسًا متينًا من أمن المعلومات قبل تطبيق تقنيات جديدة.
- استخدم نهجًا متعدد الطبقات: لا تعتمد على تقنية واحدة لحماية معلوماتك.
- ابق على اطلاع دائم: ابق على اطلاع دائم بأحدث التهديدات وتقنيات الحماية.
- اختبر تقنيات الحماية: اختبر تقنيات الحماية بشكل دوري لضمان فعاليتها.
- قم بتثقيف المستخدمين: قم بتثقيف المستخدمين حول مخاطر أمن المعلومات وأفضل الممارسات لحماية أنفسهم.

تطبيقات مكافحة الفيروسات والحماية المتاحة لأجهزة الكمبيوتر والهواتف المحمولة بعض الخيارات المجانية والموثوقة:

- تطبيق Avast Free Antivirus : تطبيق مجاني يحمي جهاز الكمبيوتر الخاص بك من الفيروسات والبرمجيات الخبيثة. يُعتبر Avast من أكثر البرامج شهرةً واستخدامًا حول العالم.
- تطبيق Kaspersky Free Antivirus : تطبيق مجاني يوفر حماية قوية ضد الفيروسات والبرمجيات الخبيثة. يمكنك تجربته لمدة 30 يومًا.
- تطبيق Microsoft Defender : برنامج مكافحة البرمجيات الخبيثة المدمج مع نظام التشغيل Windows. يوفر حماية أساسية ويتم تحديثه تلقائيًا من خلال Windows Update.

تحليل الهجمات السيبرانية.

- قبل التعرف على طريقة تقييم المخاطر السيبرانية يجب النظر أولاً على مفهوم مخاطر الأمن السيبراني ومراحل إدارتها، يشير مفهوم مخاطر الأمن السيبراني إلى التهديدات والهجمات الإلكترونية المسببة لتعطيل الأنظمة التكنولوجية للمؤسسات وخدماتها الإلكترونية، وهي مخاطر يتعرض لها الأفراد أيضاً.
- ولا تضر هذه المخاطر بتقنيات وأجهزة المؤسسات فحسب بل أيضاً تكبدها خسائر مالية وتلحق أضراراً بسمعتها.

تتطلب المخاطر السيبرانية توفير قسم خاص بإدارة المخاطر يقوم على تحليل الهجمات والتهديدات التي تتعرض لها الأنظمة الإلكترونية للمؤسسات ووضع خطة للتصدي لها باستخدام التقنيات والأدوات الحديثة.

دارة مخاطر الأمن السيبراني على أنها مجموعة خطوات تتخذ بشكل دوري لمواجهة التهديدات الإلكترونية ومعالجتها من خلال رصدها وتحديدها وتقييمها، ومن أجل إدارتها بفاعلية فإن ذلك يتطلب نظرة شاملة لهذه المخاطر وتعاون من كافة أفراد العمل، ليس فقط من أفراد إدارة المخاطر وإنما أفراد الإدارات الأخرى.

وتُعرف إدارة مخاطر الأمن السيبراني أيضاً بأنها عملية مستمرة لتحديد وتحليل وتقييم ومعالجة تهديدات الأمن السيبراني التي تواجهها المؤسسة.

تعتمد إدارة مخاطر الأمن السيبراني على استراتيجيات تساعد على ترتيب أولويات المخاطر المطلوب معالجتها؛ لرصد التهديدات الأكثر ضرراً والمطلوب مواجهتها في الوقت المطلوب.

1- تحديد المخاطر: يعمل القائمون على إدارة المخاطر في تلك المرحلة على تحديد التهديدات المحتملة سواء في الوقت الحالي أو في المستقبل، كما أن هذه المرحلة تتطلب معرفة وتحديد بيانات وبرامج وأجهزة المنظمة.

2- الحماية من المخاطر: تستهدف هذه المرحلة حماية البيانات والبرامج والأجهزة الخاصة بالمنظمة، وذلك من خلال تطبيق وسائل الحماية من أبرزها استخدام برامج مكافحة الفيروسات.

3- كشف المخاطر

تتطلب هذه المرحلة الكشف عن المخاطر المحتملة عبر تنفيذ أنظمة رصد التهديدات الإلكترونية.

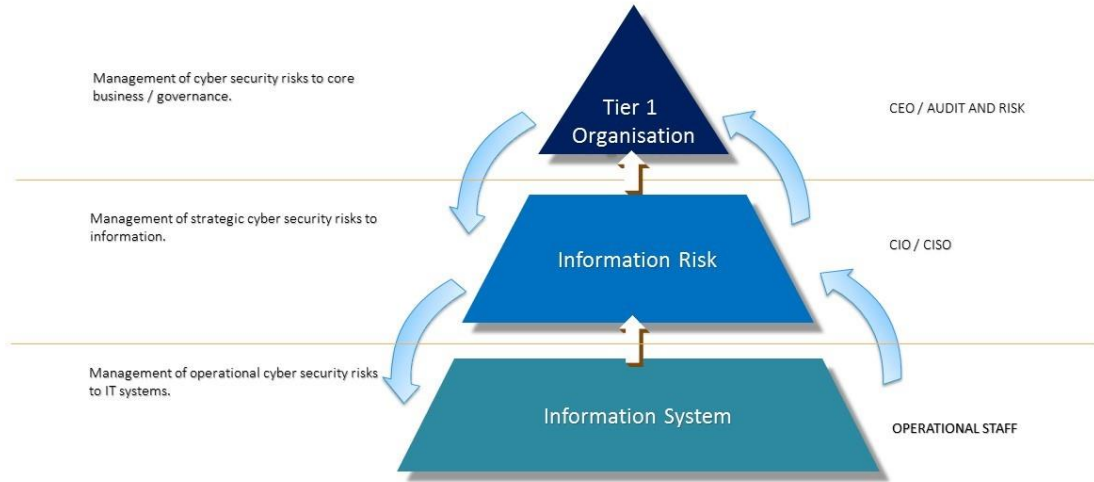
4- الاستجابة للمخاطر

عقب الانتهاء من مرحلة رصد المخاطر تأتي مرحلة الاستجابة والتي تُطبق فيها استراتيجيات بالاستجابة للمخاطر والتي تتضمن الاتصال والتعافي والاستجابة للتهديدات.

5- التعافي من المخاطر

العودة إلى الوضع الافتراضي قبل التعرض للتهديدات الإلكترونية هو ما تتطلبه هذه المرحلة من أجل سير العمل من جديد، كما أنها خطوة تستهدف الحد من حوادث الهجوم الإلكتروني فيما بعد من خلال تطوير البرامج الخاصة بالأمن السيبراني.

Cyber Security Risk Management Process



خطوات عملية إدارة مخاطر الأمن السيبراني:

1. تحديد النطاق والسياق العام والمعايير:
 - تحديد الأصول والعمليات ذات الصلة بالمنظمة وطريقة استخدامها.
 - تحديد السياق العام الداخلي والخارجي لعملية إدارة مخاطر الأمن السيبراني.
 - تحديد المعايير التي سيتم استخدامها لتقييم المخاطر.
2. تقييم مخاطر الأمن السيبراني:
 - تحديد التهديدات والثغرات المتعلقة بالأمن السيبراني التي قد تؤثر على الأصول المعلوماتية والتقنية.
 - تقييم احتمالية وتأثير المخاطر المحددة.
3. معالجة مخاطر الأمن السيبراني:
 - تحديد أساليب التعامل مع المخاطر السيبرانية.
 - تنفيذ الضوابط والتدابير للحد من المخاطر إلى مستوى مقبول.
4. التسجيل وإعداد التقارير:
 - توثيق عملية إدارة مخاطر الأمن السيبراني.
 - إعداد تقارير منتظمة للإدارة وأصحاب المصلحة.
5. التواصل والمتابعة:
 - التواصل مع جميع أصحاب المصلحة حول عملية إدارة مخاطر الأمن السيبراني.

- مراجعة وتحديث عملية إدارة مخاطر الأمن السيبراني بشكل منتظم.

نصائح عند القيام بهذه الخطوات:

- هذه الخطوات هي عملية مستمرة يجب مراجعتها وتحديثها بشكل منتظم.
- يجب أن تكون عملية إدارة مخاطر الأمن السيبراني متكاملة مع العمليات الأخرى للمنظمة.
- يجب أن يكون لدى المنظمة فريق متخصص لإدارة مخاطر الأمن السيبراني.

بعض الممارسات الجيدة لإدارة مخاطر الأمن السيبراني:

- استخدام أدوات تقييم المخاطر.
- تطبيق مبادئ الأمن السيبراني الأساسية.
- إجراء اختبارات اختراق منتظمة.
- توفير برامج تدريبية للتوعية الأمنية للموظفين.

تطبيق أساليب الوقاية والتدريب.

يعد أمن المعلومات أحد أهم العوامل التي تضمن استمرارية الأعمال وحماية البيانات الحساسة من المخاطر المتزايدة في عالمنا الرقمي.

أساليب الوقاية:

1. التحكم في الوصول: تحديد المستخدمين الذين يمكنهم الوصول إلى المعلومات والأنظمة، وتحديد مستوى الوصول لكل مستخدم.
2. التشفير: تحويل المعلومات إلى نص مشفر لا يمكن قراءته إلا من قبل المستخدمين المخولين.
3. جدران الحماية: منع الوصول غير المصرح به إلى الشبكات والأجهزة.
4. برامج مكافحة الفيروسات: اكتشاف وإزالة البرامج الضارة من الأجهزة.
5. أنظمة الكشف عن الاختراق: اكتشاف الأنشطة المشبوهة التي قد تشير إلى هجوم إلكتروني.
6. التوعية بأمن المعلومات: توعية المستخدمين بمخاطر أمن المعلومات وأفضل الممارسات لحماية أنفسهم.

التدريب:

1. تدريب المستخدمين على ممارسات أمن المعلومات: يجب أن يتلقى جميع المستخدمين تدريباً على ممارسات أمن المعلومات، مثل إنشاء كلمات مرور قوية وفريدة من نوعها، وتجنب مشاركة المعلومات الشخصية، وتوخي الحذر عند استخدام الإنترنت.
2. تدريب متخصصي أمن المعلومات: يجب أن يتلقى متخصصي أمن المعلومات تدريباً متقدماً على تقنيات وأساليب أمن المعلومات، مثل اختبار الاختراق وتحليل المخاطر.

أهمية تطبيق أساليب الوقاية والتدريب:

1. حماية المعلومات الحساسة: تهدف أساليب الوقاية والتدريب إلى حماية المعلومات الحساسة، مثل المعلومات الشخصية، والمعلومات المالية، والملكية الفكرية.
2. تقليل المخاطر: تساعد أساليب الوقاية والتدريب على تقليل المخاطر التي تواجهها المنظمات، مثل المخاطر المالية، والسمعة، والتشغيلية.
3. الامتثال للقوانين: تتطلب العديد من القوانين، مثل قانون حماية البيانات، تطبيق أساليب الوقاية والتدريب.
4. تعزيز الثقة: يساعد تطبيق أساليب الوقاية والتدريب على تعزيز ثقة العملاء والمستثمرين في المنظمة.



الوحدة السادسة

الدفاع عن المعلومات وأساليب الحماية السيبرانية

- فهم مفهوم الدفاع عن المعلومات.
- فهم مفهوم الأمان السيبراني.
- تحليل المخاطر والتقييم الأمني.
- تطبيق تقنيات الحماية.
- تطبيق أساليب الوقاية والاستجابة.
- تحليل الهجمات السيبرانية.

الدفاع عن المعلومات وأساليب الحماية السيبرانية

في عالمنا الرقمي المترابط، يزداد الاعتماد على المعلومات الرقمية بشكل متسارع، مما يجعلها عرضة للتهديدات والمخاطر المختلفة.

الدفاع عن المعلومات:

يشير مصطلح "الدفاع عن المعلومات" إلى مجموعة من الإجراءات والتقنيات التي تُستخدم لحماية المعلومات من الوصول غير المصرح به، والاستخدام غير السليم، والتغيير، أو التدمير.

تحليل الهجمات السيبرانية:

يجب تحليل الهجمات السيبرانية بدقة لفهم كيفية تنفيذها والأضرار المحتملة.

يشمل ذلك تحديد نقاط الضعف والثغرات في الأنظمة والشبكات.

تقييم المخاطر:

يجب تقييم المخاطر السيبرانية لتحديد الأولويات وتطبيق استراتيجيات الأمان.

يشمل ذلك تحديد قيمة المعلومات وتحديد البنية التحتية التكنولوجية للمؤسسة.

أنواع المخاطر السيبرانية:

التنصت: اختراق الأنظمة والاستماع إلى البيانات.

الاختراق: اختراق الأمان والوصول غير المصرح به.

التصيد: استغلال الأخطاء البشرية للوصول إلى المعلومات.

التشويش: تعطيل الخدمات الإلكترونية.

البرمجيات الخبيثة: الفيروسات والديدان وبرامج التجسس.

تطبيق استراتيجيات الأمان:

يجب أن يكون الأمن السيبراني جزءاً من استراتيجية المؤسسة للتعامل مع هذه المخاطر.

يجب تحديث استراتيجيات الأمان بشكل دوري للتصدي للتهديدات الجديدة.

فهم مفهوم الدفاع عن المعلومات.

يشير مصطلح "الدفاع عن المعلومات" إلى مجموعة من الإجراءات والتقنيات التي تُستخدم لحماية المعلومات من الوصول غير المصرح به، والاستخدام غير السليم، والتغيير، أو التدمير.

أهداف الدفاع عن المعلومات:

1. حماية البيانات الحساسة: تهدف أساليب الدفاع عن المعلومات إلى حماية البيانات الحساسة، مثل المعلومات الشخصية، والمعلومات المالية، والملكية الفكرية.

2. تقليل المخاطر: تساعد أساليب الدفاع عن المعلومات على تقليل المخاطر التي تواجهها المنظمات، مثل المخاطر المالية، والسمعة، والتشغيلية.
3. الامتثال للقوانين: تتطلب العديد من القوانين، مثل قانون حماية البيانات، تطبيق أساليب الدفاع عن المعلومات.
4. تعزيز الثقة: يساعد تطبيق أساليب الدفاع عن المعلومات على تعزيز ثقة العملاء والمستثمرين في المنظمة.

عناصر الدفاع عن المعلومات:

1. السرية: ضمان عدم الوصول إلى المعلومات إلا من قبل المستخدمين المخولين.
2. النزاهة: ضمان دقة المعلومات واكتمالها.
3. التوافر: ضمان توفر المعلومات للمستخدمين المخولين عند الحاجة إليها.
4. اللا إنكار: ضمان قدرة المنظمة على إثبات صحة المعلومات ورفض أي إنكار لها.

أنواع التهديدات التي تواجه الدفاع عن المعلومات:

1. البرامج الضارة: برامج ضارة تُستخدم لسرقة البيانات أو تعطيل الأنظمة.
2. هجمات التصيد الاحتيالي: رسائل بريد إلكتروني أو رسائل نصية خادعة تهدف إلى خداع المستخدمين للكشف عن معلوماتهم الشخصية.
3. هجمات رفض الخدمة: هجمات تهدف إلى إغراق خادم أو شبكة بالطلبات، مما يجعلها غير متاحة للمستخدمين الشرعيين.
4. هجمات الهندسة الاجتماعية: تقنيات تعتمد على التلاعب النفسي لخداع المستخدمين للكشف عن معلوماتهم أو تنفيذ إجراءات ضارة.

ممارسات الدفاع عن المعلومات الجيدة:

1. تطبيق سياسة أمن المعلومات: يجب أن يكون لدى المنظمة سياسة أمن معلومات تحدد متطلبات الأمن.
2. التوعية بأمن المعلومات: يجب أن يكون جميع المستخدمين على دراية بمخاطر أمن المعلومات وأفضل الممارسات لحماية أنفسهم.
3. التحكم في الوصول: يجب أن يكون الوصول إلى المعلومات محدودًا بالمستخدمين الذين يحتاجون إليها لأداء وظائفهم.
4. استخدام حلول الأمن: يجب استخدام حلول الأمن، مثل جدران الحماية، وبرامج مكافحة الفيروسات، وأنظمة الكشف عن الاختراق.

5. التدقيق والتقييم: يجب مراجعة ممارسات الدفاع عن المعلومات بشكل دوري لتقييم فعاليتها.

فهم مفهوم الأمان السيبراني.

مفهوم مخاطر الأمان السيبراني ومراحل إدارتها، يشير مفهوم مخاطر الأمان السيبراني إلى التهديدات والهجمات الإلكترونية المسببة لتعطيل الأنظمة التكنولوجية للمؤسسات وخدماتها الإلكترونية، وهي مخاطر يتعرض لها الأفراد أيضاً.

ولا تضر هذه المخاطر بتقنيات وأجهزة المؤسسات فحسب بل أيضاً تكبدها خسائر مالية وتلحق أضراراً بسمعتها. بأنه الأمان الذي يُعنى بتطبيق التقنيات، والعمليات، والضوابط؛ بهدف حماية الأنظمة، وشبكات الحواسيب، والبرامج، والأجهزة، والبيانات من التعرض للهجمات الإلكترونية.

عناصر الأمان السيبراني تشمل:

1. الأشخاص: يشمل الأشخاص المعنيين بإدارة شبكة الأمان السيبراني، ويجب أن يكونوا قادرين على التحقق من التهديدات الإلكترونية والتعامل معها.
2. السلطة: يجب تعيين شخص مسؤول عن تنفيذ استراتيجية الأمان السيبراني ومنحه النفوذ اللازم لتطبيق التغييرات المطلوبة.
3. الدعم من الإدارة العليا: يجب أن يحظى برنامج الأمان السيبراني بدعم كامل من مجلس الإدارة وفريق القيادة.
4. العملية الفعالة: يجب أن يشمل برنامج الأمان السيبراني على نهج فعال لإدارة الأمان ومواجهة المخاطر الإلكترونية.
5. التقنيات المناسبة: يجب أن تكون التقنيات المستخدمة قادرة على مواجهة التهديدات المكتشفة والتحقيق في التهديدات المحتملة.
6. التواصل في الوقت المناسب: يجب التنسيق بين فريق الأمان السيبراني والجهات الأخرى داخل المؤسسة.
7. الميزانية: يتطلب نجاح برنامج الأمان السيبراني تخصيص ميزانية مناسبة له.
8. باختصار، الأمان السيبراني يعد جزءاً أساسياً من الحفاظ على سلامة البيانات والمعلومات في عالمنا الرقمي المتطور

تحليل المخاطر والتقييم الأمني.

هناك عدة خطوات متضمنة في إجراء تحليل مخاطر الأمان.

1. الخطوة الأولى هي تحديد أنواع المخاطر التي يجب تقييمها. يمكن القيام بذلك من خلال مراجعة سياسات المنظمة وإجراءاتها، بالإضافة إلى المشهد الحالي لتهديدات الأمان السيبراني.

2. الخطوة الثانية هي تحديد المخاطر الأكثر أهمية بالنسبة للمنظمة. يمكن القيام بذلك عن طريق تحديد الأنظمة أو البيانات أو الأصول الهامة، أو عن طريق تصنيف المخاطر وفقاً لشدتها.

3. الخطوة الثالثة هي تحديد مقدار المخاطر التي يشكلها كل خطر على المنظمة. يمكن القيام بذلك عن طريق حساب احتمال حدوث تهديد، وتأثير التهديد في حالة حدوثه، وتكلفة التخفيف من هذا الخطر.

4. الخطوة الرابعة هي تطوير خطة التخفيف لكل خطر محدد. يجب أن تتضمن هذه الخطة تدابير لتقليل احتمالية حدوث تهديد، وتأثير التهديد في حالة حدوثه، والتكلفة المرتبطة بتخفيف هذا الخطر. أخيراً، يجب تنفيذ الخطة ومراقبتها.

أنواع المخاطر الأمنية

المخاطر الأمنية هي التهديدات لأمن النظام والتي قد تؤدي إلى الوصول غير المصرح به أو تدمير أو تغيير البيانات أو المعلومات. يمكن أن تأتي من عدة مصادر، بما في ذلك المستخدمين غير المصرح لهم والبرامج الضارة وأعطال الأجهزة.

خمسة أنواع رئيسية من مخاطر الأمان:

1. التهديدات من المستخدمين غير المصرح لهم: يمكن للمستخدمين غير المصرح لهم الوصول إلى البيانات أو الأنظمة بطرق قد تؤدي إلى إتلاف أو تدمير النظام أو بياناته. يمكنهم أيضاً الوصول إلى المعلومات أو الأنظمة الحساسة باستخدام بيانات اعتماد الوصول المصرح بها.
 2. التهديدات من البرامج الضارة: يمكن أن تتسبب البرامج الضارة في إتلاف الأنظمة أو تعطيلها، أو سرقة البيانات أو كلمات المرور، أو حتى إصابة أجهزة الكمبيوتر بالفيروسات.
 3. التهديدات من أعطال الأجهزة: يمكن أن تتسبب أعطال الأجهزة في تعطل الأنظمة أو تسرب البيانات أو نقل البيانات دون تأمينها بشكل صحيح.
 4. التهديدات من الإخفاقات التشغيلية: يمكن أن تؤدي الأنظمة سيئة التصميم أو المنفذة إلى تعطل النظام أو الوصول غير المصرح به أو فقدان البيانات.
- التهديدات من الهجمات الجسدية: يمكن أن تنطوي الهجمات الجسدية على الدخول غير المصرح به إلى الأنظمة أو تدمير البيانات أو المعدات.
- تحليل المخاطر الأمنية هو عملية تقييم وتحديد أولويات وإدارة المخاطر المرتبطة باستخدام أنظمة تكنولوجيا المعلومات. إنها خطوة حاسمة في ضمان أمن أنظمة تكنولوجيا المعلومات وبياناتها. الهدف من تحليل المخاطر الأمنية هو تحديد وتقييم التهديدات المحتملة لأمن المعلومات، ووضع خطة للتخفيف من تلك المخاطر.

تطبيق تقنيات الحماية.

الأمان السبيرياني هو مجال حيوي لحماية الأنظمة الرقمية والشبكات الإلكترونية من الهجمات والتهديدات. يعتمد على تقنيات متعددة للحفاظ على سلامة المعلومات وضمان الخصوصية والتوافر. هذه بعض تطبيقات الذكاء الاصطناعي في الأمان السبيرياني:

1. التحقق من الهوية: يساعد الذكاء الاصطناعي المطورين في رفع فاعلية التقنيات الحيوية وزيادة دقتها.
2. خفض هجمات التصيد: يستخدم الذكاء الاصطناعي وتعلم الآلة في صنع أدوات تحدد وتتابع هجمات التصيد وتحد من حدوثها بطريقة أكثر فاعلية من الإنسان.
3. تحليل السلوك: تُصمم خوارزميات تعلم الآلة بطريقة تمكنها من تعلم سلوك المستخدم وخلق نمط خاص به يستفاد منه في تحليل الهجمات.
4. إدارة الثغرات: يستخدم الذكاء الاصطناعي وتعلم الآلة في تقييم الأنظمة بشكل سريع وتحديد نقاط الضعف في الأنظمة والشبكات وكذلك في تصميم أنظمة استباقية لإدارة الثغرات.
5. أمن الشبكات: يعمل الذكاء الاصطناعي على تسريع عملية إنشاء السياسات الأمنية وتحديد تصميم شبكات المؤسسات، بالإضافة إلى إدارة عدد كبير من الأجهزة وتحديثها وتصحيح الأمان فيها تلقائيًا.
6. في الأمان السبيرياني، يجب أن تكون الاستراتيجية شاملة وتأخذ في الاعتبار السياسات والعمليات والتقنيات في كل جانب من جوانب المنظمة.

تطبيق أساليب الوقاية والاستجابة.

أهمية تطبيق أساليب الوقاية والاستجابة:

1. حماية البيانات الحساسة: تهدف أساليب الوقاية والاستجابة إلى حماية البيانات الحساسة، مثل المعلومات الشخصية، والمعلومات المالية، والملكية الفكرية.
2. تقليل المخاطر: تساعد أساليب الوقاية والاستجابة على تقليل المخاطر التي تواجهها المنظمات، مثل المخاطر المالية، والسمعة، والتشغيلية.
3. الامتثال للقوانين: تتطلب العديد من القوانين، مثل قانون حماية البيانات، تطبيق أساليب الوقاية والاستجابة.
4. تعزيز الثقة: يساعد تطبيق أساليب الوقاية والاستجابة على تعزيز ثقة العملاء والمستثمرين في المنظمة.

أمثلة على أساليب الوقاية:

1. التحكم في الوصول: تحديد المستخدمين الذين يمكنهم الوصول إلى المعلومات والأنظمة، وتحديد مستوى الوصول لكل مستخدم.
2. التشفير: تحويل المعلومات إلى نص مشفر لا يمكن قراءته إلا من قبل المستخدمين المخولين.
3. جدران الحماية: منع الوصول غير المصرح به إلى الشبكات والأجهزة.
4. برامج مكافحة الفيروسات: اكتشاف وإزالة البرامج الضارة من الأجهزة.
5. أنظمة الكشف عن الاختراق: اكتشاف الأنشطة المشبوهة التي قد تشير إلى هجوم إلكتروني.
6. التوعية بأمن المعلومات: توعية المستخدمين بمخاطر أمن المعلومات وأفضل الممارسات لحماية أنفسهم.
7. التدريب: تدريب المستخدمين على ممارسات أمن المعلومات، وتدريب متخصصي أمن المعلومات على تقنيات وأساليب أمن المعلومات.

أمثلة على أساليب الاستجابة:

1. خطط الاستجابة للحوادث: وضع خطط محددة للتعامل مع مختلف أنواع الحوادث الأمنية.
2. الاستجابة السريعة: اتخاذ الإجراءات اللازمة للحد من تأثير الحادث الأمني في أسرع وقت ممكن.
3. تحليل الحوادث: تحديد سبب الحادث وتحديد خطوات لمنع تكراره.
4. التعافي من الحوادث: استعادة الأنظمة والبيانات إلى حالتها قبل الحادث.
5. التوثيق: توثيق جميع جوانب الحادث الأمني لأغراض التعلم والامتنال.

تحليل الهجمات السيبرانية:

تحليل وتقييم المخاطر السيبرانية هو عملية أساسية في مجال أمن المعلومات تهدف إلى تحديد وتقييم المخاطر التي قد تواجهها المنظمات والأفراد في العالم الرقمي. لتحليل وتقييم المخاطر السيبرانية بشكل فعال، يجب على المنظمات والأفراد اتباع عملية شاملة تشمل الخطوات التالية:

1. تحديد الموجودات الحساسة: يتعين على المنظمات تحديد المعلومات والأصول الحساسة التي يجب حمايتها، مثل البيانات الشخصية للعملاء أو المعلومات التجارية السرية.
2. تحديد التهديدات المحتملة: يجب تحديد وتصنيف التهديدات المحتملة التي يمكن أن تستهدف الموجودات الحساسة، مثل الاختراقات الإلكترونية، الفيروسات، هجمات الاحتيال عبر البريد الإلكتروني، والتصيد الاحتيالي (Phishing).

3. تقييم الضرر المحتمل: يتعين على المنظمات تقييم الأضرار المحتملة التي يمكن أن تحدث نتيجة للاختراقات السيبرانية، مثل فقدان البيانات، التأثير على العمليات التجارية، والتأثير على السمعة والثقة لدى العملاء.

4. تحديد مستوى الأولوية: يجب تحديد مستوى الأولوية لكل تهديد وفقًا لتأثيره المحتمل واحتمالية حدوثه، مما يساعد في تحديد الموارد والجهود المطلوبة للتعامل مع المخاطر السيبرانية.

5. اتخاذ تدابير الحماية: يتعين على المنظمات اتخاذ تدابير الحماية المناسبة للتصدي للمخاطر السيبرانية، مثل تحديث البرامج والأنظمة بانتظام، واستخدام حلول الأمان القوية مثل جدران الحماية (Firewalls) وبرامج مكافحة الفيروسات.

6. رصد واكتشاف التهديدات: يجب أن يكون لديك نظام رصد قوي لكشف التهديدات السيبرانية المحتملة والهجمات السيبرانية في الوقت الفعلي. هذا يساعد في اكتشاف الاختراقات المحتملة بسرعة واتخاذ التدابير اللازمة.

7. التحقق والاستجابة: في حالة حدوث اختراق سيبراني، يجب أن تكون لديك خطة استجابة وتعامل مع الحوادث السيبرانية. يتضمن ذلك التحقق من أصل المشكلة واستعادة النظام وتعزيز الأمان لتجنب حدوثها مرة أخرى تحليل المخاطر السيبرانية يوفر العديد من الفوائد للمنظمات، بما في ذلك:

- تحسين الأمان السيبراني: يمكن لتحليل المخاطر السيبرانية أن يساعد في تحديد الثغرات والنقاط الضعيفة في نظام المعلومات وتقديم توصيات لتعزيز الأمان وتقليل المخاطر.

- الحد من التكاليف: عن طريق تحديد وتقييم المخاطر المحتملة، يمكن للمنظمات اتخاذ تدابير وقائية للحد من الأضرار والتكاليف المرتبطة بالهجمات السيبرانية.

- الامتثال التنظيمي: يعتبر تحليل المخاطر السيبرانية جزءًا هامًا من الامتثال التنظيمي في مجال أمن المعلومات. يساعد في تلبية متطلبات الامتثال ومعايير الأمان المعترف بها دوليًا.

- الحفاظ على سمعة العلامة التجارية: من خلال تحليل المخاطر والتصدي للتهديدات السيبرانية، يمكن للمنظمات الحفاظ على سمعتها وثقة عملائها والحفاظ على البيانات والمعلومات الحساسة.

في الختام، يمكن القول إن تحليل وتقييم المخاطر السيبرانية هو عملية حيوية لضمان الأمان السيبراني وحماية المعلومات والبيانات الحساسة. من خلال تحليل المخاطر، يمكن للمنظمات تحديد وتقييم

مشروع بحثي يستخدم فيه الطلاب مهارات التشفير والتوقيع الرقمي والحماية السيبرانية التي تم تعلمها في المقرر

1. تحليل وتقييم الضعف الأمني لمواقع الويب وتوفير التوصيات لتحسينها.
2. إنشاء نظام للكشف عن الاختراقات السيبرانية عن طريق مراقبة حركة المرور على الشبكة.
3. تطوير تقنية تشفير جديدة لحماية البيانات الحساسة من الاختراقات السيبرانية.
4. تطوير برنامج لإدارة كلمات المرور وحمايتها من الاختراقات السيبرانية.
5. تطوير نظام للتعرف على البرامج الضارة والحد من انتشارها.
6. إنشاء نظام للكشف عن الهجمات السيبرانية على شبكات IoT الأشياء المتصلة بالإنترنت
7. تطوير تقنية للكشف عن الثغرات الأمنية في أجهزة الكمبيوتر وتحديد الأجهزة التي تحتاج إلى تحديثات أمنية
8. إعداد دليل للمستخدمين لتوفير النصائح والإرشادات للحفاظ على الأمان السيبراني.
9. تطوير برامج تعليمية لتوعية المستخدمين بمخاطر الأمن السيبراني وكيفية حماية أنفسهم.
10. تطوير أدوات لتحليل الهجمات السيبرانية وتحديد مصادرها ومسارها.
11. بناء آلية للتحقق من هجمات ال SQL Injection و إرسال تنبيه المسؤول النظام عند وقوعها.

آلية البناء:

- تركيب تطبيق ويب proof of concept مثلاً وردبريس
- استخدام (Apache or Nginx) كخدمات الويب .
- تفعيل خيارات Web access Logs عبر الويب سيرفر
- بناء سكربت عبر Python او Bash مع (Cron job) القراءة السجلات الجديدة كل 5 دقائق مثلاً؟
- السكربت سيقوم بالبحث عن (http query) قد تكون محاولات (SQL injection).
- في حال وجود محاولات، سيقوم السكربت بإرسال بريد الكتروني كتنبيه لمدير النظام.
- هذا المشروع بسيط و لكن قد يشكل نواة لتطبيق فحص امني أوتوماتيكي.

| | | |
|--|----|---------|
| Cryptography Engineering: Design Principles and Practical Applications" by Niels" Tadayoshi Kohno and Bruce Schneier, Ferguson . | -١ | المراجع |
| Applied Cryptography: Protocols, Algorithms, and Source Code in C" by Bruce Schneier. | -٢ | |
| Introduction to Cryptography with Coding Theory" by Wade Trappe and Lawrence C. Washington. | -٣ | |