

1. ما هو التشفير المتماثل؟ اشرح كيف يعمل مع تقديم مثال عملي.

التشفير المتماثل هو نوع من التشفير حيث يتم استخدام نفس المفتاح لتشفير وفك تشفير البيانات. يعمل التشفير المتماثل عن طريق تحويل النص العادي إلى نص مشفر باستخدام خوارزمية ومفتاح معين، ويمكن عكس العملية باستخدام نفس المفتاح.

****مثال عملي****

والمفتاح هو "3"، يمكننا استخدام خوارزمية التشفير القيصري لتحويل "HELLO" التشفير: ** إذا كان لدينا النص العادي ** - "KHOOR" النص إلى

"HELLO" إلى النص العادي "KHOOR" فك التشفير: ** باستخدام نفس المفتاح "3"، يمكننا تحويل النص المشفر ** -

2. ما هو التشفير غير المتماثل؟ اشرح كيف يعمل مع تقديم مثال عملي.

التشفير غير المتماثل يستخدم زوجًا من المفاتيح: مفتاح عام للتشفير ومفتاح خاص لفك التشفير. المفتاح العام يمكن مشاركته مع الجميع، بينما المفتاح الخاص يجب أن يبقى سرّيًا.

****مثال عملي****

التشفير: ** إذا أراد شخص ما إرسال رسالة مشفرة إليك، يمكنه استخدام مفتاحك العام لتشفير الرسالة ** -

فك التشفير: ** يمكنك استخدام مفتاحك الخاص لفك تشفير الرسالة واستعادة النص العادي ** -

3. قارن بين التشفير المتماثل والتشفير غير المتماثل من حيث السرعة والأمان.

السرعة: ** التشفير المتماثل أسرع بكثير من التشفير غير المتماثل لأنه يستخدم خوارزميات أبسط وأقل تعقيدًا ** -

الأمان: ** التشفير غير المتماثل أكثر أمانًا لأنه لا يتطلب مشاركة المفتاح الخاص، مما يقلل من خطر تعرضه للاختراق ** -

4. ما هي الخطوات الأساسية لتشفير رسالة باستخدام خوارزمية التشفير المتماثل؟

1. اختيار خوارزمية التشفير (مثل AES).

2. توليد مفتاح التشفير.

3. استخدام المفتاح والخوارزمية لتشفير النص العادي.

4. إرسال النص المشفر إلى المستلم.

5. كيف يتم استخدام التشفير غير المتماثل في نظام التشفير الحديث؟ اشرح دور المفتاح العام والمفتاح الخاص.

في نظام التشفير الحديث، يتم استخدام التشفير غير المتماثل لتأمين تبادل المفاتيح وتوقيع البيانات. المفتاح العام يستخدم لتشفير البيانات أو التحقق من التوقيع الرقمي، بينما المفتاح الخاص يستخدم لفك تشفير البيانات أو إنشاء التوقيع الرقمي.

6. ما هي مزايا التشفير المتماثل مقارنة بالتشفير غير المتماثل؟

السرعة: ** التشفير المتماثل أسرع وأكثر كفاءة ** -

البساطة:** يتطلب إدارة مفتاح واحد فقط ** -

ما هي عيوب التشفير المتماثل؟ وكيف يمكن التغلب عليها باستخدام تقنيات إضافية؟ 7. ###

مشاركة المفتاح:** يجب مشاركة المفتاح السري بين الأطراف، مما يزيد من خطر تعرضه للاختراق ** -

التغلب على العيوب:** يمكن استخدام التشفير غير المتماثل لتأمين تبادل المفاتيح، مما يقلل من خطر تعرض المفتاح ** -
السري للاختراق.

اشرح كيف يمكن استخدام التشفير غير المتماثل لضمان سلامة وتوثيق البيانات في عملية تبادل الرسائل 8. ###

يمكن استخدام التشفير غير المتماثل لتوقيع الرسائل رقميًا باستخدام المفتاح الخاص للمرسل. يمكن للمستلم استخدام المفتاح العام للمرسل للتحقق من صحة التوقيع وضمان أن الرسالة لم تتغير.

وكيف يمكن تقليل احتمالية حدوثه في التشفير المتماثل؟ (Dictionary Attack) ما هو هجوم القاموس 9. ###

هجوم القاموس هو نوع من الهجمات التي يستخدم فيها المهاجم قائمة من الكلمات الشائعة أو العبارات لتخمين المفتاح أو كلمة المرور. لتقليل احتمالية حدوثه:

استخدام كلمات مرور قوية ومعقدة -

لإضافة عشوائية إلى كلمات المرور (salting) استخدام تقنيات مثل التمليح -

أعط مثالاً على تطبيق عملي لاستخدام التشفير في حماية البيانات على الإنترنت، ووضح أي نوع من التشفير يُفضل 10. ###
استخدامه في هذا السياق.

HTTPS مثال عملي:** تأمين الاتصالات عبر الإنترنت باستخدام بروتوكول **

نوع التشفير:** يتم استخدام التشفير غير المتماثل لتأمين تبادل المفاتيح، ثم يتم استخدام التشفير المتماثل لتشفير ** -
البيانات الفعلية المتبادلة بين الخادم والمستخدم. هذا يوفر سرعة وأماناً عاليين.