معهد العراب العالي للتدريب

اساسيات علم التشفير

103سيبر

م. سمية أحمد

نبذة عن المقرر

يشمل هذا المقرر أهمية علم التشفير مع تطور الفكر البشري و التكنولوجي لإخفاء النصوص التي تحمل تلك الأفكار وتزايدت أهميته أكثر فأكثر مع تشكل الممالك والجيوش الضخمة ليلعب التشفير دورًا حيويًا في الحروب منذ القدم ومع التطور في علم الرياضيات واختراع الحاسب الآلي تشكل التشفير الحديث الذي يختلف كثيرًا عن سابقه وازداد الاهتمام به مع تطور الشبكات وظهور الشبكة وقد وجدت الطرق الحديثة لعدم ملائمة الطرق التقليدية للحاسوب الذي يتعامل مع الأصفار والواحدات مع أحرف الأبجدية ، لتشكل بعض المفاهيم الحديثة كدالة التجزئة والتشفير العام والتوقيع الالكتروني

معهد العراب العالي للتدريب

الأهداف العامة والتفصيلية من المقرر

الهدف العام:

يهدف هذا المقرر الى منطقية علم التشفير وتطبيقاته وتاريخ تطوره عبر العصور.

الأهداف التفصيلية:

- فهم علم التشفير / القيمة لعملية التشفير
- إدراك أنواع التشفير وأهميته وأسس كسر أنظمة التشفير
- يتابع التطورات لعلم التشفير في العصور الوسطى وعصر النهضة.
- يكتشف التقدم في لعلم التشفير أكثر في القرون الحديثة.
- يفهم أساسيات علم التشفير في عصر الكمبيوتر.
- يستخدم طرق أساسيات علم التشفير.
- يتمكن من أهمية أساسيات علم التشفير.
- يستخدم المفاتيح إما في عملية التشفير أو فك التشفير.
- يفهم المجالات الرئيسية للتشفير.
- يطبق أسس كسر أنظمة التشفير.
- يستخدم الأنظمة القوية المدعومة في التشفير.

معهد العراب العالي للتدريب

01

المحاضرة الأولى

مفهوم التشفير

القيمة العملية لعملية التشفير

2024

محتويات المحاضرة

1. ماهو التشفير
2. ما استخدامات التشفير
3. ماهو التشفير المتماثل وكيف يعمل
4 استخدامات التشفير المتماثل
5. مزاياه وعيوبه
6. المفاهيم الأمنية الرئيسية
7. أمثلة على متطلبات الأمان

ماهو التشفير

التشفير هو عبارة عن ممارسة حماية المعلومات باستخدام الخوارزميات المشفرة وعلامات التجزئة والتوقيعات. يمكن أن تكون المعلومات غير نشطة (مثل ملف على القرص الصلب)، أو متنقلة (مثل الاتصالات الإلكترونية المتبادلة بين طرفين أو أكثر) ، أو قيد الاستخدام (أثناء الحوسبة على البيانات)

أهداف التشفير

1. سرية - إتاحة المعلومات للمستخدمين المصرح لهم فقط.
2. النزاهة - ضمان عدم التلاعب بالمعلومات.
3. المصادقة – تأكيد صحة المعلومات أو هوية المستخدم.
4. عدم الإنكار - منع المستخدم من إنكار الالتزامات أو الإجراءات السابقة

ما إستخدامات التشفير

تعود أصول علم التشفير إلى إرسال معلومات حساسة بين الشخصيات العسكرية والسياسية. ويمكن تشفير الرسائل بحيث تبدو وكأنها نص عشوائي لأي شخص باستثناء المستلم المقصود. لكن في الوقت الحالي، جرى فك تقنيات التشفير الأصلية بالكامل. وجرى فك هذه التقنيات إلى درجة وجودها في أقسام الألغاز في بعض الصحف فقط. لحسن الحظ، حقق هذا المجال تقدما كبيرا في ناحية الأمن، وتعتمد الخوارزميات المستخدمة اليوم على التحليل الدقيق والرياضيات لضمان أمنها. ومع تطور الأمن، توسع مجال التشفير ليشمل نطاقًا أكبر من أهداف الأمان. ومن هذه الأهداف مصادقة الرسائل وتكامل البيانات والحساب الآمن وغيرها الكثير.

يُعد التشفير أساس المجتمع الحديث، وهو أساس لعدد لا يحصى من تطبيقات الإنترنت من خلال برتوكول النقل الآمن للنصوص التشعبية (HTTPS) والاتصالات النصية والصوتية الآمنة، وحتى العملات الرقمية

خوارزمية التشفير

عبارة عن إجراء يحوّل الرسالة المكونة من نص عادي الى معلومات مشفرة، وتستخدم الخوارزميات الحديثة مثل الرياضيات المتقدمة ومفتاح تشفير او أكثر، وهي تسهل نسبيًا تشفير الرسالة، ولكنها تجعل من المستحيل تقريبًا فك تشفيرها بدون معرفة المفاتيح .

وتنقسم تقنيات التشفير الى فئتين:

1. تشفير متماثل
2. تشفير غير متماثل

على أساس كيفية عمل مفاتيحها

ماهو التشفير المتماثل

لتشفير المتماثل هو نوع من التشفير حيث يتم استخدام مفتاح واحد فقط (مفتاح سري) لتشفير وفك تشفير البيانات الإلكترونية.

يجب على الكيانات التي تتواصل عبر التشفير المتماثل تبادل المفتاح بحيث يمكن استخدامه في عملية فك التشفير.

باستخدام خوارزميات التشفير المتماثل ، يتم "خلط" البيانات بحيث لا يمكن فهمها من قبل أي شخص لا يمتلك المفتاح السري لفك تشفيرها.

بمجرد حصول المستلم المقصود الذي يمتلك المفتاح على الرسالة ، تقوم الخوارزمية بعكس عمله بحيث يتم إرجاع الرسالة إلى شكلها الأصلي المقروء. يمكن أن يكون المفتاح السري الذي يستخدمه كل من المرسل والمستلم كلمة مرور او رمز معين أو يمكن أن يكون سلسلة عشوائية من الأحرف أو الأرقام التي تم إنشاؤها بواسطة منشئ رقم عشوائي آمن

ماهو التشفير المتماثل

يعمل التشفير المتماثل بنفس طريقة قفل الباب المؤدي إلى المنزل الذي لا يملك سوى الزوج والزوجة مفتاحه. حتى عندما يحاول شخص آخر فتح الباب ، لا يمكنه فعل ذلك ما لم يستخدموا أيًا من مفاتيح الزوجين. عندما يأخذ الآخرون المفتاحم من الزوج أو الزوجة ، يمكنهم فتح الباب حتى بدون علم الزوجين أو حضورهما. في التشفير المتماثل ، يكون المفتاح الذي يقوم بتشفير رسالة أو ملف هو نفس المفتاح الذي يمكنه فك تشفيرها. يستخدم مرسل البيانات خوارزمية المفتاح المتماثل لتشفير البيانات الأصلية وتحويلها إلى نص مشفر. ثم يتم إرسال الرسالة المشفرة إلى المتلقي الذي يستخدم نفس المفتاح المتماثل لفك تشفير أو فتح نص التشفير أو إعادته إلى شكل قابل للقراءة. في التشفير المتماثل ، يكون المفتاح الذي يقوم بتشفير رسالة أو ملف هو نفس المفتاح الذي يمكنه فك تشفيرها. يستخدم مرسل البيانات خوارزمية المفتاح المتماثل لتشفير البيانات الأصلية وتحويلها إلى نص مشفر. ثم يتم إرسال الرسالة المشفرة إلى المتلقي الذي يستخدم نفس المفتاح المتماثل لفك تشفير أو فتح نص التشفير أو إعادته إلى شكل قابل للقراءة. إذا تمكن شخص آخر غير المستلم المقصود من الوصول إلى المفتاح المتماثل ، فيمكنه أيضا فك تشفير الرسالة. لذلك، يعتبر التشفير المتماثل أقل أمانًا مقارنة بالتشفير غير المتماثل. وغني عن القول ، إن التعامل الدقيق والآمن مع المفتاح لحماية البيانات ومالكيها

الهدف من التشفير المتماثل

الهدف من التشفير المتماثل هو تأمين المعلومات الحساسة أو السرية أو السرية. يستخدم التشفير المتماثل مفتاحًا خاصًا لتشفير وفك تشفير بريد إلكتروني مشفر. يستخدم ايضا المفتاح العام للمستلم لتشفير الرسالة. ثم إذا أراد المستلم فك تشفير الرسالة ، فسيتعين على المستلم استخدام مفتاحه الخاص لفك التشفير. إذا كانت المفاتيح متوافقة ، فسيتم فك تشفير الرسالة. يستخدم التشفير غير المتماثل ، المعروف أيضًا باسم تشفير المفتاح العام ، مفتاحين منفصلين للتشفير وفك التشفير - مفتاح عام ومفتاح خاص مزدوج. وهو يختلف عن تشفير المفتاح المتماثل ، والذي يستخدم نفس المفتاح السري لوظائف التشفير وفك التشفير. في التشفير غير المتماثل ، يكون المفتاح العام متاحًا على نطاق واسع ويستخدمه الآخرون الذين يرغبون في تشفير رسالة يتم إرسالها إليك. المفتاح الخاص هو مفتاح سري مطابق يحتفظ به المستخدم وهو المفتاح الوحيد الذي يمكنه فك تشفير الرسائل التي يتم إرسالها إليه

الاستخدامات في أنظمة التشفير الحديثة

مع إدخال الإلكترونيات ولاحقًا في علوم الكمبيوتر ، أصبح من الممكن تنفيذ تقنيات تشفير أكثر تقدمًا استنادًا إلى حسابات رياضية معقدة. في هذه المرحلة ، اعتمدت تقنيات التشفير على خوارزميات التشفير المتماثل. باستخدام مثل هذه الخوارزميات ، يلزم وجود مفتاح سري واحد لتشفير الرسالة وفك تشفيرها.

يمتلك كلا الطرفين المشتركين في الاتصال والمرسل والمتلقي المفتاح السري.. RC4، AES، DES، 3DES، QUA تستخدم الخوارزميات التالية في التشفير المتماثل: يبلغ طول المفاتيح المتماثلة عادةً 128 أو 256 بت. كلما كان حجم المفتاح أكبر ، كان من الصعب كسره. على سبيل المثال ، يحتوي مفتاح 128 بت على حوالي 340.000.000.000.000.000.000.000.000.000.000.000.000 من إمكانيات كود التشفير.

هذا يعني أن هجوم القوة الغاشمة لم يعد أسلوبًا واقعيًا لكسر مثل هذا المفتاح

الاستخدامات في أنظمة التشفير الحديثة

في العالم الرقمي ، كانت هناك حاجة لتطوير نهج مختلف للتشفير ، يسمى التشفير غير المتماثل. باستخدام هذا الأسلوب ، يتم استخدام زوج من المفاتيح المرتبطة ويتكون من مفتاح عام يستخدم لتشفير البيانات ومفتاح خاص يستخدم لفك تشفير البيانات. المفتاح العام متاح لكل من يرغب فيإرسال رسالة. من ناحية أخرى ، يتم الاحتفاظ بالمفتاح الخاص في مكان آمن من قبل مالك المفتاح العام.

التشفير غير المتماثل يتم فيه استخدام مفتاح عام لتشفير نص عادي إلى نص مشفر بينما يتم استخدام مفتاح خاص لفك تشفير نص مشفر. ويستخدم بروتوكول HTTPSعلى الإنترنت ، تستخدم الكثير من مواقع الويب الآن بروتوكول وهي تقنية أمان قياسية لإنشاء ارتباط مشفر بين الخادم والعميل HTPPS SSL

المزايا والعيوب

تتضمن بعض مزايا التشفير المتماثل ما يلي:

- الأمان: مليارات السنين للتصدع باستخدام هجمات القوة الغاشمة. تستغرق خوارزميات التشفير المتماثل مثل AES .
- السرعة التشفير المتماثل ، بسبب أطوال مفاتيحه الأقصر وبساطته النسبية مقارنة بالتشفير غير المتماثل ، يكون أسرع بكثير في التنفيذ. في حين أن طريقة التشفير هذه لها مزايا ،

إلا أنها تحتوي على بعض **العيوب** التي تشمل:

- عرضة لتسرب المفتاح:

من السهل اختراق التشفير المتماثل لأنه بمجرد تسريب جزء من المفتاح ، يمكن للقراصنة إعادة بناء المفتاح بأكمله بسهولة والوصول إلى البيانات السرية.

هذه مشكلة خاصة بالنسبة للمعاملات التي تحتوي على الكثير من المعلومات الحساسة

المزايا والعيوب

- نقص بيانات الإسناد:

استخدام التشفير المتماثل يفتقر إلى البيانات الوصفية المضمنة أو بيانات الإحالة. و لا يسمح للمستخدمين بتسجيل المعلومات في قائمة التحكم في الوصول ولا يسمح لهم بمراقبة الاستخدام بناءًا على تواريخ انتهاء الصلاحية.

- غياب نظام الإدارة:

تعد إدارة المفاتيح أمرًا ضروريًا عند استخدام التشفير المتماثل. عندما تظل المفاتيح قيد الاستخدام قليلة ، تكون المراقبة اليدوية ممكنة و مع ذلك ، عند استخدامها على نطاق واسع ، يمكن أن يكون تتبع المفاتيح السرية يدويًا أمرًا غير عملي ، مما قد يصبح أكثر عرضة للاختراق

المفاهيم الرئيسة

- أمن الشبكات - تدابير لحماية البيانات أثناء نقلها.
- أمن الإنترنت – تدابير لحماية البيانات أثناء نقلها عبر مجموعة من الشبكات المترابطة

- أهداف أمن الحاسوب

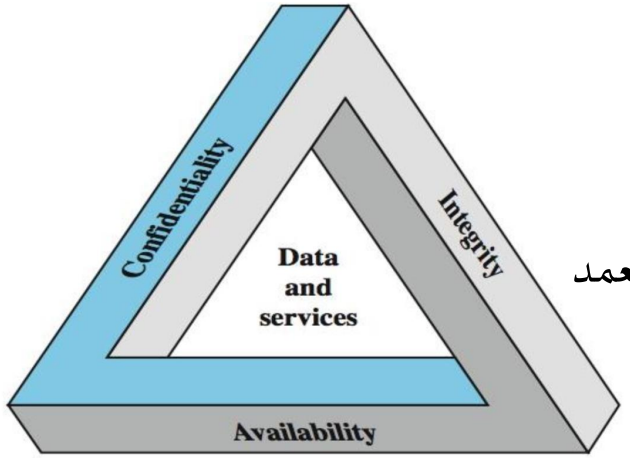
حماية أصول الكمبيوتر من: – الأخطاء البشرية والكوارث الطبيعية والأذى الجسدي والإلكتروني

المفاهيم الرئيسة

- سرية (السرية والخصوصية) c :

سرية البيانات يضمن عدم إتاحة المعلومات الخاصة أو السرية أو الكشف عنها لأفراد غير مصرح لهم .

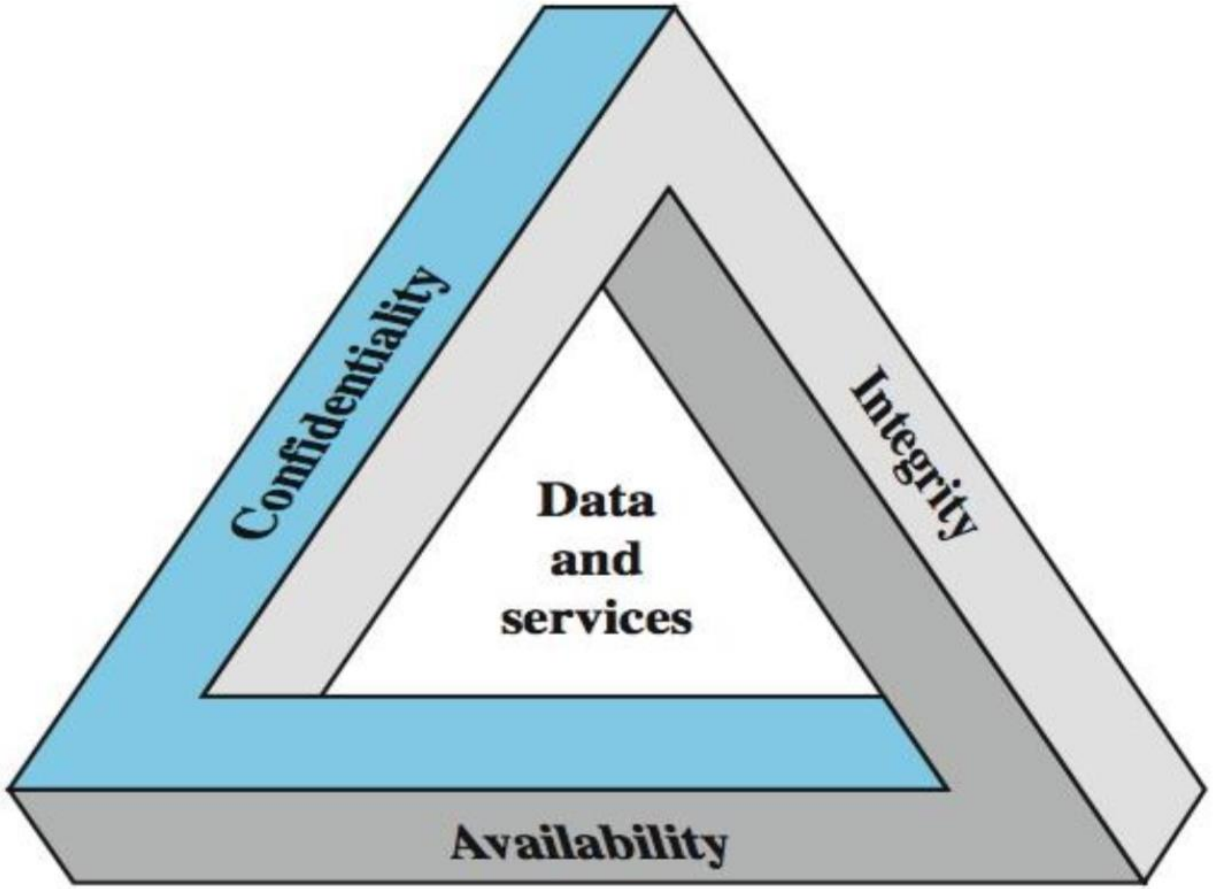
- خصوصية:
- يضمن أن الأفراد يتحكمون أو يؤثرون على المعلومات المتعلقة بهم التي يمكن جمعها وتخزينها ومن الذي يمكن الكشف عن هذه المعلومات
- التأكد من أن النظام لا يمكن الوصول إليه إلا من قبل الأطراف المصرح لها.



- النزاهة i:
- تكامل البيانات : يضمن عدم تغيير المعلومات والبرامج إلا بطريقة محددة ومصرح بها
- سلامة النظام : يضمن أن النظام يؤدي وظيفته المقصودة بطريقة سليمة، وخالية من التلاعب غير المصرح به المتعمد أو غير المقصود للنظام
- التوفر (الإتاحية) A :
- يضمن أن الأنظمة تعمل على الفور ولا يتم رفض الخدمة للمستخدمين المصرح لهم التأكد من عدم حرمان الأطراف المصرح لها من الوصول إلى المعلومات والموارد التأكد من أن الكمبيوتر يعمل عندما من المفترض أن يعمل وأنه يعمل بالطريقة التي ينبغي.(الوصول إلى موارد الحوسبة دون صعوبات.)

أمثلة على متطلبات الأمان

- سرية (السرية والخصوصية) c :
  - درجات الطلاب
- النزاهة i:
  - معلومات المريض
- التوفر (الإتاحية) A :
  - خسارة الخدمة تترجم الى خسارة مالية كبيرة



سؤال وإجابة

- المطلب الأمني الأهم لدرجات الطلاب: (السرية ، النزاهة ، الاتاحية، لاشيئ)
- المطلب الأمني الأهم لبيانات المريض هو : (لسرية ، النزاهة ، الاتاحية ، لاشيئ)

معهد العراب العالي للتدريب

مراجعة عامة

2024

معهد العراب العالي للتدريب

اساسيات علم التشفير

103سيبر

م. سمية أحمد

معهد العراب العالي للتدريب

02

المحاضرة الثانية

طرق التشفير

2024

محتويات المحاضرة

1. خوارزميات التشفير
2. جوانب الأمن

متطلبان للاستخدام الآمن للتشفير المتماثل:
خوارزمية تشفير قوية
مفتاح سري معروف فقط للمرسل/المتلقي
رياضيا لديها:

$$Y = E_K(X)$$

$$X = D_K(Y)$$

بعض المصطلحات الأساسية

نص عادي - الرسالة الأصلية

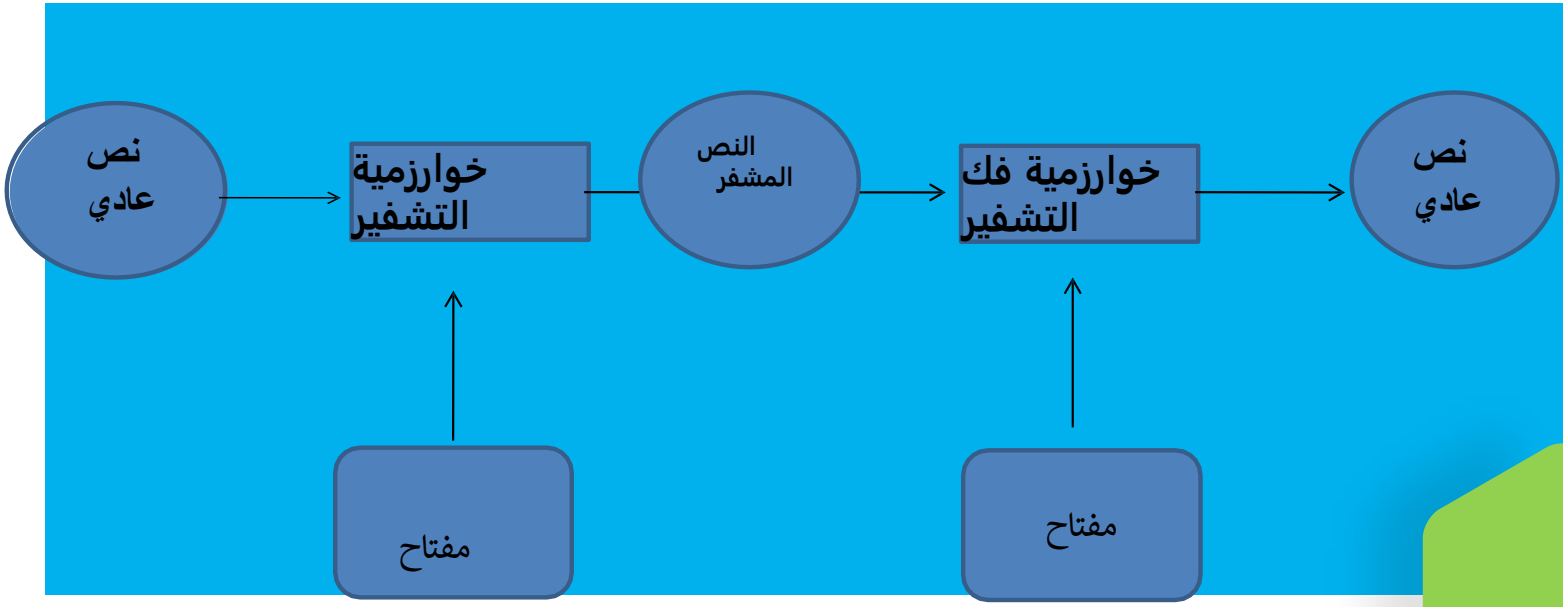
النص المشفر - رسالة مشفرة

خوارزمية التشفير: لتحويل النص العادي إلى نص مشفر

المفتاح - المعلومات المستخدمة في التشفير المعروفة فقط للمرسل/المتلقي

التشفير (التشفير) - تحويل النص العادي إلى نص مشفر

فك التشفير (فك التشفير) - استعادة النص المشفر من النص العادي


نص
عادي
خوارزمية
التشفير
النص
المشفر
خوارزمية فك
التشفير
نص
عادي
مفتاح
مفتاح

أنواع التشفير:
تشفير متماثل
تشفير غير متماثل

تشفير متماثل :

أو تقليدي / مفتاح خاص / مفتاح واحد

يتشارك المرسل والمستلم في مفتاح مشترك

جميع خوارزميات التشفير الكلاسيكية هي مفتاح خاص

كان هذا النوع من الكتابة فقط قبل اختراع المفتاح العام في السبعينيات

والأكثر استخدامًا على نطاق واسع

تحليل الشفرات:
الهدف هو استعادة المفتاح وليس الرسالة فقط
النهج العام:
هجوم تحليل التشفير
تعتمد على طبيعة الخوارزمية بالإضافة إلى بعض المعرفة بالخصائص العامة للنص العادي أو حتى بعض نماذج أزواج النص العادي والنص المشفر.
هجوم القوة الغاشمة
جرب كل مفتاح ممكن على جزء من النص المشفر حتى يتم الحصول على ترجمة واضحة إلى نص عادي

هجمات تحليل التشفير:

النص المشفر فقط

يعرف فقط الخوارزمية والنص المشفر

نص عادي معروف

تعرف/تشتبه في النص العادي والنص المشفر

نص عادي مختار

حدد النص العادي واحصل على النص المشفر

النص المشفر المختار

حدد النص المشفر واحصل على نص عادي

النص المختار

حدد نصًا عاديًا أو نصًا مشفرًا للتشفير/فك التشفير

بحث القوة الغاشمة:
من الممكن دائمًا تجربة كل مفتاح ببساطة
الهجوم الأساسي، بما يتناسب مع حجم المفتاح
تفترض إما معرفة/التعرف على النص العادي

Key Size (bits)	**Number of Alternative Keys**	**Time required at 1 decryption/μs**	**Time required at 10^6 decryptions/μs**
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	6.4×10^6 years

التقنيات الأساسية اثنين الرئيسية:

الاستبدال

تبديل

شفرات الاستبدال الكلاسيكية

حيث يتم استبدال حروف النص العادي بأحرف أخرى أو بأرقام أو رموز
أو إذا تم عرض النص العادي على أنه سلسلة من البايت، فإن الاستبدال
يتضمن استبدال أنماط البايت النص العادي بأنماط بتات النص المشفر

قيصر الشفرات

أقدم تشفير بديل معروف

بواسطة يوليوس قيصر

شهد الاستخدام لأول مرة في الشؤون العسكرية

يستبدل كل حرف بالحرف الثالث

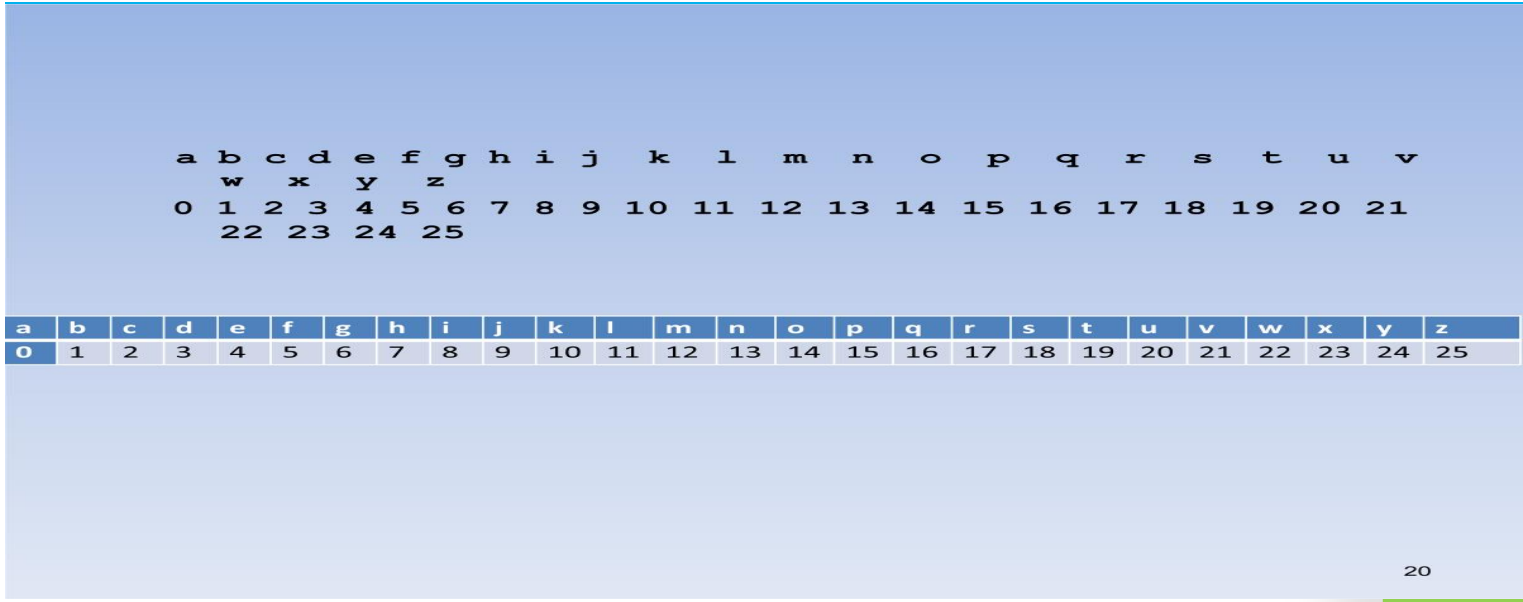
- example:

M e e t m e a f t e r

t h et o g a p a r t y

P H H W P H D I W H W R J D S

D U W B



a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

20

سؤال و إجابة

بأستخدام طريقة قيصر للتشفير قم بتشفسر التالي

1. Tea
2. Good Morning
3. Hello World

معهد العراب العالي للتدريب

اساسيات علم التشفير

103سيبر

م. سمية أحمد

معهد العراب العالي للتدريب

03

المحاضرة الثالثة

خوارزميات وبروتوكولات التشفير

2024

محتويات المحاضرة

1. خوارزميات التشفير
2. جوانب الأمن

يمكن تقسيم خوارزميات وبروتوكولات التشفير
الي أربع أقسام رئيسية

التشفير المتماثل

التشفير المتماثل يُستخدم لإخفاء محتويات الكتل أو تدفقات البيانات من أي حجم، بما في ذلك الرسائل والملفات ومفاتيح التشفير وكلمات المرور

التشفير غير المتماثل

يستخدم لإخفاء كتل صغيرة من البيانات، مثل مفاتيح التشفير والتجزئة القيم الوظيفية المستخدمة في التوقيعات الرقمية

خوارزميات سلامة البيانات

يستخدم لحماية كتل البيانات، مثل الرسائل، من التغيير

بروتوكولات المصادقة

مخططات تعتمد على استخدام خوارزميات التشفير المصممة للتحقق من هوية الكيانات

جوانب الأمن

خذ بعين الاعتبار ثلاثة جوانب لأمن المعلومات:

هجوم أمني

آلية أمنية

خدمات الأمن

هجوم أمني

أنواع الخروقات الأمنية

1-الضعف: هو ضعف في النظام الأمني يمكن استغلاله لإحداث خسارة أو ضرر — 1-Vulnerability

2-التهديد - احتمال انتهاك الأمن — 2- Threat

3- الهجوم: اعتداء على أمن النظام، محاولة متعمدة للتهرب من الأجهزة الأمنية — 3- Attack

تهديد Threat

التهديد:- احتمال انتهاك الأمن

التهديدات المادية - الطقس والكوارث الطبيعية والقنابل والطاقة وما إلى ذلك.

التهديدات البشرية - السرقة، الخداع، التجسس، التخريب، الحوادث

. تهديدات البرامج - الفيروسات وأحصنة طروادة والقنابل المنطقية.

أنواع التهديد

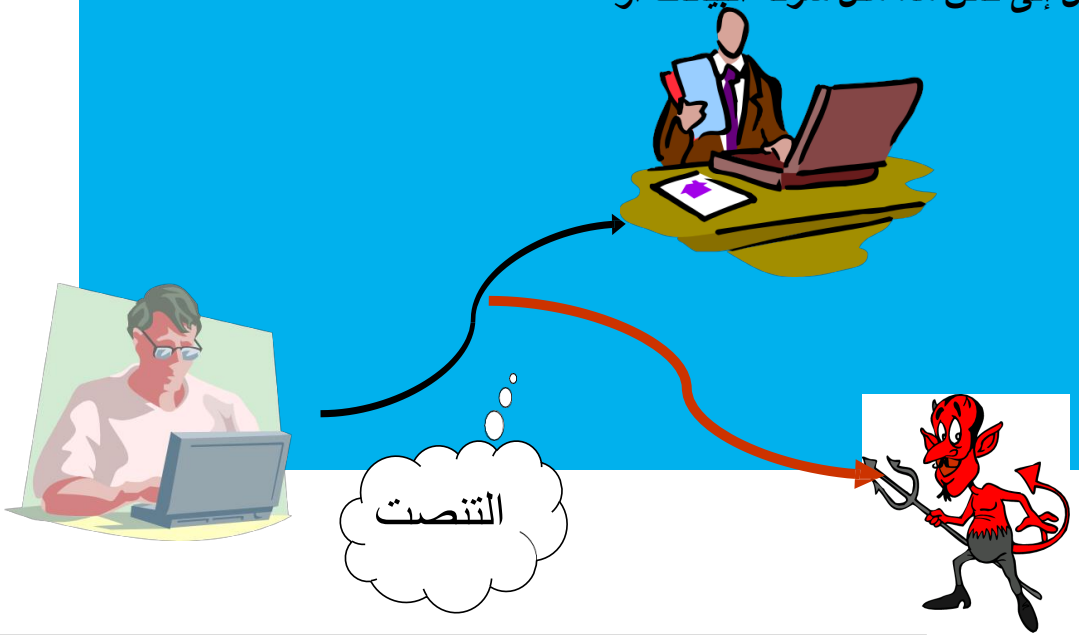
أربعة أنواع من الهجمات المحتملة هي:

1. **الانقطاع: تصبح الخدمات أو البيانات غير متاحة، أو غير قابلة للاستخدام، أو مدمرة، وما إلى ذلك، مثل فقدان الملف، أو رفض الخدمة**

قطع خطوط
الأسلاك، تشويش
الإشارات اللاسلكية،
إسقاط الحزم بيانات

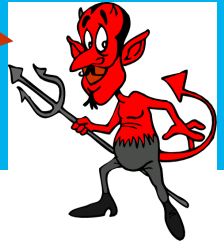
الاعتراض:

تمكن شخص غير مصرح له من الوصول إلى كائن ما، مثل سرقة البيانات أو التنصت على اتصالات الآخرين



التعديل:

التغيير غير المصرح به للبيانات أو تعديل الخدمات، مثل تغيير البيانات أو تعديل الرسائل



تقاطع

معلومات مستبدلة

التصنيع:

يتم إنشاء بيانات أو أنشطة إضافية لا توجد عادةً، مثل إضافة كلمة مرور إلى النظام، أو إعادة تشغيل الرسائل المرسلة سابقًا

تهديد امني

أي إجراء يهدد أمن المعلومات المملوكة للمنظمة

- يتعلق أمن المعلومات بكيفية منع الهجمات، أو الفشل في ذلك، لاكتشاف الهجمات على الأنظمة القائمة على المعلومات

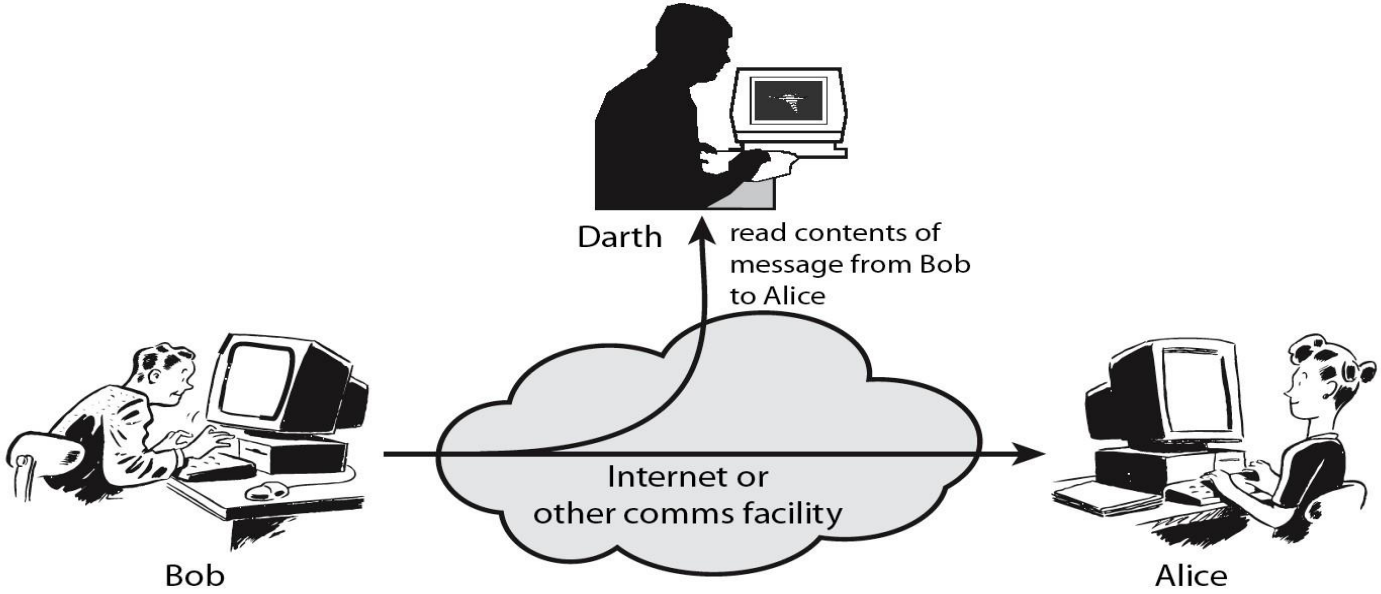
- يمكن أن تركز على أنواع عامة من الهجمات

- سلبي

- نشيط

الهجمات السلبية

يحاول الهجوم السلبي التعلم أو الاستفادة من المعلومات من النظام ولكنه لا يؤثر على موارد النظام

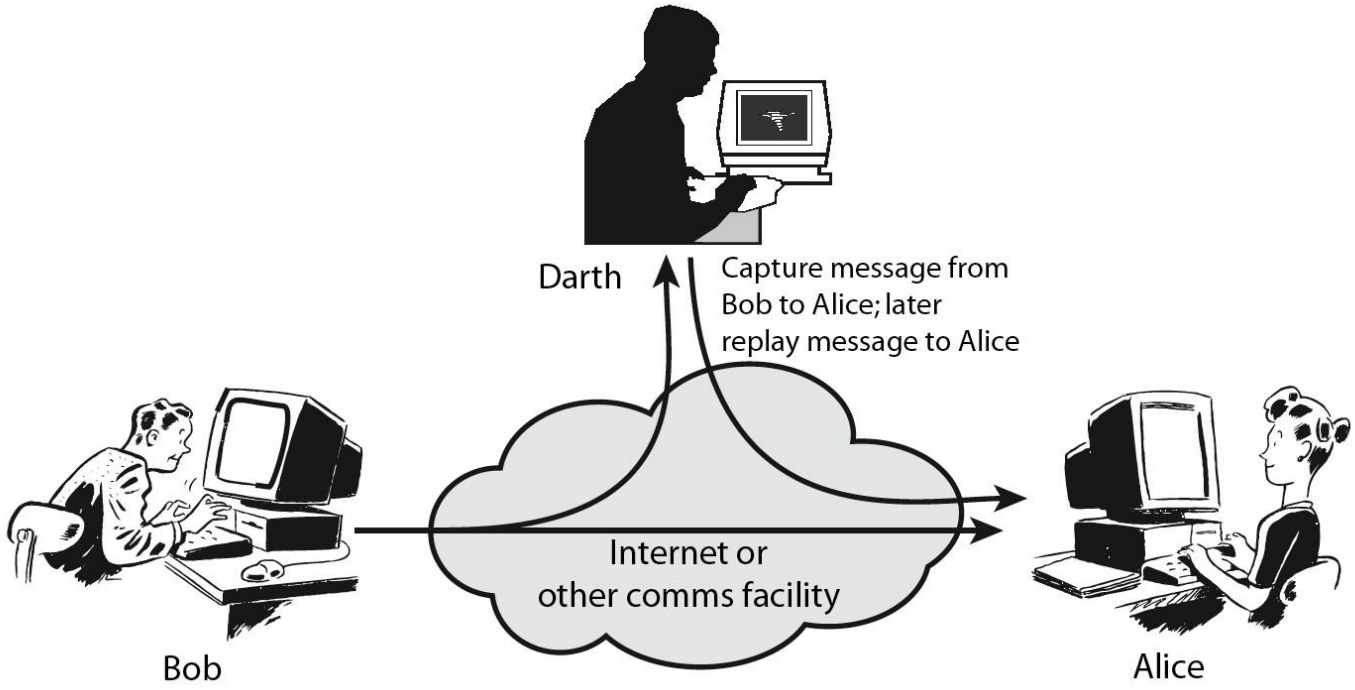

Darth
read contents of
message from Bob
to Alice
Internet or
other comms facility
Bob
Alice

تكون ذات طبيعة تنصت على عمليات الإرسال أو مراقبتها
هدف الخصم هو للحصول على المعلومات التي يتم إرسالها

هناك نوعان من الهجمات السلبية هما: الافراج عن محتويات الرسالة تحليل حركة المرور

الهجمات النشطة

يحاول الهجوم النشط تغيير موارد النظام أو التأثير على تشغيلها


Darth
Capture message from
Bob to Alice; later
replay message to Alice
Internet or
other comms facility
Bob
Alice

تتضمن بعض التعديلات على دفق البيانات أو إنشاء دفق خاطئ يصعب منعه بسبب التنوع الكبير في نقاط الضعف المادية والبرمجية والشبكية المحتملة الهدف هو اكتشاف الهجمات والتعافي من أي انقطاع أو تأخير ناجم عنها

سؤال و إجابة

جوانب لأمن المعلومات الثلاثة هي؟
.....و.....و.....

(هجوم أمني_آلية أمنية _خدمات الأمن_جميع ما سبق)

من أنواع التهديدات الأمنية .....و....و.....
(التهديدات المادية _ التهديدات البشرية_ برامج_ لا شئ)

معهد العراب العالي للتدريب

شكرا

معهد العراب العالي للتدريب

المحاضرة الرابعة

03

معيار تشفير البيانات

2023

معهد العراب العالي للتدريب

، وهو "Data Encryption Standard" هو اختصار لـ " DES
خوارزمية تشفير تم تطويرها في أوائل السبعينيات كوسيلة
لتأمين البيانات السرية. تم اعتمادها للتشفير من قبل
الحكومة الأمريكية في ذلك الوقت.

تعتمد خوارزمية DES على شبكة فيستل (Feistel Network) وتعمل على تشفير البيانات بشكل متماثل، حيث يتم تقسيم البيانات إلى كتلة بحجم 64 بت وتمريرها من خلال سلسلة من الجولات (Rounds). كل جولة تتكون من تطبيق عمليات التشفير والخلط والدوران المكررة.

تتكون عملية التشفير في DESمن ثلاث مراحل رئيسية:

1- مرحلة المفتاح السري (Key Generation): يتم توليد 16 مفتاحًا فرعيًا بطول 48 بت لكل جولة من مفتاح التشفير الأساسي البالغ طوله 56 بت. تتم عملية توليد المفاتيح الفرعية بواسطة تحويلات وتحويلات معقدة تستخدم البتات من المفتاح الأساسي وتطبيق عمليات الدوران والاختزال.

2- مرحلة التشفير (Encryption): يتم تشفير كل كتلة بيانات بحجم 64 بت باستخدام المفاتيح الفرعية المولدة وعمليات التشفير والخلط والدوران المتكررة لعدد محدد من الجولات.

3- مرحلة الإخراج (Output): يتم استخراج النص المشفر النهائي بعد إتمام جميع الجولات، ويتم إزالة بادئة تحقق التزامن (Initialization Vector) وتقسيم النص المشفر إلى كتل صغيرة.

ومع ذلك، تم اكتشاف بعض الضعف في DES على مر السنين، وأدى ذلك إلى تطوير خوارزميات التشفير الأكثر أمانًا مثل Advanced Encryption Standard (AES). ومع ذلك، لا يزال DES يستخدم في بعض التطبيقات الأقدم التي تتطلب التوافق مع المعايير القديمة.

توضيح خطوات عمل DES

لنفترض أن لدينا مستخدمًا يرغب في إرسال رسالة سرية باستخدام DESلتأمين البيانات. سنستخدم مفتاحًا سريًا مشتركًا بين المرسل والمستقبل لتشفير وفك تشفير الرسالة.

الخطوات التالية توضح كيفية استخدام DESفي تأمين البيانات:

1- توليد المفتاح: يتم توليد مفتاح عشوائي وتبادله بشكل آمن بين المرسل والمستقبل. يجب أن يكون طول المفتاح 56 بت في DES.

2- تحويل الرسالة إلى بلوكات: يتم تقسيم الرسالة إلى بلوكات بحجم 64 بت. وإذا كانت الرسالة لا تتناسب مع هذا الحجم، يتم إضافة تعبئة (paddingللرسالة لجعلها تتناسب.

3- تشفير البلوكات: يتم تطبيق خوارزمية التشفير DESعلى كل بلوك على حدة. يتم استخدام المفتاح السري المشترك لتشفير البيانات.

4- إرسال البيانات المشفرة: يتم إرسال البيانات المشفرة (ciphertext) إلى المستقبل عبر قناة آمنة.
5- فك تشفير البيانات: يستخدم المستقبل المفتاح السري المشترك لفك تشفير البيانات المشفرة باستخدام نفس خوارزمية DES.
6- إعادة تجميع الرسالة الأصلية: يتم تجميع البلوكات المفكوكة لإعادة بناء الرسالة الأصلية. يتم إزالة التعبئة إذا تمت إضافتها في الخطوة الثانية

باستخدام هذه الخطوات، يتم تأمين البيانات وتشفيرها باستخدام DES. يجب أن يتم تبادل المفتاح السري بشكل آمن بين المرسل والمستقبل لضمان سرية البيانات. قوة الأمان تعتمد على مدى سرية وصعوبة تخمين المفتاح المستخدم في التشفير وفك التشفير.

على الرغم من أن خوارزمية التشفير DESقد أصبحت قديمة نسبيًا وقد تم استبدالها بواسطة خوارزميات أكثر أمانًا مثل AES، إلا أنها لا تزال تستخدم في بعض الاستخدامات الأخرى. إليك بعض الأمثلة:

1- الاستخدام في أنظمة المصرفية: تستخدم بعض البنوك والمؤسسات المالية لا يزال DESفي بعض الأنظمة والتطبيقات القديمة لتأمين المعاملات المالية والبيانات الحساسة.

2- الاستخدام في أنظمة الهاتف المحمول: تستخدم بعض شركات الاتصالات خوارزمية DESفي بعض أنظمة تشفير المكالمات الهاتفية وتأمين البيانات في شبكات الهاتف المحمول القديمة.

3- الاستخدام في أجهزة التحكم الصناعية: تستخدم بعض أنظمة التحكم الصناعي المستخدمة في القطاع الصناعي DESلتأمين البيانات وتشفير التواصل بين الأجهزة.

4- الاستخدام في بعض الأجهزة القديمة: قد يتم استخدام DESفي بعض الأجهزة القديمة التي تحتاج إلى دعم معايير التشفير القديمة للتوافق والتكامل مع أنظمة أخرى.

سؤال و إجابة

عدد المفاتيح الفرعية المستخدمة في الDES

(16-42- 48-32)

المرحلة الأولي في ال DES تسمي ....

(مرحلة المفتاح السري-مرحلة التشفير-لا شئ)

معهد العراب العالي للتدريب

شكرا

معهد العراب العالي للتدريب

المحاضرة الخامسة

05

2024

تطورات علم التشفير

الجذور القديمة للتشفير

في أوائل العصور الوسطى، تم استخدام شفرات الاستبدال البسيطة، حيث تم استبدال الحروف بأحرف أخرى بناءً على قاعدة محددة مسبقًا.

باستخدام أدوات مثل scytale

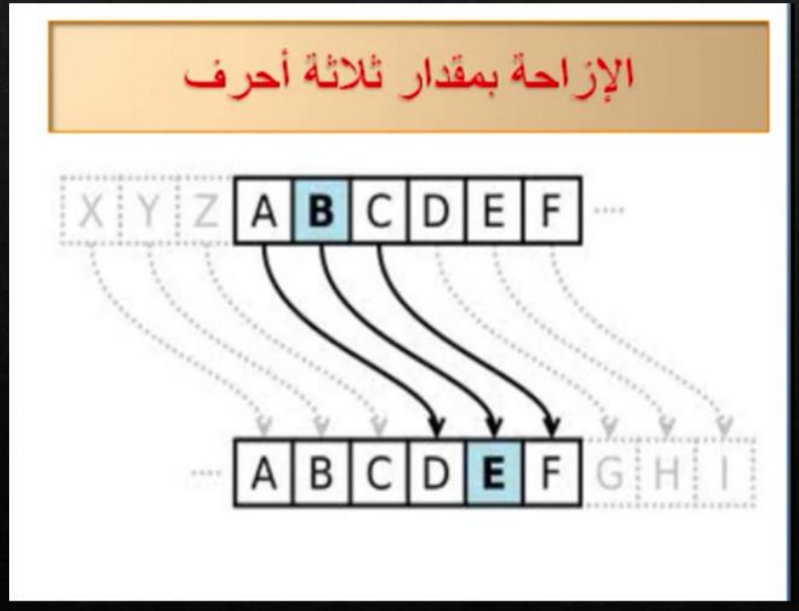
وهو قضيب يستخدم لتغليف الرسائل، توفر شكلاً أساسيًا من أشكال التشفير الأصفار الأحادية الأبجدية

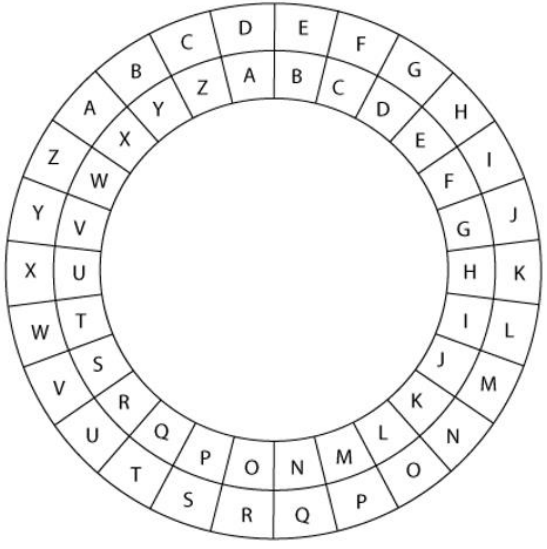
التطورات فى العصور الوسطى وعصر النهضة

- شهدت العصور الوسطى تحولًا إلى شفرات أحادية الأبجدية أكثر تعقيدًا، وكانت شفرة قيصر مثالًا بارزًا على ذلك.

- حيث ينطوي على تحويل الحروف لرسالة مشفرة بواسطة عدد معين من الأماكن أسفل الأبجدية اللاتينية.

مثال 1: شفرة قيصر





«ماكينة» تنفّذ شفرة قيصر.

مثال 2: شفرات الاستبدال البسيط

- شفرة الاستبدال البسيط (أو الشفرة أحادية الأحرف)
- في حالة شفرات الاستبدال البسيط نكتب الأحرف الأبجدية عشوائيًّا تحت أحرف الهجاء تمامًا كما هي مرتبة أبجديًّا.

A	B	C	D	E	F	G	H	I	J	K	L	M
D	**I**	**Q**	**M**	**T**	**B**	**Z**	**S**	**Y**	**K**	**V**	**O**	**F**
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	**R**	**J**	**A**	**U**	**W**	**P**	**X**	**H**	**L**	**C**	**N**	**G**

طرق التشفير

هناك العديد من طرق التشفير والخوارزميات المستخدمة لتأمين البيانات. فيما يلي بعض طرق التشفير الشائعة الاستخدام:

معيار التشفير المتقدم Advanced Encryption Standard (AES)

- عبارة عن خوارزمية تشفير متماثل تم إنشاؤها كمعيار بواسطة المعهد الوطني الأمريكي للمعايير والتكنولوجيا (NIST)في عام 2001.
- حلت محل معيار تشفير البيانات الأقدم DES نظرًا لضعفه. تعمل على كتل بيانات ذات حجم ثابت (128 بت) وتدعم أطوال مفاتيح تبلغ 128 أو 192 أو 256 بت. ويستخدم على نطاق واسع لتأمين البيانات الحساسة، بما في ذلك المعاملات المالية والاتصالات الحكومية.

معيار تشفير البيانات

Data Encryption Standard (DES):

..

- هي خوارزمية تشفير متماثلة مبكرة تستخدم مفتاح 56 بت. إنه يعمل على كتل بيانات 64 بت ويطبق سلسلة من التحويلات.
- على الرغم من كونها رائدة في وقت تطويرها، تعتبر الآن غير آمنة نظرًا لصغر حجم مفتاحها.
- يعد Triple DES (3DES) متغيرًا أكثر أمانًا يطبق خوارزمية DES ثلاث مرات على كل كتلة بيانات، ولكنه أقل كفاءة من الخوارزميات المتماثلة الأكثر حداثة.

معيار تشفير البيانات 3

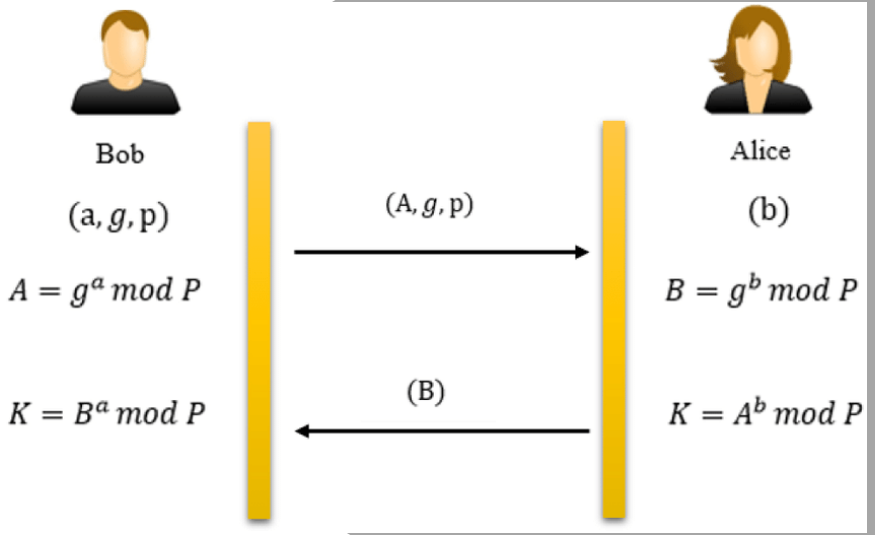
Data Encryption Standard 3 (DES):

عبارة عن خوارزمية تشفير متماثلة تطبق خوارزمية DES ثلاث مرات على كل كتلة بيانات. يستخدم مفتاحين أو ثلاثة مفاتيح، مما يوفر أمانًا أكبر مقارنةً بـ DESالأصلي.

ومع ذلك، فإن 3 DESأبطأ وأقل كفاءة من الخوارزميات المتماثلة الأكثر حداثة مثل AES، وقد انخفض استخدامه لصالح طرق التشفير الأحدث..

- **RSA** (Rivest-Shamir-Adleman)هي خوارزمية تشفير غير متماثلة تستخدم زوجًا من المفاتيح: مفتاح عام للتشفير ومفتاح خاص لفك التشفير. تم تسمية RSA على اسم مخترعيها، وهي تستخدم على نطاق واسع لنقل البيانات بشكل آمن والتوقيعات الرقمية. يعتمد أمانها على صعوبة تحليل ناتج رقمين أوليين كبيرين. تتراوح أطوال مفاتيح RSA عادة من 1024 إلى 4096 بت.

- **تشفير المنحنى الإهليلجي Elliptic Curve Cryptography(ECC)**:
هي خوارزمية تشفير غير متماثلة تعتمد على رياضيات المنحنيات الإهليلجية. فهو يوفر أمانًا قويًا بأطوال مفاتيح أقصر مقارنة بالخوارزميات التقليدية غير المتماثلة مثل RSA. غالبًا ما يتم تفضيل ECC للبيئات المحدودة الموارد، مثل الأجهزة المحمولة وأجهزة إنترنت الأشياء، حيث تعد الكفاءة الحسابية أمرًا بالغ الأهمية.



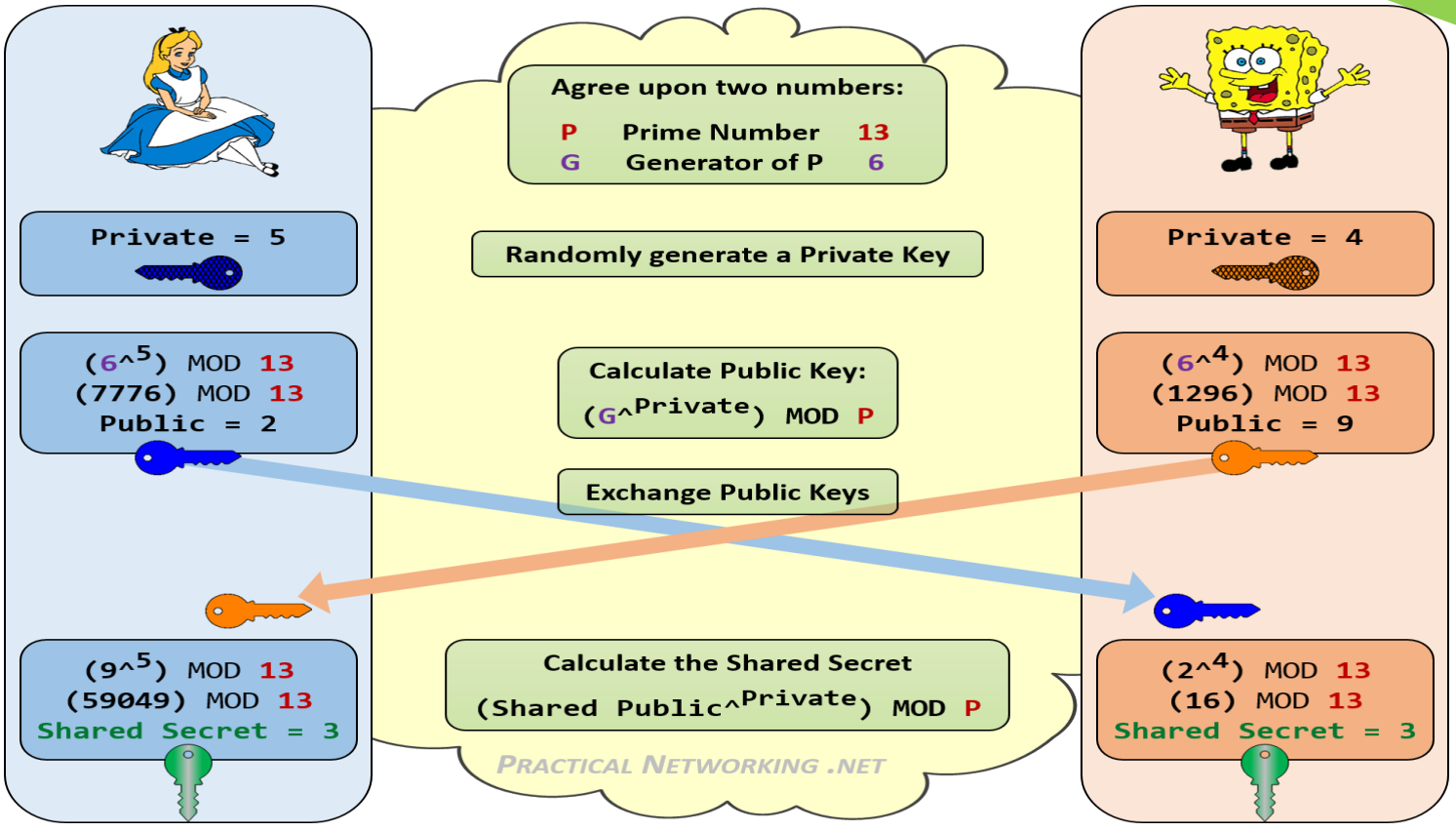
❑ **تبادل مفاتيح ديفي-هيلمان:** Diffie-Hellman

هي خوارزمية تبادل مفاتيح تسمح لطرفين بإنشاء سر مشترك بشكل آمن عبر شبكة غير موثوقة. غالبًا ما يتم استخدامه مع التشفير المتماثل لإنشاء مفتاح سري مشترك للاتصال الآمن. يعتمد ديفي هيلمان على صعوبة مشكلة اللوغاريتم المنفصلة من أجل أمنها.

نشاط

لمعرفة المفتاح السري المشترك مع زميلتك

قومي بتطبيق طريقة **مفاتيح ديفي-هيلمان**



Blowfishو Twofishعبارة عن خوارزميات تشفير متماثلة صممها Bruce Schneier. تعمل السمكة المنتفخة على كتل 64 بت وتدعم أطوال مفاتيح متغيرة تصل إلى 448 بت. يعد Twofishخليفة أكثر تعقيدًا لـ Blowfish، حيث يدعم أحجام الكتل التي تصل إلى 128 بت وأطوال المفاتيح التي تصل إلى 256 بت. في حين أن كلاهما يعتبران آمنين، فقد حلت AESمحلهما إلى حد كبير في الاستخدام على نطاق واسع.

خوارزمية التجزئة الآمنة تشتمل عائلة SHAعلى وظائف تجزئة متنوعة (SHA-1، وSHA-256، وSHA-384، وSHA-512، وما إلى ذلك) التي تنشئ قيم تجزئة ذات حجم ثابت من بيانات الإدخال. تُستخدم خوارزميات SHAبشكل شائع لضمان تكامل البيانات

PGP(خصوصية جيدة جدًا):
(Pretty Good Privacy)

هو نظام تشفير هجين يجمع بين التشفير بالمفتاح المتماثل والمفتاح العام. وغالبا ما يستخدم PGP لتأمين رسائل البريد الإلكتروني والملفات. يستخدم مفتاح جلسة متماثل لتشفير البيانات، ثم يتم تشفير مفتاح الجلسة بالمفتاح العام للمستلم. يدعم خوارزميات التشفير المختلفة، ويتضمن تطبيقه ميزات لضغط البيانات والتوقيعات الرقمية

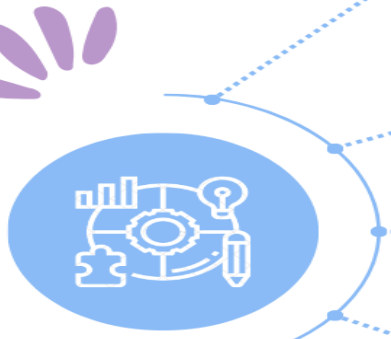
لكل طريقة تشفير نقاط القوة والضعف وحالات الاستخدام. يعتمد اختيار الطريقة التي سيتم استخدامها على عوامل مثل متطلبات الأمان، والكفاءة الحسابية، والتطبيق المحدد الذي سيتم استخدامه فيه.

طريقة التشفير	النوع	اطوال المفاتيح	الوصف
معيار التشفير المتقدم (AES)	تشفير متماثل.	128 أو 192 أو 256 بت.	يستخدم على نطاق واسع لتأمين البيانات الحساسة. إنها خوارزمية التشفير القياسية التي اعتمدتها حكومة الولايات المتحدة
معيار تشفير البيانات (DES)	تشفير متماثل.	56 بت (يعتبر غير آمن اليوم).	خوارزمية مفاتيح متماثلة قديمة، يتم استبدالها غالبًا بخوارزميات أكثر أمانًا مثل AES.
ثلاثية DES (3DES)	تشفير متماثل.	112 أو 168 بت.	إصدار أكثر أمانًا من DES يطبق خوارزمية DES ثلاث مرات على كل كتلة بيانات.
آر إس إيه (ريفست-شمير-أدلمان)RSA	تشفير غير متماثل.	توصي NIST بحد أدنى من مفاتيح 2048 بت لـ RSA.	يستخدم على نطاق واسع لنقل البيانات بشكل آمن والتوقيعات الرقمية. إنه مكثف حسابيًا وغالبًا ما يستخدم لتبادل المفاتيح.
تشفير المنحنى الاهليلجي (ECC)	تشفير غير متماثل.	عادة أعداد صحيحة 256 بت.	يوفر أمانًا قويًا بأطوال مفاتيح أقصر مقارنةً بـ RSA، مما يجعله أكثر كفاءة من حيث الموارد الحسابية.

طريقة التشفير	النوع	اطوال المفاتيح	الوصف
السمكة المنتفخة والسمكة المزدوجة	تشفير متماثل	متغيرة (تصل إلى 448 بت للسمكة المنتفخة).	خوارزميات تشفير الكتل مناسبة لمجموعة متنوعة من التطبيقات.
تبادل مفاتيح ديفي-هيلمان-Diffie Hellman	خوارزمية تبادل المفاتيح.	bits 2048 - 1024	يُستخدم للتبادل الآمن لمفاتيح التشفير عبر شبكة غير موثوقة، وغالبًا ما يستخدم مع التشفير المتماثل.
SHA (خوارزمية التجزئة الآمنة)	دالة التجزئة.	الإصدارات: SHA-1، SHA-256، SHA-384، SHA-512، إلخ. SHA-1 hash is 160 bits long, whereas SHA-256 is256 bits	يستخدم لإنشاء قيم تجزئة ذات حجم ثابت من بيانات الإدخال. يشيع استخدامها للتحقق من سلامة البيانات.
PGP (خصوصية جيدة جدًا)	التشفير الهجين Hybrid encryption (يجمع بين التشفير المتماثل وغير المتماثل)	بين 512 الى 4096 bytes	يستخدم لتأمين رسائل البريد الإلكتروني وتشفير الملفات. يجمع بين التشفير بالمفتاح المتماثل والمفتاح العام.

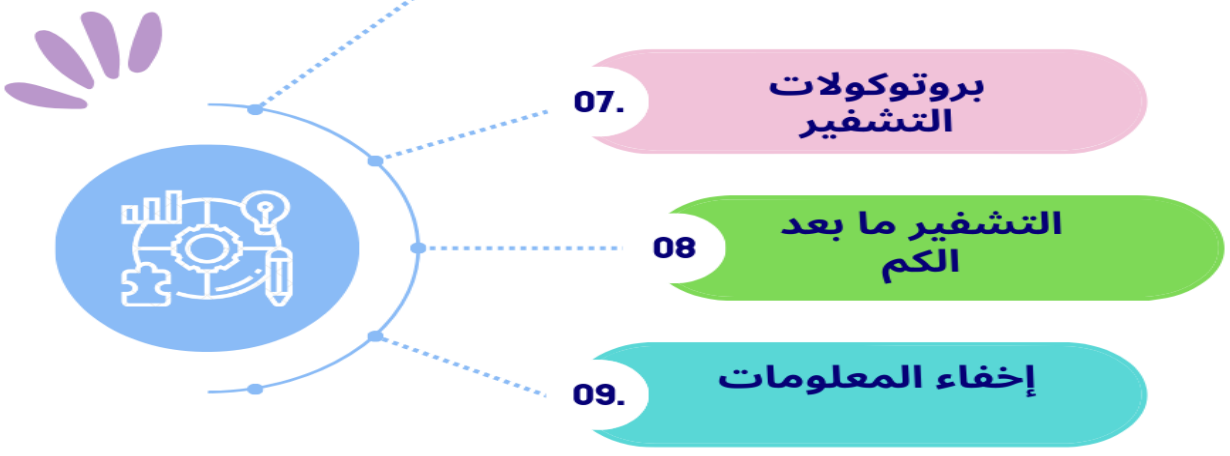
• المجالات الرئيسية للتشفير

يعد التشفير مجالًا واسعًا وله تطبيقات في مجالات مختلفة. يمكن تصنيف المجالات الرئيسية للتشفير على النحو التالي:



01. تشفير المفتاح المتماثل
02. تشفير غير المفتاح المتماثل(المفتاح العام)
03. وظائف التجزئة
04. التوقيعات الرقمية
05. بروتوكولات تبادل المفاتيح

يعد التشفير مجالًا واسعًا وله تطبيقات في مجالات مختلفة. يمكن تصنيف المجالات الرئيسية للتشفير على النحو التالي:



إخفاء المعلومات

قد تكون رسالة نصية عادية مخفية. تخفي طرق steganography وجود الرسالة، في حين أن طرق التشفير تجعل الرسالة غير مفهومة للغرباء من خلال التحولات المختلفة للنص

تم استخدام العديد من التقنيات الأخرى تاريخيا؛ بعض الأمثلة هي ما يلي

وضع علامات الأحرف: تتم الكتابة فوق الحروف المختارة من النص المطبوع أو المكتوب بالقلم الرصاص. عادة ما تكون العلامات غير مرئية ما لم يتم تثبيت الورقة بزاوية للضوء الساطع.

الحبر غير المرئي: يمكن استخدام عدد من المواد للكتابة، ولكن لا تترك أي أثر مرئي حتى يتم تطبيق الحرارة أو بعض المواد الكيميائية على الورق.

ثقوب الدبوس: عادة ما تكون ثقوب الدبوس الصغيرة على الحروف المحددة غير مرئية ما لم يتم تثبيت الورقة أمام الضوء.

شريط تصحيح الآلة الكاتبة: يستخدم بين الخطوط المكتوبة بشريط أسود، نتائج الكتابة بشريط التصحيح مرئية فقط تحت ضوء قوي.

LSB Steganography(Embedding Process)

Secret message to be embedded

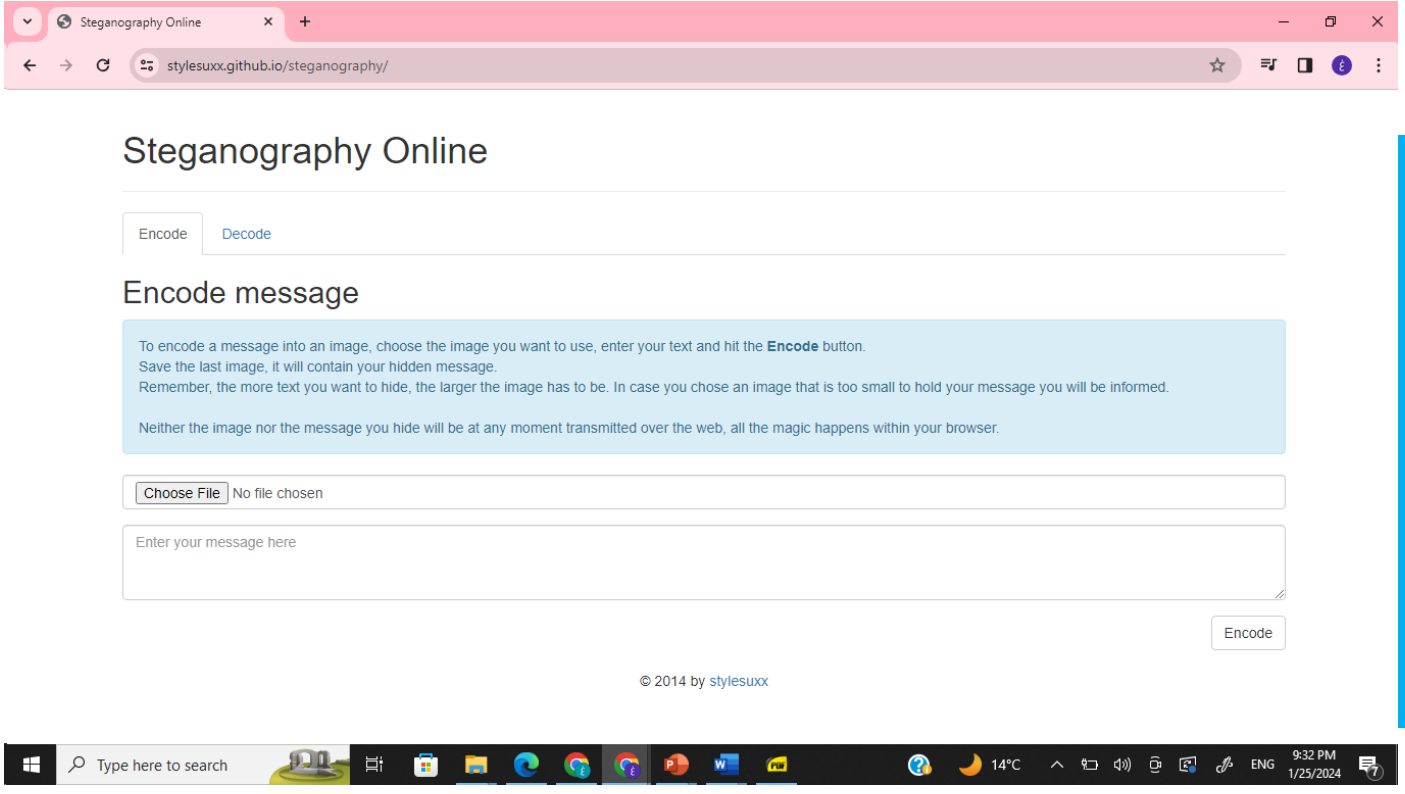
The word "Steganography" is a Greek word which means "covered or hidden writing".
In other words Steganography is technique of hiding information behind the cover medium.

Original Image

Stego Image

Open | Embed | Save into new file | Reset

https://stylesuxx.github.io/steganography/



يتم دعم التشفير القوي من خلال أنظمة وتقنيات مختلفة لضمان أمان وخصوصية البيانات. فيما يلي بعض الأمثلة على الأنظمة والتطبيقات التي تدعم التشفير القوي على نطاق واسع:

أنظمة التشغيل:

BitLocker :Windows: برنامج تشفير القرص المضمن في Windows.
Windows Defender Credential Guard يستخدم الأمان المستند إلى الأجهزة لحماية الأسرار وبيانات الاعتماد ومفاتيح التشفير.

FileVault:ماك: تشفير القرص بالكامل لأنظمة macOS.

dm-crypt/LUKS:لينكس: وحدات تشفير kernel Linux وأدوات مساحة المستخدم لتشفير القرص بالكامل.

متصفحات الانترنت: جوجل كروم، موزيلا فايرفوكس، مايكروسوفت إيدج:يضمن دعم HTTPS (SSL/TLS) الاتصال الآمن بين المتصفح وخوادم الويب.التشفير المعتمد على المتصفح لكلمات المرور والبيانات الحساسة الأخرى.

OpenVPN، WireGuard، IPSec:

بروتوكولات التشفير التي تستخدمها شبكات VPN لتأمين اتصالات الإنترنت. يحمي البيانات أثناء النقل عن طريق تشفيرها بين جهاز المستخدم وخادم VPN. سحابة التخزين:

Signal:

تطبيق مراسلة يركز على الخصوصية ويستخدم التشفير الشامل للرسائل النصية والمكالمات الصوتية ومكالمات الفيديو.واتساب:يستخدم بروتوكول Signal للتشفير الشامل في الرسائل والمكالمات.برقية:يوفر تشفيرًا شاملاً للمحادثات السرية.تشفير البريد الإلكتروني:

معهد العراب العالي للتدريب

شكرا