Encryption Inrtoduction

Cryptography

- دا علم التشفير او علم ممارسة تأمين البيانات والمعلومات عن طريق اني بحولها لشكل غير مفهوم واتأكد اني محدش يقدر يفك التشفير دا غير الاشخاص اللي انا محددهم

  شويه مفاهيم كدا ليها علاقه بالcryptography

- **Plaintext (النص الصريح):** البيانات الأصلية التي نريد تشفيرها
- **Ciphertext (النص المشفر):** البيانات بعد تحويلها إلى شكل غير مفهوم
- **Encryption (التشفير):** عملية تحويل النص الصريح إلى نص مشفر باستخدام خوارزمية ومفتاح
- **Decryption (فك التشفير):** إعادة النص المشفر إلى حالته الأصلية باستخدام مفتاح مناسب
- **Key (المفتاح):** قيمة سرية تُستخدم في عملية التشفير وفك التشفير

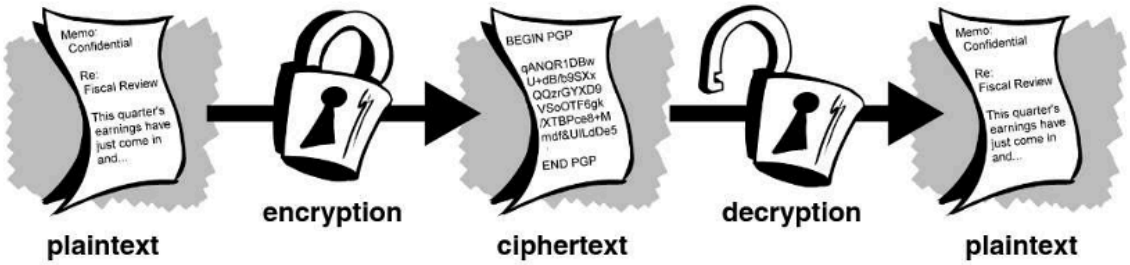
  انواع ال cryptography

1. Encryption
2. Hashing
3. Encoding

Encryption

- الencryption ده هو نظام تشفير بستخدم فيه مفتاح للتشفير ولفك التشفير
- يعني لو ببعت حاجه لحد من غير تشفير وهبعتها كا نص عادي كدا (plaintext) ممكن الهاكر يتجسس علي ال traffic ويعرف ايه محتوي الرساله دي
- الحل هنا ان احنا نشفر الرساله طيب بس لما نشفرها الشخص اللي هيستلمها هيعرف يفك التشفير ازاي؟

- هنا اقولك محنا هنشفر بمفتاح وهنبعت الحاجه متشفره ومعاها المفتاح عشان يفك الشخص يفك التشفير



Encryption Types

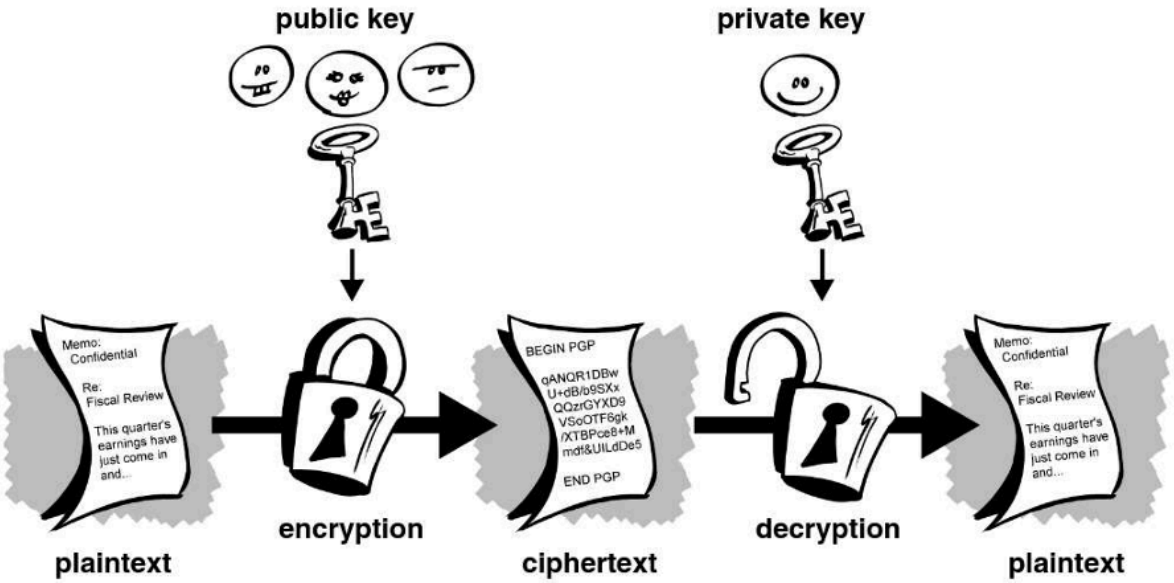
Symmetric Key

- اول حاجه النوع ده انت بتستخدم فيه نفس المفتاح ف التشفير وفي فك التشفير برضو
- طيب احنا اصلا بنشفر الرساله ليه؟ عشان الهاكر ميعرفش ايه اللي بيتبعت ده
- طيب تخيل معايا الهاكر بيتجسس عليك وانت بتبعت رساله متشفره لصاحبك وبتستخدم Symmetric Key الهاكر هنا هيلاقي الرساله متشفره فعلا بس هيلاقي معاها المفتاح هيروح فاكك التشفير ولا كأنك عملت حاجه
- طب ايه الحل؟ الحل هنا بيكون فالنوع التاني

Asymmetric Key

- هنا انا بستخدم مفتاح للتشفير (Public Key) ومفتاح تاني لفك التشفير (Private Key)
- خلي بالك اني المفتاحين مرتبطين ببعض يعني مينفعش تجبلي اي key وتقولي هفك التشفير مينفعش لازم نفس ال key اللي اتعمله generate مع ال public عشان هو بيعملك الاتنين مع بعض وهقولك تعمل كده ازاي
- تخيل معايا بقي كدا انت شفرت الرساله بالpublic key وبعتها لصحبك ومعاها الprivate key والهاكر بيتجسس عليكو هيلاقي الرساله متشفره بس معاها الprivate key اللي بيفك بيه التشفير برضو هيجي واحد يقولي ياعم انت بتهزر احنا محلياش الموضوع برضو هقولك فكر شويه كدا ف الحل ولو موصلتش لحل بص النقطه اللي بعد دي
- احنا هنا هنخلي اللي هيستلم الرساله هو اللي هيgenerate المفاتيح وبعد كدا هيبعت الpublic key للشخص اللي هيبعتلو الحاجه يقولو خد شفر الرساله بالمفتاح البابليك هيجي واحد ناصح يقولي الهاكر وهو بيتجسس عليك هيقدر ياخد ال public key اقولك ياغبي بص كدا لأول نقطه خالص احنا بنستخدم ال public فالتشفير بس فا هو لما يبقي معاه ال Public عادي كدا كدا مش هيعرف يعمل بيه حاجه المهم بعد كدا الراسل هيشفر الرساله بالpublic وهيبعت للشخص التاني اللي هو عمل generate

للمفاتيح اصلا ومعاه الprivate key يروح فاكك التشفير بالprivate بس كدا سهله اهي



- احنا كا هاكرز الاهم بالنسبالنا اهم حاجه نحصل عليها ال private مش ال public لأني الprivate هو اللي بيفك التشفير
- تعالي اقولك بقي ازاي تعمل مفتاحين

`ssh-keygen -t rsa`

```
┌──(root💀lulz-GlideFeed)-[~]
└─# ssh-keygen -t rsa

Generating public/private rsa key pair.
Enter file in which to save the key (/sec/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /sec/root/.ssh/id_rsa
Your public key has been saved in /sec/root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:UvgUb/MAZVqtRbv99qwTMzrCpg4/0gomRGyRQ4TNCe8 root@lulz-GlideFeed
The key's randomart image is:
+---[RSA 3072]----+
|.B+o     o.+o.   |
|.o*.    . B  o.  |
|  =.   . + =o.   |
| +      + ..+ o  |
|  E    . S   o .  |
| .       .      +. |
|  . o .. .    . +o|
|   o ..oo + o .o.|
|      .+++ . ..oo|
+----[SHA256]-----+
```

- هنا بيحددلي المسار ده `sec/root/.ssh/id_rsa/` بيقولك انا هحفظ الفايل اللي هيكون فيه المفتاح فالمسار ده لو دوست enter تمام هيعملك فيه طب لو عاوز تغيرو تكتب المسار اللي انت عاوزه عادي بس كدا

Hashing

- الهاش عباره عن تشفير للحاجه بفورمات معين كده
- مبدأيا فال encryption كنا بنشفر ونفك بمفاتيح والدنيا جميله يعني
- فالhash بقي مبيتفكش هو بيتخمن بس

Hash Types

1. md4
2. md5 (32 bits)
3. sha1 (40 bits)
4. sha256 (64 bits)
5. sha512 (128 bits)
6. bycrypt

- طبعا دي اشهر الانواع انما الهاش فيه انواع كتير جدا
- علي فكره الفيس بيستخدم نوع ال bycrypt فالتشفير
- بس ثواني ياعم انت قولتلي انه مبيتفكش دا بيتخمن ازاي يعني؟
- انا مثلا معايا هاش زي ده

`3dd29b9d75e470682695d3ca7ba2aa6c0536aced`

هفكه ازاي؟ هجيب جدول فيه مليارات الكلمات ومعاها ال hash بتاع كل كلمه وهبدأ اقارن الهاش بالهاش لحد ما اوصل للكلمه اللي انا عاوزها

- حد هيجي يقولي انت عبيط؟ انا هقعد اعمل كدا ف مليار كلمه؟ هقولك لأ في ادوات بتعملك كل الكلام ده او مواقع زي Hashcat او John&Ripper ومواقع زي CrackStation.net

ali	b42a6d93d796915222f6ffb2ffdd6137d93c1cdb
12345@11	ff7bf06a610599df34afa8c92904d18f7595845d
123456789	f7c3bc1d808e04732adf679965ccc34ca7ae3441
01201331839	aa9ac46ce6321eabd4ad6f2120e8e201e1a98d5c
admin	fd0db110793105a640db0b3e4f73e6312b0ba9a5
kali123	4c0394bc580826e067765fbf618d2229010b130c
hossam	3dd29b9d75e470682695d3ca7ba2aa6c0536aced

- علي فكره معظم ال databases او كلهم تقريبا بيستخدمو ال hash هتقولي ازاي؟ هقولك انا
- تخيل معايا انت بتعمل اكونت علي الفيس وعملتو حطيت باسورد مثلا `mohamed123` انت متخيل اني الباسورد بيتخزن ف الdatabase كده؟ تبقي اهبل لأنه الفيس او كل المواقع تقريبا بيحولو الباسورد لهاش ويخزنوه فالداتا بيز علي شكل هاش
- طيب تمام تخيل بقي انت رايح تعمل login وبتحط الباسورد بتاعك انت عارف ايه اللي بيحصل؟ بيحول الباسورد اللي انت دخلته ده (سواء كان صح او غلط) لهاش ويروح عالداتا بيز ويقارن الهاش ده بهاش الباسورد بتاعك اللي متخزن فالداتا بيز لو صح اوكي ادخل لو غلط يقولك الباس غلط

Encoding

- فال encoding انا بس بغير شكل الكلام
- تخيل معايا انت لو رايح لصحبك هتلبس ايه؟ هتلبس بنطلون وتيشرت مثلا او ترينج طب لو رايح مؤتمر هتلبس بدله هو انا نفس الشخص فالمرتين لما روحت ولما روحت المؤتمر بس الاختلاف كان فالشكل او التنسيق
- بالظبط ده الEncoding انا بس بغير شكل الكلام

Encoding Types

`< this is testing >`

- Url Encoding: `%3Cthis%20is%20testing%3E` => بيستخدم فالروابط
- HTML Encoding: `<` `this is testing` `>` => بيستخدم عشان اشفر حاجه ف كود الhtml
- Base64 Enconding: `PHRoaXMgaXMgdGVzdGluZyA+IA==` => بيستخدم فالتشفير في عمليات نقل الداتا اللي حجمها كبير