الأكاديمية العربية الدولية
Arab International Academy

خوارزميات التشفير

encryption algorithms

م. خليل المحمد

كلية العلوم – ماجستير علم البيانات

المحاور

1. مقدمة في علم التشفير
2. أنواع التشفير
3. خوارزميات التشفير المتماثل
4. خوارزميات التشفير غير المتماثل
5. خوارزميات التجزئة (Hashing)
6. التشفير في التطبيقات العملية
7. التهديدات والتحديات
8. مستقبل التشفير والتقنيات الحديثة

المخرجات المتوقعة من المحاضرة

1. **فهم مفهوم التشفير** ودوره في تأمين البيانات داخل أنظمة المعلومات الحديثة.
2. **التمييز بين أنواع التشفير** (المتماثل وغير المتماثل والتجزئة)، ومعرفة الفروق الجوهرية في الاستخدام والآلية.

شرح أهم خوارزميات التشفير مثل:

- **AES** و **DES** التشفير المتماثل
- **RSA** و **Diffie-Hellman** التشفير غير المتماثل
- **SHA** و **MD5** خوارزميات التجزئة

3. **تحليل التطبيقات العملية للتشفير** في مختلف البيئات مثل: الشبكات، الهواتف، الأنظمة البنكية، والبريد الإلكتروني.
4. **التعرّف على التهديدات الحديثة** التي تواجه أنظمة التشفير مثل هجمات القوة الغاشمة، التحليل الرياضي، والتحديات الكمومية
5. **استكشاف الاتجاهات المستقبلية** في علم التشفير، مثل التشفير الكمومي، وتكامل الذكاء الاصطناعي في الأمن السيبراني.
6. **استخدام أدوات بسيطة ومفتوحة المصدر** لتجريب عمليات التشفير والتجزئة، وتنمية المهارات العملية.
7. **اختيار مصادر تعلّم ذاتي موثوقة** لمواصلة تطوير المعرفة في التشفير وأمن المعلومات.

1. مقدمة في التشفير

1.1 ما هو التشفير؟

يُعرَّف التشفير بأنه عملية تهدف إلى حماية المعلومات من خلال تحويلها من صيغة مفهومة إلى صيغة غير قابلة للقراءة أو التفسير إلا من قبل الأشخاص المصرح لهم بذلك.

أهمية التشفير: التشفير يُعد من الركائز الأساسية في أمن المعلومات، حيث يساهم بشكل مباشر في تحقيق مبدأ السرية Confidentiality.

كيف يعمل التشفير؟

تُجرى عملية التشفير عبر برامج وخوارزميات خاصة تستخدم ما يُعرف بالمفاتيح. هذه المفاتيح قد تكون متماثلة في بعض الأنظمة، أو تتكوّن من زوج (عام وخاص) في أنظمة أخرى. عند فك التشفير، تتم استعادة البيانات الأصلية باستخدام المفتاح المناسب.

أمثلة واقعية:

نستخدم التشفير في حياتنا اليومية بشكل تلقائي دون أن ننتبه، مثلًا في التطبيقات التي تدعم المحادثات المشفرة كواتساب، وفي المواقع الإلكترونية التي تستخدم بروتوكول HTTPS لحماية البيانات، وفي بطاقات الصراف الإلكتروني التي تشفر معلومات الحساب.

ملاحظة: لا يُخفي التشفير وجود البيانات، لكنه يجعلها عديمة القيمة لمن لا يمتلك المفتاح الصحيح.

1. مقدمة في التشفير

1.2 لماذا نحتاج إلى التشفير؟

في عالمنا الرقمي المتسارع، أصبح التشفير ضرورة ملحّة لحماية المعلومات الحساسة من التعرّض للاختراق أو التلاعب.

حماية البيانات أثناء النقل والتخزين:

أهم أسباب استخدام التشفير هو حماية المعلومات عند إرسالها من جهاز إلى آخر، مثلما يحدث عند إرسال بريد إلكتروني أو رسالة على تطبيق محادثة. كذلك، يُستخدم التشفير لتأمين الملفات المخزنة على الأقراص أو في قواعد البيانات.

ضمان الخصوصية:

التشفير يحمي خصوصية الأفراد والمؤسسات، ويمنع المتطفلين من الاطلاع على الرسائل أو الملفات الخاصة. على سبيل المثال، في التطبيقات الطبية أو البنكية، تُشفّر البيانات الشخصية لتفادي أي تسريب أو إساءة استخدام.

التحقق من الهوية والنزاهة:

إحدى وظائف التشفير المهمة هي التحقق من هوية المرسل والمستلم، من خلال ما يُعرف بالتوقيع الرقمي.

مطلب قانوني وتنظيمي:

في بعض القطاعات مثل البنوك، والمؤسسات الصحية، والتعليم الإلكتروني، يُلزم القانون باستخدام التشفير لحماية معلومات العملاء والمرضى والطلاب. عدم الالتزام بهذه المعايير قد يؤدي إلى غرامات قانونية أو فقدان الثقة.

1. مقدمة في التشفير

1.3 الفرق بين التشفير وأمن المعلومات:

يُعتبر أمن المعلومات مجالًا شاملاً يهتم بحماية البيانات من جميع أنواع التهديدات، سواء أثناء التخزين أو النقل أو المعالجة. ويهدف إلى الحفاظ على سرية البيانات وسلامتها وتوافرها من خلال مجموعة من السياسات والتقنيات والضوابط.
أما التشفير، فهو أحد الأدوات الأساسية المستخدمة داخل أمن المعلومات، ويُستخدم تحديدًا لضمان السرية، أي منع الوصول إلى البيانات من قبل غير المصرح لهم.

المبادئ الأساسية لأمن المعلومات:

- السرية: Confidentiality
- النزاهة: Integrity
- التوافر: Availability

التشفير يُستخدم لتحقيق السرية فقط، بينما تتطلب حماية البيانات بشكل شامل الاعتماد على مجموعة متنوعة من الأدوات الأخرى مثل جدران الحماية، أنظمة كشف التسلل، نسخ البيانات الاحتياطي، وإدارة الوصول.
باختصار، التشفير هو وسيلة ضمن منظومة أمنية أوسع، ولا يمكن الاعتماد عليه وحده لتأمين الأنظمة والمعلومات بالكامل.

1. مقدمة في التشفير

1.4 أمثلة من الواقع: هذه الأمثلة توضّح كيف أصبح التشفير جزءًا أساسيًا من حياتنا الرقمية، سواء في الاتصالات أو المعاملات أو تخزين المعلومات.

التشفير في تطبيقات المراسلة: تعتمد تطبيقات مثل واتساب وتيليغرام على تقنية التشفير من الطرف إلى الطرف، حيث يتم تشفير الرسالة قبل مغادرتها جهاز المُرسل، ولا يمكن فك تشفيرها إلا على جهاز المُستلم فقط.

التشفير في المواقع الإلكترونية: عند زيارة موقع إلكتروني آمن يستخدم بروتوكول HTTPS، يتم تشفير الاتصال بين المستخدم والخادم.

التشفير في البطاقات البنكية

تعتمد البطاقات البنكية والأنظمة المالية على تقنيات تشفير قوية لحماية بيانات المعاملات والمعلومات الشخصية للعملاء.

التشفير في التخزين السحابي: توفر خدمات التخزين مثل Google Drive أو Dropbox خيارًا لتشفير الملفات أثناء التخزين، مما يحمي المحتوى من الوصول غير المصرح به حتى في حالة اختراق الحساب أو الخدمة.

1. مقدمة في التشفير

1.5 التشفير كعنصر أساسي في العصر الرقمي: مع توسّع الاعتماد على الإنترنت والخدمات السحابية، أصبح التشفير ضرورة لحماية المعلومات وليس مجرد إضافة, و يُستخدم التشفير اليوم في الهواتف، المواقع، التعليم الإلكتروني، المعاملات البنكية، والتطبيقات اليومية.

تطبيقات التشفير في الحياة اليومية: معظم الهواتف الذكية تدعم التشفير الكامل للقرص بشكل مدمج ضمن نظام التشغيل, و كذلك خدمات البريد الإلكتروني مثل Gmail و Outlook تستخدم بروتوكولات تشفير متقدمة , كما ان خدمات التخزين السحابي مثل Google Drive توفّر التشفير أثناء رفع الملفات وأثناء تخزينها.

أهمية التشفير للمؤسسات

- المؤسسات مطالبة قانونيًا باستخدام التشفير، خصوصًا في القطاعات الحساسة كالصحة والمال.
- الامتثال لتشريعات مثل GDPR في أوروبا و HIPAA في الولايات المتحدة يتطلب وجود تشفير فعّال.
- التشفير يُقلّل من خطر الاختراقات ويساهم في الحفاظ على ثقة العملاء.

التشفير أساس الثقة الرقمية: التشفير يحمي المستخدمين من التنصت والتلاعب وسرقة البيانات ويدعم مصداقية الخدمات الإلكترونية.

2. أنواع التشفير

2.1 – التشفير المتماثل Symmetric Encryption

ما هو التشفير المتماثل؟

التشفير المتماثل هو أسلوب يُستخدم فيه نفس المفتاح لتشفير البيانات وفك تشفيرها, أي أن الطرفين (المرسل والمستقبل) يجب أن يمتلكا نفس المفتاح مسبقًاو يُعتبر هذا النوع من التشفير من أقدم وأكثر الأساليب استخدامًا بسبب بساطته وسرعته.

أمثلة على استخداماته

- يُستخدم التشفير المتماثل لحماية الملفات المخزنة محليًا على الأجهزة.
- شائع في الشبكات المغلقة أو البيئات التي يمكن فيها تبادل المفاتيح بأمان.
- يُستخدم في بعض بروتوكولات الشبكة والتخزين المشفر.

مزاياه

- يتميز بسرعة الأداء وانخفاض استهلاك الموارد.
- مناسب للأنظمة التي تتعامل مع كميات كبيرة من البيانات بسرعة.

تحدياته

- مشكلة توزيع المفاتيح: يجب مشاركة المفتاح بطريقة آمنة بين الطرفين.
- إذا تم اختراق المفتاح، تُصبح كل البيانات المعتمدة عليه غير آمنة.

2. أنواع التشفير

2.2 التشفير غير المتماثل Asymmetric Encryption

ما هو التشفير غير المتماثل؟ هو نوع من التشفير يُستخدم فيه زوج من المفاتيح: مفتاح عام للتشفير، ومفتاح خاص لفك التشفير.

يُمكن لأي شخص استخدام المفتاح العام لتشفير الرسالة، ولكن لا يستطيع فكها إلا من يملك المفتاح الخاص و يعتمد هذا النوع على مسائل رياضية معقّدة تجعل من شبه المستحيل كسر التشفير دون معرفة المفتاح الخاص.

كيفية عمله: المفتاح العام يتم توزيعه علنًا ويُستخدم لتشفير الرسائل - المفتاح الخاص يحتفظ به صاحبه فقط ويُستخدم لفك التشفير.

مثال: عند إرسال رسالة إلى جهة رسمية، نستخدم مفتاحهم العام، وهم فقط يمكنهم فك التشفير بمفتاحهم الخاص.

أمثلة على الاستخدامات: البريد الإلكتروني المشفّر - التوقيع الرقمي للتحقق من المصدر - تبادل المفاتيح في بروتوكولات مثل SSL/TLS - شهادات الأمان في المواقع الإلكترونية HTTPS .

مزاياه: لا حاجة لتبادل المفتاح السري مسبقًا - مناسب للاتصالات المفتوحة مثل الإنترنت.

تحدياته: أبطأ من التشفير المتماثل بسبب العمليات الحسابية المعقدة - غير عملي لتشفير كميات كبيرة من البيانات بمفرده، وغالبًا ما يُستخدم لتبادل المفاتيح فقط.

2. أنواع التشفير

2.3 مقارنة بين التشفير المتماثل وغير المتماثل

طريقة استخدام المفاتيح:

- التشفير المتماثل يستخدم مفتاحًا واحدًا للتشفير وفك التشفير.
- التشفير غير المتماثل يستخدم مفتاحين: عام وخاص.

السرعة والأداء:

- التشفير المتماثل أسرع في التنفيذ ويستهلك موارد أقل.
- التشفير غير المتماثل أبطأ بسبب العمليات الحسابية المعقدة.

توزيع المفاتيح:

- المتماثل يتطلب تبادل المفتاح بشكل آمن بين الطرفين.
- في غير المتماثل، المفتاح العام يُمكن نشره دون خطر.

الاستخدام المثالي:

- المتماثل مناسب للبيئات المغلقة أو الملفات المحلية.
- غير المتماثل مثالي للإنترنت والاتصالات المفتوحة.

2. أنواع التشفير

2.4 مقارنة بين التشفير المتماثل وغير المتماثل

درجة الأمان:

- التشفير غير المتماثل يُعتبر أكثر أمانًا في تبادل المفاتيح، لأنه لا يتطلب إرسال المفتاح الخاص.
- بينما في التشفير المتماثل، إذا تم اعتراض المفتاح، تصبح كل البيانات مهددة.

الاستخدام العملي:

- غالبًا ما يُستخدم التشفير غير المتماثل في بداية الاتصال لتبادل مفتاح سري، ثم يُستخدم التشفير المتماثل لتبادل البيانات بسرعات أعلى.
- هذا الدمج بين النوعين يُعرف باسم التشفير الهجين، ويُستخدم في بروتوكولات مثل TLS/SSL

الموثوقية:

- التشفير غير المتماثل يُستخدم أيضًا لإنشاء التوقيعات الرقمية، التي تضمن أن الرسالة لم يتم تغييرها، وتُثبت هوية المرسل.
- التشفير المتماثل لا يقدّم وسيلة للتحقق من هوية المرسل بدون استخدام تقنيات إضافية.

أمثلة توضيحية:

- عند زيارة موقع إلكتروني آمن HTTPS ، يبدأ الاتصال باستخدام RSA تشفير غير متماثل ، ثم يتم الاتفاق على مفتاح AES تشفير متماثل لتبادل البيانات.

2. أنواع التشفير

2.5 التشفير الكلاسيكي

يُعتبر التشفير الكلاسيكي أقدم أنواع التشفير، وقد استخدم منذ آلاف السنين لحماية المراسلات في الحروب والسياسة. يقوم هذا النوع من التشفير على قواعد بسيطة مثل الاستبدال أو التبديل، دون الاعتماد على خوارزميات رياضية معقدة كما في التشفير الحديث.

أمثلة مشهورة:

- **تشفير قيصر:** يعتمد على تحريك كل حرف بعدد ثابت من المواقع في الأبجدية.
- **تشفير الاستبدال:** يتم استبدال كل حرف برمز أو حرف آخر بناءً على جدول سري.
- **تشفير التبديل:** يتم تغيير ترتيب الحروف داخل الرسالة وفقًا لنمط معيّن.

الخصائص العامة:

- سهل الفهم والتنفيذ يدويًا.
- لا يعتمد على الحوسبة أو المفاتيح المعقدة.
- يُعتبر غير آمن حاليًا ويمكن كسره بسهولة باستخدام التحليل الإحصائي.

أهميته التعليمية:

رغم ضعفه الأمني، لا يزال التشفير الكلاسيكي يُستخدم لأغراض تعليمية لتوضيح المفاهيم الأساسية في علم التشفير، مثل مفهوم "المفتاح" و"السرية".

2. أنواع التشفير

2.6 تطبيقات التشفير المتماثل

التشفير المتماثل يُستخدم على نطاق واسع في الأنظمة التي تتطلب سرعة وكفاءة عالية. يعتمد عليه في حماية البيانات المخزنة أو عند تبادل كميات كبيرة من المعلومات داخل بيئات آمنة.

أمثلة على الاستخدامات:

- **تشفير الملفات:** مثل ملفات PDF أو الأقراص الصلبة باستخدام خوارزمية AES
- **التخزين المحلي:** الأجهزة المحمولة وأجهزة التخزين الخارجية.
- **الشبكات الخاصة:** التشفير بين خوادم داخل نفس المؤسسة.
- **أنظمة قواعد البيانات:** تشفير أعمدة البيانات الحساسة مثل أرقام الهويات.

السبب في الاعتماد عليه:

- أداؤه السريع مقارنةً بالخوارزميات غير المتماثلة.
- مناسب جدًا للأنظمة التي تتيح تبادل المفاتيح بطريقة آمنة مُسبقًا.

نقطة هامة: رغم سرعته، لا يُنصح باستخدام التشفير المتماثل في بيئات مفتوحة مثل الإنترنت دون حماية مناسبة للمفتاح.

2. أنواع التشفير

2.7 تطبيقات التشفير غير المتماثل

يتميّز التشفير غير المتماثل بإمكانية استخدامه في البيئات المفتوحة، مما يجعله أساسًا في حماية الإنترنت والبنية التحتية الرقمية الحديثة.

أمثلة على الاستخدامات:

- **الاتصال الآمن بالمواقع:** عبر HTTPS باستخدام SSL/TLS.
- **إرسال رسائل مشفّرة عبر البريد الإلكتروني:** مثل تقنية PGP.
- **التوقيع الرقمي:** للتحقق من مصدر البيانات وعدم تغييرها.
- **إدارة الهوية:** في أنظمة المصادقة وبطاقات الهوية الرقمية.
- **تبادل المفاتيح:** يُستخدم لتوليد مفتاح مشترك يتم استخدامه لاحقًا في التشفير المتماثل.

الميزة الكبرى: لا حاجة لإرسال المفتاح السري، مما يقلل من خطر اعتراضه.

أسئلة

1. ما الفرق بين التشفير وأمن المعلومات؟
2. اذكر الفرق الرئيسي بين التشفير المتماثل وغير المتماثل من حيث استخدام المفاتيح.
3. اذكر مثالين من الحياة اليومية يتم فيهما استخدام التشفير.
4. لماذا نحتاج إلى التشفير عند نقل أو تخزين البيانات؟
5. ما هي أبرز نقاط القوة والضعف في التشفير الكلاسيكي؟

الأجوبة

1. أمن المعلومات هو مجال شامل يهدف إلى حماية المعلومات من الوصول غير المصرح به، ويشمل عناصر مثل السرية، النزاهة، والتوافر,أما التشفير، فهو تقنية تُستخدم داخل أمن المعلومات لتحقيق عنصر السرية فقط، من خلال تحويل البيانات إلى صيغة غير مفهومة.
2. في التشفير المتماثل، يُستخدم مفتاح واحد مشترك بين الطرفين لتشفير وفك تشفير البيانات, أما في التشفير غير المتماثل، فيتم استخدام مفتاحين: مفتاح عام للتشفير ومفتاح خاص لفك التشفير.
3. تطبيق واتساب الذي يستخدم التشفير من الطرف إلى الطرف لحماية المحادثات - المواقع الإلكترونية التي تستخدم بروتوكول HTTPS لتأمين الاتصال بين المستخدم والخادم.
4. لأن التشفير يضمن حماية البيانات من الوصول غير المصرح به أثناء تنقّلها عبر الشبكات أو عند تخزينها على الأجهزة, كما يساعد في حماية الخصوصية، التحقق من الهوية، وضمان أن البيانات لم تتغيّر.
5. نقاط القوة: سهل الفهم، ويمكن تطبيقه يدويًا - نقاط الضعف: ضعيف أمنيًا وسهل الكسر باستخدام التحليل الإحصائي، لذلك لم يعد مناسبًا لحماية البيانات الحديثة.

3. خوارزميات التشفير المتماثل

3.1 خوارزمية DES – Data Encryption Standard

تُعد خوارزمية DES من أوائل خوارزميات التشفير المتماثل التي حظيت باعتماد رسمي في الولايات المتحدة، وكانت تُستخدم لحماية المعلومات السرية لعقود. ورغم بساطتها، لم تعد آمنة اليوم أمام قدرات الحوسبة الحديثة.

الخصائص:

- تستخدم مفتاحًا بطول 56 بت
- تُشفر البيانات على شكل كتل بحجم 64 بت
- تمر البيانات بـ 16 جولة من العمليات
- تعتمد على خلط واستبدال البتات Substitution & Permutation

ملاحظات: تم كسرها باستخدام هجمات القوة الغاشمة - لم تعد معتمدة في الأنظمة الحديثة

3. خوارزميات التشفير المتماثل

3.2 خوارزمية AES – Advanced Encryption Standard

تم تطوير خوارزمية AESلتحل محل DESوتُوفر مستوى أمان أعلى. وهي اليوم المعيار العالمي المُعتمد في أغلب المؤسسات، بما في ذلك الاستخدامات العسكرية والتجارية.

الخصائص:

- تدعم مفاتيح بطول 128، 192، أو 256 بت
- تُشفر البيانات على شكل كتل بحجم 128 بت
- تمر البيانات بعدة جولات (10–14 جولة حسب طول المفتاح)
- توفر مزيجًا من الأمان والكفاءة في الأداء

مزايا إضافية: مناسبة للأجهزة الضعيفة والمحمولة - شائعة في الشبكات اللاسلكية وتشفير الأقراص الصلبة

3. خوارزميات التشفير المتماثل

3.3 مقارنة بين DES و AES

كلتا الخوارزميتين تنتميان إلى التشفير المتماثل، لكن الفروقات بينهما كبيرة من حيث الأمان والفعالية، مما أدى إلى استبدال DESبـ AESرسميًا.

نقاط المقارنة:

- طول المفتاح: DES 56بت – AES حتى 256 بت
- عدد الجولات: DES 16جولة – AES 10–14 جولة
- الأمان: DES سهل الكسر، AESمقاوم للهجمات
- الأداء: AES أكثر كفاءة عند التنفيذ في الأجهزة الحديثة

خلاصة: AES يُعد الخيار الأفضل حاليًا من جميع النواحي، بينما DES أصبح غير صالح للاستخدام العملي.

3. خوارزميات التشفير المتماثل

3.4 مزايا التشفير المتماثل

يمتاز التشفير المتماثل بعدة جوانب تجعله مفضّلًا في أنظمة معينة، خاصة تلك التي تحتاج إلى سرعة في معالجة البيانات.

أهم المزايا:

- سرعة التشفير وفك التشفير
- كفاءة في استهلاك الموارد
- سهولة التنفيذ البرمجي
- فعالية في تشفير كميات كبيرة من البيانات
- مناسب للأنظمة المحلية أو الشبكات الداخلية

3. خوارزميات التشفير المتماثل

3.5 عيوب التشفير المتماثل

رغم كفاءته، يعاني التشفير المتماثل من بعض التحديات التي تحد من استخدامه في البيئات المفتوحة والعامة.

العيوب الأساسية:

- الحاجة إلى قناة آمنة لتبادل المفتاح
- سهولة اختراق البيانات إذا تم تسريب المفتاح
- عدم القدرة على التحقق من هوية المرسل
- لا يدعم التوقيع الرقمي بشكل مباشر

ملاحظة:

لهذا السبب يُستخدم التشفير المتماثل غالبًا مع التشفير غير المتماثل في أنظمة هجينة.

3. خوارزميات التشفير المتماثل

3.6 تطبيقات التشفير المتماثل

يُستخدم التشفير المتماثل بشكل واسع في التطبيقات التي تتطلب أداء عاليًا وحجم بيانات كبير مع بيئة تحكم داخلي بالمفاتيح.

أمثلة واقعية:

- تشفير الملفات الشخصية والنسخ الاحتياطية
- حماية الأقراص الصلبة باستخدام BitLocker أو FileVault
- قواعد البيانات الحساسة في الشركات
- تطبيقات VPN التي تتطلب تشفيرًا سريعًا للاتصال
- تشفير اتصالات الأجهزة الذكية ضمن نفس الشبكة

ملاحظة: عند استخدامه في بيئة غير آمنة، يجب تأمين المفتاح جيدًا أو دمجه مع تقنيات أخرى.

4. خوارزميات التشفير غير المتماثل

4.1 خوارزمية RSA – Rivest–Shamir–Adleman

خوارزمية RSA هي أشهر خوارزميات التشفير غير المتماثل، وتُستخدم على نطاق واسع في الإنترنت لتأمين الاتصالات والمصادقة الرقمية. تعتمد على مفاهيم رياضية تتعلق بالأعداد الأولية.

الخصائص:

- تقوم على توليد زوج من المفاتيح (عام وخاص) باستخدام ضرب عددين أوليين كبيرين
- المفتاح العام يُستخدم للتشفير، والخاص لفك التشفير
- يعتمد أمانها على صعوبة تحليل العوامل الأولية للأعداد الكبيرة

الاستخدامات: إرسال الرسائل المشفّرة عبر الإنترنت - التوقيع الرقمي والتحقق من الهوية - تبادل المفاتيح في بروتوكولات مثل TLS

4. خوارزميات التشفير غير المتماثل

4.2 آلية عمل RSA

تتكوّن RSAمن ثلاث مراحل رئيسية: توليد المفاتيح، التشفير، وفك التشفير. يُعتبر فهم طريقة عملها مفتاحًا لفهم التشفير غير المتماثل بشكل عام.

مراحل العمل:

- اختيار عددين أوليين كبيرين
- حساب حاصل ضربهما وإنشاء مفاتيح بناءً على خواص رياضية
- استخدام المفتاح العام لتشفير البيانات
- استخدام المفتاح الخاص لفك التشفير

ملاحظة: كلما زاد طول المفتاح، زادت صعوبة كسره، ولكن ذلك يؤدي أيضًا إلى بطء في الأداء.

4. خوارزميات التشفير غير المتماثل

4.3 خوارزمية Diffie-Hellman

خوارزمية Diffie-Hellman تُستخدم لتبادل المفاتيح بين طرفين بطريقة آمنة حتى في وجود طرف ثالث يتجسس على الاتصال.

آلية العمل:

- لا تُشفّر البيانات نفسها، بل تُستخدم لإنشاء مفتاح مشترك
- تعتمد على العمليات الحسابية ضمن المجموعات الرياضية (الضرب المعياري)
- يُمكن للطرفين التوصل إلى نفس المفتاح دون إرسال أي مفتاح صريح

الأهمية: تتيح لاحقًا استخدام تشفير متماثل بمفتاح تم توليده بأمان - تُستخدم في بروتوكولات TLSوVPN

4. خوارزميات التشفير غير المتماثل

4.4 الفرق بين RSA وDiffie-Hellman

كلا الخوارزميتين تُستخدمان في أنظمة التشفير غير المتماثل، لكن بينهما فروقات من حيث الهدف وطريقة العمل.

المقارنة:

- RSA تُستخدم لتشفير البيانات أو توقيعها
- Diffie-Hellman تُستخدم فقط لتوليد مفتاح مشترك
- RSA توفر مصادقة وهوية
- Diffie-Hellman لا توفّر مصادقة وحدها
- كلاهما مبني على مشاكل رياضية يصعب حلها (تحليل العوامل أو اللوغاريتمات)

ملاحظة: في العديد من البروتوكولات يتم الجمع بينهما حسب الحاجة.

4. خوارزميات التشفير غير المتماثل

4.5 الاستخدامات العملية للتشفير غير المتماثل

التشفير غير المتماثل يشكّل الأساس للعديد من تقنيات الأمان الرقمية المستخدمة يوميًا سواء من قبل الأفراد أو المؤسسات.

أمثلة على الاستخدام:

- المصادقة عند تسجيل الدخول إلى مواقع الإنترنت
- إرسال بريد إلكتروني مشفّر بين طرفين
- التحقق من توقيع الملفات والمستندات
- إنشاء اتصال آمن بين المتصفح والموقع ((HTTPS
- حماية معاملات التجارة الإلكترونية

النتيجة: بدون التشفير غير المتماثل، ستكون الإنترنت بيئة غير آمنة للمعاملات والمراسلات الحساسة.

4. خوارزميات التشفير غير المتماثل

4.6 مزايا وعيوب التشفير غير المتماثل

رغم الأمان العالي الذي يوفّره هذا النوع من التشفير، إلا أن له بعض القيود، خاصة عند التعامل مع البيانات الكبيرة أو الأجهزة الضعيفة.

المزايا:

- لا حاجة لتبادل المفاتيح مسبقًا
- يوفر مصادقة وتوقيع رقمي
- مناسب للبيئات المفتوحة مثل الإنترنت

العيوب:

- أبطأ من التشفير المتماثل
- غير عملي لتشفير كميات كبيرة من البيانات
- قد يكون أكثر تعقيدًا من حيث التنفيذ البرمجي

ملاحظة: يتم التغلب على هذه العيوب باستخدامه لتبادل المفاتيح فقط، ثم اعتماد تشفير متماثل لنقل البيانات.

5. خوارزميات التجزئة Hashing

5.1 ما هي خوارزميات التجزئة؟

خوارزميات التجزئة هي دوال رياضية تُستخدم لتحويل البيانات من أي حجم إلى سلسلة ثابتة الطول تُسمّى **قيمة التجزئة Hash Value** . تُستخدم للتحقق من سلامة البيانات وليس لتشفيرها.

الخصائص الأساسية:

- المدخلات قد تكون بأي حجم، لكن الناتج دائمًا ثابت الطول
- لا يمكن إعادة بناء البيانات الأصلية من قيمة التجزئة
- تغيير بسيط في البيانات يؤدي إلى تغيير كامل في ناتج التجزئة
- لا يُفترض وجود حالتين مختلفتين تُنتجان نفس القيمة Collision

ملاحظة:

خوارزميات التجزئة ليست وسيلة لتأمين البيانات بسرّية، بل للتحقق من سلامتها.

5. خوارزميات التجزئة Hashing

5.2 أشهر خوارزميات التجزئة

على مر السنوات، ظهرت عدة خوارزميات تجزئة، بعضها أصبح غير آمن، والبعض الآخر ما زال يُستخدم في التطبيقات الحديثة.

أشهر الخوارزميات:

- **MD5**: كانت شائعة، لكن كُسرت ويُمنع استخدامها في الأنظمة الحديثة
- **SHA-1**: أكثر أمانًا من MD5 لكنها لم تعد موثوقة بالكامل
- **SHA-256**: جزء من عائلة SHA-2، وتُعد من أكثر الخوارزميات استخدامًا وأمانًا حاليًا
- **SHA-3**: الأحدث، تم تطويره بتقنيات مختلفة لمزيد من الأمان المستقبلي

نقطة مهمة:

كلما زاد طول ناتج التجزئة، زادت صعوبة العثور على تصادم (Collision).

5. خوارزميات التجزئة Hashing

5.3 أمثلة عملية على استخدام التجزئة

تُستخدم التجزئة بشكل واسع في كثير من التطبيقات اليومية التي تتعلق بالتحقق من الهوية أو سلامة الملفات.

أمثلة على الاستخدام:

- التحقق من سلامة الملفات: عند تحميل ملف، يتم مقارنته بقيمة تجزئة منشورة مسبقًا
- المصادقة: تُستخدم لتخزين كلمات المرور على شكل قيم تجزئة بدلًا من النص الأصلي
- التوقيع الرقمي: يتم توقيع قيمة التجزئة بدلاً من توقيع المستند بالكامل
- أنظمة النسخ الاحتياطي: لتحديد الملفات التي تغيّرت فقط

خلاصة: تُستخدم التجزئة في كل ما يحتاج إلى التحقق دون الحاجة لكشف البيانات الأصلية.

5. خوارزميات التجزئة Hashing

5.4 التجزئة وتخزين كلمات المرور

واحدة من أهم استخدامات التجزئة هي حماية كلمات المرور في قواعد البيانات. بدلاً من حفظ كلمة المرور بنص صريح، يتم حفظ قيمتها التجزيئية فقط.

الآلية:

- عندما يُدخل المستخدم كلمة مروره، يتم تجزئتها فورًا
- تتم مقارنة القيمة الناتجة مع القيمة المخزّنة
- إذا تطابقت، يتم السماح بالدخول

تعزيز الأمان باستخدام تقنيات إضافية:

- **Salt:** سلسلة عشوائية تُضاف لكلمة المرور قبل تجزئتها لمنع هجمات القواميس
- **Iterations:** تكرار عملية التجزئة عدة مرات لزيادة صعوبة الكسر

ملاحظة: لا يمكن استرجاع كلمة المرور من قيمة التجزئة، مما يجعل هذه الطريقة أكثر أمانًا.

5. خوارزميات التجزئة Hashing

5.5 التجزئة في البلوكتشين والعملات الرقمية

البلوك تشين Blockchain يعتمد بشكل كبير على خوارزميات التجزئة لضمان سلامة البيانات وربط الكتل ببعضها بطريقة آمنة.

أوجه الاستخدام:

- **ربط الكتل:** كل كتلة تحتوي على تجزئة الكتلة السابقة، ما يمنع تعديل البيانات دون كسر السلسلة
- **إثبات العمل Proof of Work :** يُطلب العثور على تجزئة تبدأ بعدد معيّن من الأصفار، ما يتطلب جهدًا حاسوبيًا
- **توقيع المعاملات:** يتم توليد تجزئة للمعاملة وتوقيعها لضمان صحتها

النتيجة: من دون التجزئة، لن يكون بالإمكان تحقيق سلامة البيانات أو مقاومة التلاعب في نظم البلوك تشين.

اسئلة

1. ما الفرق الأساسي بين خوارزمية DES وAES؟ ولماذا تم استبدال DES؟
2. كيف تختلف RSA عن Diffie-Hellman من حيث الوظيفة والاستخدام؟
3. اذكر استخدامين عمليين لخوارزميات التجزئة.
4. ما هي أهم مزايا التشفير المتماثل، ولماذا يُستخدم مع التشفير غير المتماثل في بعض الأحيان؟
5. هل يمكن استرجاع البيانات الأصلية من قيمة التجزئة؟ ولماذا؟

الاجوبة

1. الفرق الأساسي هو أن DES تستخدم مفتاحًا بطول 56 بت، بينما AESتدعم مفاتيح أطول (128، 192، 256 بت)، مما يجعل AES أكثر أمانًا.

تم استبدال DES بسبب ضعفها أمام هجمات القوة الغاشمة، في حين أن AES توفر أمانًا عاليًا وسرعة وكفاءة أكبر.

2. RSA تُستخدم لتشفير البيانات والتوقيع الرقمي، وهي تتيح إرسال رسائل مشفّرة يمكن فقط للمستلم فك تشفيرها.

Diffie-Hellman لا تُستخدم لتشفير البيانات، بل لتبادل مفتاح مشترك بين طرفين بأمان حتى عبر قناة غير موثوقة. أي أنها تُستخدم لإنشاء قناة آمنة لتشفير لاحق باستخدام مفاتيح متماثلة.

3. تخزين كلمات المرور في قواعد البيانات بشكل آمن بحيث لا تُحفظ النصوص الأصلية - التحقق من سلامة الملفات عند تحميلها من الإنترنت، من خلال مقارنة قيمة التجزئة.

الاجوبة

4. أهم مزاياه: السرعة، الكفاءة، واستهلاك منخفض للموارد.

يُستخدم مع التشفير غير المتماثل لتجاوز مشكلة توزيع المفاتيح، حيث يُستخدم التشفير غير المتماثل أولًا لتبادل مفتاح التشفير المتماثل، ثم يُستخدم الأخير لنقل البيانات بسرعة.

5. لا، لا يمكن استرجاع البيانات الأصلية من قيمة التجزئة لأن التجزئة عملية **غير قابلة للعكس**. تم تصميم دوال التجزئة بحيث تكون أحادية الاتجاه، مما يمنع استرجاع المدخلات الأصلية.

6. التشفير في التطبيقات العملية

6.1 التشفير في الشبكات

تُعد الشبكات من أبرز البيئات التي تتطلب حماية المعلومات أثناء انتقالها. يُستخدم التشفير لضمان سرّية الاتصال وسلامة البيانات بين الأطراف المختلفة عبر الإنترنت.

أمثلة على التشفير في الشبكات:

HTTPS تأمين نقل البيانات بين المتصفح والموقع باستخدام بروتوكولات SSL/TLS.

VPN تستخدم بروتوكولات تشفير قوية لإنشاء نفق مشفّر بين المستخدم والشبكة.

TLS/SSL بروتوكولات تشفير تعتمد على التشفير غير المتماثل في البداية، ثم التشفير المتماثل لنقل البيانات.

ملاحظة: من دون التشفير، فإن البيانات المرسلة عبر الإنترنت تكون مكشوفة وسهلة الاعتراض.

6. التشفير في التطبيقات العملية

6.2 التشفير في الهواتف المحمولة

أصبحت الهواتف الذكية تحتوي على كميات كبيرة من البيانات الشخصية والحساسة، ولذلك يتم دمج تقنيات التشفير فيها بشكل أساسي.

أهم تطبيقات التشفير في الهواتف:

- تشفير المحادثات: تطبيقات مثل واتساب وتيليغرام تستخدم التشفير من الطرف إلى الطرف End-to-End Encryption .
- تشفير الجهاز بالكامل: أنظمة iOS وAndroid توفّر خاصية تشفير القرص الكامل Full Disk Encryption .
- حماية النسخ الاحتياطية: تُشفّر النسخ السحابية أو المحلية لضمان عدم الوصول إليها من قبل الغير.

ملاحظة:

فقدان كلمة المرور في بعض الأنظمة يُعني فقدان البيانات بالكامل بسبب قوة التشفير المطبق.

6. التشفير في التطبيقات العملية

6.3 التشفير في الأنظمة البنكية

تُعد الأنظمة البنكية من أكثر البيئات التي تحتاج إلى حماية مشددة للبيانات، خصوصًا في المعاملات الإلكترونية والحسابات المصرفية.

أوجه استخدام التشفير في البنوك:

- حماية بيانات العملاء: مثل أرقام الحسابات والبطاقات البنكية.
- تشفير العمليات: جميع المعاملات المصرفية عبر الإنترنت تمر عبر قنوات مشفّرة.
- توقيعات رقمية: تُستخدم للتحقق من صحة التحويلات أو الوثائق الإلكترونية.
- أجهزة الصرّاف الآلي: تعتمد على تشفير بين الجهاز والمخدّم البنكي.

خلاصة:

دون تشفير فعّال، فإن الأنظمة البنكية تصبح معرضة للاختراق وفقدان الثقة.

6. التشفير في التطبيقات العملية

6.4 التشفير في البريد الإلكتروني:

يُستخدم التشفير في البريد الإلكتروني لحماية الرسائل من أن تُقرأ من قبل أي جهة غير مصرح لها، وخاصة عند إرسال معلومات حساسة.

أنواع التشفير في البريد الإلكتروني:

- PGP / GPG: أنظمة تعتمد على التشفير غير المتماثل لتأمين المراسلات.
- S/MIME: تستخدم شهادات رقمية لتشفير البريد وتوقيعه رقميًا.
- Webmail Encryption: مثل Gmail أو Outlook التي تقدم تشفيرًا تلقائيًا للبريد المخزن.

تحديات التشفير في البريد:

توزيع المفاتيح العامة، صعوبة الاستخدام بالنسبة للمستخدم العادي، وعدم دعم بعض المنصات للبروتوكولات القوية.

6. التشفير في التطبيقات العملية

6.5 شهادات الأمان الرقمية Digital Certificates

شهادات الأمان هي ملفات رقمية تُصدرها هيئات موثوقة وتُستخدم للتأكد من هوية المواقع أو الأفراد وتشفير الاتصال.

مكونات الشهادة:

- الاسم، اسم الجهة المالكة، المفتاح العام، توقيع الهيئة المصدّرة، وتاريخ الانتهاء.
- تُستخدم الشهادات ضمن بروتوكول HTTPS لتأمين الاتصال.

دورها في التشفير:

- توفر الثقة بين المتصفح والموقع الإلكتروني
- تُستخدم لتشفير الجلسات باستخدام مفتاح الجهة المالكة
- تؤدي دورًا مهمًا في المصادقة وتجنب الهجمات مثل man-in-the-middle

ملاحظة:

يجب أن تكون الشهادة صادرة من جهة موثوقة ومعتمدة ليتم قبولها من قبل المتصفحات.

6. التشفير في التطبيقات العملية

6.6 التشفير في التطبيقات اليومية

التشفير أصبح جزءًا لا يتجزأ من أدواتنا اليومية، حتى لو لم نلاحظه بشكل مباشر، ويُستخدم بشكل تلقائي في عدد من الخدمات والبرامج.

أمثلة على تطبيقات التشفير اليومية:

- تخزين الملفات في السحابة: مثل Google Drive وiCloud
- تطبيقات المراسلة: مثل Signal، Viber، iMessage
- تطبيقات الدفع: Apple Pay، Google Pay
- الأنظمة التشغيلية: تشفير الملفات والمجلدات في أنظمة ويندوز وmacOS

النتيجة:

الوعي بأهمية التشفير واستخدام الأدوات التي تضمن الأمان الرقمي أصبح ضرورة في العالم الحديث.

7. التهديدات والتحديات

7.1 هجمات القوة الغاشمة Brute Force Attacks

هجمات القوة الغاشمة هي واحدة من أقدم وأكثر أنواع الهجمات المباشرة على أنظمة التشفير. يقوم المهاجم فيها بمحاولة تجربة كل الاحتمالات الممكنة حتى يتمكن من كسر المفتاح وفك التشفير.

خصائص الهجوم:

- لا تحتاج إلى معرفة مسبقة بالخوارزمية أو المفتاح
- تعتمد على قدرة الحوسبة وعدد المحاولات في الثانية
- فعّالة ضد الخوارزميات ذات المفاتيح القصيرة مثل DES
- كلما زاد طول المفتاح، أصبحت الهجمة أبطأ وغير عملية

ملاحظة:

أهم وسيلة دفاع ضد هذا النوع من الهجمات هي استخدام مفاتيح طويلة ومعقدة يصعب توليدها عشوائيًا.

7. التهديدات والتحديات

7.2 الهجمات الرياضية والتحليلية

بعض الخوارزميات قد تحتوي على نقاط ضعف رياضية، يمكن استغلالها في اختراق النظام دون تجربة كل الاحتمالات، مما يجعل هذه الهجمات أخطر من القوة الغاشمة.

أمثلة على الهجمات التحليلية:

- هجمات التحليل التفاضلي Differential Cryptanalysis : تعتمد على مقارنة عدة رسائل مشفّرة وملاحظة الفروقات
- التحليل الخطي Linear Cryptanalysis : يستهدف إيجاد علاقات خطية بين المدخلات والمخرجات
- هجمات التصادم Collision Attacks : تستهدف دوال التجزئة لإيجاد مدخلين لهما نفس الناتج

ملاحظة:

كل خوارزمية تمر باختبارات أكاديمية مكثفة قبل اعتمادها للتأكد من عدم وجود هذه الثغرات.

7. التهديدات والتحديات

7.3 التحدي الكمومي Quantum Threat

مع تطوّر الحوسبة الكمومية، ظهرت تهديدات حقيقية لخوارزميات التشفير التقليدية، خاصة تلك التي تعتمد على مشاكل رياضية قد تُحل بكفاءة باستخدام الحوسبة الكمومية.

أثر الحوسبة الكمومية:

- يمكنها كسر خوارزميات مثل RSA وDiffie-Hellman باستخدام خوارزمية Shor
- قد تُضعف دوال التجزئة باستخدام خوارزمية Grover
- تعتمد على مفاهيم غير تقليدية مثل التراكب والتشابك

الاستجابة:

بدأ الباحثون في تطوير خوارزميات مقاومة للكم Post-Quantum Cryptography استعدادًا للانتقال إلى عصر ما بعد الكم.

7. التهديدات والتحديات

7.4 التوازن بين الأمان وسهولة الاستخدام

كلما زادت قوة التشفير وتعقيده، زادت الصعوبة في استخدام النظام، والعكس صحيح. لهذا السبب، يواجه المطورون تحديًا مستمرًا في تحقيق التوازن المطلوب.

أمثلة على التحديات:

- تشفير البريد الإلكتروني القوي غالبًا ما يكون معقدًا للمستخدم العادي
- حماية الهواتف بكلمات مرور طويلة قد تؤدي إلى ضعف تجربة المستخدم
- الأنظمة المصرفية تحتاج إلى أمان قوي دون أن تؤثر على سهولة العمليات

الحلول المقترحة:

- تطوير واجهات استخدام سهلة تخفي التعقيد التقني
- الجمع بين الأمن القوي وتجربة المستخدم الجيدة Security by Design

7. التهديدات والتحديات

7.5 الحاجة المستمرة للتحديث والتكيّف

في عالم متسارع تقنيًا، لا يكفي أن يكون النظام مشفّرًا، بل يجب أن يتم تحديثه باستمرار لمواكبة التهديدات الجديدة وتحسين الأداء.

أسباب الحاجة للتحديث:

- ظهور ثغرات أمنية جديدة في الخوارزميات
- زيادة قدرات المخترقين والحواسيب
- تغيّرات في اللوائح والقوانين التي تفرض متطلبات أمنية محددة

أمثلة:

- الانتقال من SHA-1 إلى SHA-256
- إحلال DES بـ AES
- تطوير معايير تشفير مقاومة للهجمات الكمومية

النتيجة:

أمن المعلومات ليس حالة ثابتة، بل عملية مستمرة تتطلب مراقبة، وتحديث، وتكيّف مع المستجدات.

8. مستقبل التشفير والتقنيات الحديثة

8.1 التشفير الكمومي Quantum Cryptography

التشفير الكمومي هو نوع جديد من التشفير يعتمد على مبادئ فيزياء الكم بدلاً من المشكلات الرياضية التقليدية، مما يمنحه قوة أمنية فريدة من نوعها.

الخصائص الأساسية:

- يعتمد على الفوتونات (جسيمات الضوء) لنقل المفاتيح
- إذا حاول أي طرف خارجي التجسس، تتغير حالة الفوتونات فورًا ويتم اكتشاف الهجوم
- يستخدم في بروتوكولات مثل BB84 لتوزيع المفاتيح الآمنة Quantum Key Distribution

المزايا:

- لا يعتمد على صعوبة كسر المفتاح.
- مقاوم للهجمات المستقبلية حتى باستخدام الحواسيب الكمومية

ملاحظة:

ما زال هذا النوع من التشفير في مرحلة البحث والتجريب، لكنه واعد جدًا في تأمين الاتصالات الحساسة مستقبلاً.

8. مستقبل التشفير والتقنيات الحديثة

8.2 التشفير والذكاء الاصطناعي AI & Cryptography

الذكاء الاصطناعي أصبح عنصرًا جديدًا في ميدان التشفير، وقد يستخدم في كلا الاتجاهين: تعزيز الأمان، أو اختراق الأنظمة.

كيف يُستخدم الذكاء الاصطناعي؟

- **للتأمين:** كشف الأنماط الغريبة، التنبؤ بالهجمات، تحسين توليد المفاتيح
- **للهجوم:** تحليل كميات ضخمة من البيانات واكتشاف الثغرات أو تكرار الأنماط
- **التشفير التكيّفي:** تصميم خوارزميات تتغيّر تلقائيًا حسب طبيعة التهديد

التحدي المستقبلي:

أن تصبح الهجمات مدعومة بالذكاء الاصطناعي، مما يتطلب أنظمة دفاع أكثر ذكاءً وتفاعلًا في الوقت الحقيقي.

8. مستقبل التشفير والتقنيات الحديثة

8.3 التشفير في إنترنت الأشياء IoT Encryption

تواجه أجهزة إنترنت الأشياء IoT تحديات كبيرة فيما يخص التشفير، بسبب ضعف قدراتها الحاسوبية وقلة مواردها، رغم حساسيتها الأمنية.

أبرز التحديات:

- محدودية الطاقة والمعالجة تجعل تنفيذ التشفير التقليدي صعبًا
- صعوبة تحديث البرمجيات أو تصحيح الثغرات
- عدد الأجهزة الهائل يفتح أبوابًا لهجمات جماعية

الحلول المقترحة:

- تطوير خوارزميات تشفير خفيفة الوزن Lightweight Cryptography
- الاعتماد على المعايير المصغّرة من AES و SHA
- تطبيق مبدأ Zero Trust في البنية الشبكية للأجهزة

خلاصة:

بدون تشفير فعّال، تبقى بيئة إنترنت الأشياء عرضة للاختراق واسع النطاق.

8. مستقبل التشفير والتقنيات الحديثة

8.4 اتجاهات التشفير المستقبلية

مع التقدّم التقني المتسارع، تتجه صناعة التشفير إلى اعتماد معايير جديدة واستراتيجيات متكيّفة لحماية البيانات.

أبرز الاتجاهات:

- التشفير ما بعد الكم Post-Quantum Cryptography : خوارزميات مصمّمة لتقاوم أجهزة كمومية
- التشفير الموزّع: بدون خادم مركزي، كما في البلوك تشين
- التوقيع الرقمي البيومتري: الدمج بين التشفير وخصائص المستخدم الحيوية
- الخصوصية التفاضلية: تشفير يوازن بين الخصوصية وتحليل البيانات

ملاحظة:

الاستعداد للتغيّرات المستقبلية يبدأ بفهم التهديدات اليوم، وبناء نظم تشفير مرنة وقابلة للتطور.

روابط خارجية

كورسات تعليمية في التشفير وأمن المعلومات

1. Cryptography I – Stanford (Coursera)

https://www.coursera.org/learn/crypto

دورة أكاديمية ممتازة من جامعة ستانفورد مقدمة من البروفيسور دان بونيت.

2. Introduction to Cyber Security – FutureLearn (Open University)

https://www.futurelearn.com/courses/introduction-to-cyber-security

مقدمة شاملة لأمن المعلومات ومبادئ التشفير.

3. Applied Cryptography – edX (University of Colorado)

https://www.edx.org/course/applied-cryptography

دورة عملية لفهم التشفير المطبّق في الأنظمة الواقعية

روابط خارجية

أدوات مجانية لتجربة التشفير: OpenSSL (Linux/Windows)

https://www.openssl.org/

أداة سطر أوامر قوية لتوليد المفاتيح، التوقيع، وفك التشفير: **CyberChef (Web tool)**

https://gchq.github.io/CyberChef/

أداة مرئية تفاعلية لتحويل البيانات وتجربة التشفير، من تطوير GCHQ البريطاني: **CrypTool تعليمي – Windows**

https://www.cryptool.org/en/

برنامج مجاني يشرح كيف تعمل خوارزميات التشفير القديمة والحديثة خطوة بخطوة: **HashCalc (Windows)**

https://www.slavasoft.com/hashcalc/

أداة بسيطة لحساب التجزئة باستخدام MD5، SHA1، SHA256، إلخ.

روابط خارجية

منصات تدريب واختبار عملي

1. TryHackMe – Cybersecurity Learning Labs

https://tryhackme.com/

منصة تدريب تفاعلية تشمل مختبرات للتشفير، الشبكات، واختبار الاختراق.

2. Hack The Box – Cybersecurity Challenges

https://www.hackthebox.com/

مختبرات عملية لمستويات متقدمة في الأمن السيبراني، تشمل تمارين تشفير.

روابط خارجية

كتب مجانية مفتوحة المصدر

1. Crypto101 – A free introductory book on cryptography.

https://crypto101.io/

كتاب إلكتروني مجاني يشرح مفاهيم التشفير من الصفر.

2. Introduction to Modern Cryptography (by Katz & Lindell).

https://www.cs.umd.edu/~jkatz/imc.html

مرجع أكاديمي يستخدم في عدد من الجامعات – غير مجاني لكن ينصح به للمتقدمين.

المراجع

1. **William Stallings**
Cryptography and Network Security: Principles and Practice
(7th Edition, Pearson, 2017)
➤مرجع أكاديمي معتمد لتدريس التشفير في الجامعات حول العالم.
2. **Katz, Jonathan & Lindell, Yehuda**
Introduction to Modern Cryptography
(3rd Edition, CRC Press, 2020)
➤يناقش خوارزميات التشفير الحديثة بأسلوب رياضي دقيق.
3. **Bruce Schneier**
Applied Cryptography: Protocols, Algorithms, and Source Code in C
(2nd Edition, Wiley, 1996)
➤مرجع تطبيقي كلاسيكي يحتوي على شرح شامل لمعظم الخوارزميات.
4. **Paar, Christof & Pelzl, Jan**
Understanding Cryptography: A Textbook for Students and Practitioners
(Springer, 2010)
➤مناسب لطلاب البكالوريوس ويحتوي على شروحات مبسطة ورسوم توضيحية.

المراجع

5. **Open Web Application Security Project (OWASP)**
https://owasp.org/
➤مؤسسة مفتوحة المصدر تقدّم محتوى غنيًا حول أمن المعلومات وتطبيقات التشفير.

6. **National Institute of Standards and Technology (NIST)**
https://csrc.nist.gov/
➤الجهة الرسمية المسؤولة عن معايير التشفير مثل AES، SHA.

7. **Crypto101 – Free Book**
https://crypto101.io/
➤كتاب مفتوح المصدر يشرح أساسيات التشفير بطريقة عملية وحديثة.

8. **Coursera – Cryptography I (Stanford University)**
https://www.coursera.org/learn/crypto
➤دورة شهيرة مقدمة من جامعة ستانفورد تعرّف بأسس التشفير النظري والعملي.

شكرا لكم