* مقدمة



أسماء المشاركين :

* زكي السادة
* محمد الصفواني
* عبدالرحمن الشمراني
* حسن ال صفوان
* حسين شعبان
* فيصل الرويمي
* عبدالله ال قريش
* مبارك الشمري
* محمد رمضان
* رشيد الرويلي
* خالد ال مرعي
* تعريف التشفير:

التشفير هو العملية التي تدخل على النص المقروء، بحيث لا يمكن قراءته، إلا من عن طريق الشخص الذي لديه الرمز السري أو مفتاح فك التشفير، ويساعد في توفير أمان البيانات للمعلومات الحساسة. يمكن أن يساعد التشفير في حماية البيانات التي ترسلها وتستقبلها، ويمكن أن يشمل ذلك الرسائل النصية المخزنة على هاتفك الذكي، والمعلومات المصرفية المرسلة من خلال حسابك عبر الإنترنت.

* كيف يتم تشفير البيانات؟

يتم استخدام "تشفير البيانات" لردع الأطراف الخبيثة عن الوصول إلى البيانات الحساسة، ويعد تشفير البيانات خطًا مهمًا للدفاع في بنية الأمن السيبراني، مما يجعل استخدام البيانات التي يتم اعتراضها أمرًا صعبًا قدر الإمكان.

ويمكن تطبيق التشفير على جميع أنواع احتياجات حماية البيانات، بدءًا من معاملات الحكومة إلى معاملات بطاقات الائتمان الشخصية.

* التشفير المتماثل Symmetric Encryption

تعرف عملية التشفير التي تستخدم فيها نفس المفاتيح لتشفير وفك تشفير المعلومات بإسم تشفير المفتاح المتماثل Symmetric Key Encryption، وقد تسمى أيضا Secret Key Encryption.

**أمثلة على ذلك:**

1.Data Encryption Standard DES.

2.Triple-DES 3DES.

3.International Data Encryption Algorithm IDEA.

4.BLOWFISH.



**السمات البارزة للتشفير بالمفتاح المتماثل:**

o يجب على جميع الأشخاص مشاركة المفتاح السري قبل إرسال المعلومات.

o يوصى بتغيير المفاتيح بانتظام لمنع أي هجوم على النظام.

o هناك حاجة إلى وجود آلية قوية لتبادل المفتاح بين الأطراف المتواصلة، بما أن المفاتيح مطلوبة لتغييرها بانتظام، تصبح هذه الآلية باهظة الثمن ومكلفة.

o لتمكين الاتصال بين مجموعة من الاشخاص نحتاج إلى وجود مفتاح بين كل شخصين، حيث يكون عدد المفاتيح المطلوبة لمجموعة بها n من الأشخاص هي n × (n - 1) / 2.

**عوائق تشفير المفتاح المتماثل:**

1. **تكوين المفتاح:** قبل أي اتصال يحتاج الطرفان إلى الاتفاق على مفتاح سري، هذا يتطلب وجود آلية إنشاء مفتاح سري بشكل آمن.

2. **مشكلة الثقة:** بما أن المرسل والمستقبل يستخدمان نفس المفتاح فهناك مطلب ضمني بأن يثق المرسل والمستقبل في بعضهما البعض، فمثلا قد يفقد المستقبل المفتاح للمهاجمين ولم يتم إبلاغ المرسل!

3. **التواصل العام:** يحتاج الناس إلى تبادل المعلومات مع أطراف غير معروفة وغير موثوق بها، كالتواصل بين البائع عبر الإنترنت والعميل.

أدت جميع هذه القيود إلى ظهور أنظمة تشفير المفتاح الغير متماثل.

**معرفة أنواع التشفير المتماثل:**  
هناك نوعان رئيسيان من الشفرات المتماثلة: **الكتلة والدفق**. في تشفير الكتلة، يتم تقسيم المعلومات إلى كتل ذات طول ثابت (على سبيل المثال، 64 أو 128 بت) ثم يتم تشفير هذه الكتل واحدة تلو الأخرى، يتم تطبيق المفتاح على كل كتلة بترتيب محدد.

* التشفير بالمفتاح الغير متماثل Asymmetric Key Encryption

تعرف عملية التشفير التي تستخدم مفاتيح مختلفة لتشفير وفك تشفير المعلومات بإسم التشفير بالمفتاح الغير المتماثل، كان اخترعه للوقوف عن الحاجة إلى مفتاح سري مشترك بين الأشخاص.

على الرغم من اختلاف المفاتيح إلا أنها مرتبطة رياضياً ببعضها، وبالتالي فإن استرجاع النص الغير المشفر من خلال فك تشفير النص المشفر أمر ممكن.

أمثلة على ذلك:

1. RSA - Ron Rivest, Adi Shamir, and Len Adleman.

2. ElGamal.

**السمات البارزة للتشفير بالمفتاح الغير المتماثل:**

o يحتاج كل شخص إلى الحصول على زوج من المفاتيح المختلفة (مفتاح خاص Private Key ومفتاح عام Public Key)، حيث ترتبط هذه المفاتيح ببعضها رياضيا، فعند استخدام أحد المفاتيح للتشفير يمكن للآخر فك تشفير النص المشفر مرة أخرى إلى النص الأصلي.

o يتطلب وضع المفتاح العام Public Key في مستودع عام Public Repository وبالتالي يسمى نظام التشفير هذا أيضًا تشفير المفتاح العام Public Key Encryption.

o على الرغم من أن المفاتيح العامة والخاصة مرتبطة رياضيا، فإنه ليس من الممكن الحصول على واحد بمعلومية الآخر.

o عندما يحتاج Host1 إلى إرسال البيانات إلى Host2، فإنه يحصل على المفتاح العام لـ Host2 من المستودع، ثم يقوم بتشفير البيانات ونقلها، ومنها يستخدم Host2 المفتاح الخاص به للحصول النص العادي.

o طول المفاتيح (عدد Bits) في هذا التشفير كبير، وبالتالي فإن عملية فك التشفير هي أبطأ من تشفير المفتاح المتماثل، لذا فإن الطاقة المطلوبة لتشغيل الخوارزمية الغير المتماثلة تكون أعلى.

o أنظمة التشفير المتماثلة هي مفهوم طبيعي يمكن فهمه، ولكن في المقابل يصعب فهم أنظمة التشفير الغير متماثلة لإحتوائها على مفاهيم رياضية معقدة.

**عوائق التشفير بالمفتاح الغير متماثل:**

o يحتاج المستخدم إلى الوثوق بأن المفتاح العام الذي يستخدمه في التواصل مع شخص ما هو حقًا المفتاح العام لذلك الشخص ولم يتم خداعه من قبل طرف ثالث ضار.

o يتم تحقيق ذلك عادةً من خلال Public Key Infrastructure PKI تتألف من طرف ثالث موثوق به، حيث يقوم الطرف الثالث بإدارة وتحقيق صحة المفاتيح العامة بشكل آمن، عندما يُطلب من الطرف الثالث توفير المفتاح العام لأي شخص متصل X، يكون موثوقًا به لتوفير المفتاح العام الصحيح.

o عادة ما يتم تضمين المفاتيح العامة التي تم التحقق منها شهادة موقعة رقميا Digital Signature Certificate من قبل جهة خارجية موثوق مفادها أنها تشهد أن مفتاح عام معين ينتمي إلى شخص أو كيان معين فقط.

**معرفة أنواع التشفير الغير متماثل:**

يتم استخدام زوج من المفاتيح لتشفير المعلومات وفك تشفيرها ويُستخدم مفتاح عام للتشفير ويستخدم مفتاح خاص لفك التشفير والمفتاح العام والمفتاح الخاص مختلفان وحتى إذا كان المفتاح العمومي معروفًا للجميع فإن المتلقي المقصود يمكنه فقط فك تشفيره لأنه وحده لأنه الوحيد الذي يعرف المفتاح الخاص.

المكتبة المستخدمة :

Cryptography

الدالة المستخدمة :

Fernet Encryption

يضمن Fernet أن الرسالة المشفرة باستخدامه لا يمكن معالجتها أو قراءتها بدون المفتاح. Fernet هو تطبيق لتشفير متماثل (يُعرف أيضًا باسم "المفتاح السري"). لدى Fernet أيضًا دعم لتنفيذ تناوب المفاتيح عبر MultiFernet.

الاهداف المستقبلية :

١-كان Fernet أكثر منطقية قبل ظهور GCM ، حيث أن التنفيذ الصحيح لـ CBC + HMAC بنفسك أمر صعب ، ويتطلب وضع CBC حشو كتل من 16 بايت.

لا يزال آمنًا ولكني لا أوصي به للأنظمة الجديدة لأن AES256-GCM يجمع بين التشفير والمصادقة في نفس البروتوكول القياسي ، والذي يمكن تشفيره / فك تشفيره بواسطة المتصفحات (Javascript crypto API) وجميع مكتبات وأدوات التشفير الأخرى ، وليس فقط وحدة تشفير بايثون. يعد وضع GCM أيضًا أسرع كثيرًا ، حيث يصل إلى عدة غيغابايت في الثانية باستخدام AES-NI.

٢-استخدام التشفير الغير المتماثل لقوة التشفير وحصول الطرفين على مفتاحين للتشفير وفك التشفير

المصادر :

1-https://www.geeksforgeeks.org/fernet-symmetric-encryption-using-cryptography-module-in-python/amp/

2- <https://cryptography.io/en/latest/fernet/>



