Thibault GARCIA Mathys DOMERGUE

TP1 Eléments de crypto

1. Focntion de hachage

1.1 Calcul d'un condensé à l'aide de MD5

1. Le hash obtenue est :

```
e39a8d185112324a5416b897741588bb
```

2. On a 2^{128} condensés différents possibles

3. MD5 n'est pas sans limite et peut avoir des erreurs avec le même hash.

1.2 Vérification des propriétés du condensé

4.
```
e39a8d185112324a5416b897741588bb
```

   On peut voir que le hash ne changer, c'est normal parce que c'est le contenue qui est hasher et non le nom.

5.
```
 60b725f10c9c85c70d97880dfe8191b3
```

   On constate que le hash a changé. C'est normal car le contenu du fichier a changé.

6. Comme le contenu d'un fichier executable existe alors on peut le hasher.

2 Clefs de chiffrement

2.1 Génération des clefs

7. Lors de l'execution de la commande, on voit :

```
/home/lucky/.gnupg/pubring.kbx
------------------------------
pub   rsa3072 2024-04-05 [SC] [expires: 2026-04-05]
      D3158566827AB09B4FA97D6800D1279E54083642
uid           [ultimate] test1 <mathys.domergue@etu.umontpellier.fr>
sub   rsa3072 2024-04-05 [E] [expires: 2026-04-05]
```

le champ « pub » correspond à la partie publique.
le champ « sub » correspond à une sous-clé.
le champ « uid » correspond à une adresse email et un nom.

8. La commande est :

```
gpg --list-secret-keys
         ou
gpg -K
```

Les deux clés ont le même hash.

2.2 Diffusion de la clef publique

9. Voici le contenue

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGYQBFcBDADNabD3Y/Rc00npJ7DxzaeSl0sNnovBkKuPg8SZApWz3H1Xy110
Zfbx1wmuhtS7zUQ6GV1o5Dh55IJre0+1bmlJttyyy0SnST0rRgyGQ2gIvkROyQ9Z
RGN0uJHvcA0B5JBgo2Mcl6FxsM1+M+fF8HAfgVdVl2OVzCIVu59klGFTtS79jyxk
ZDfRYEdfg7EdXeqfS67t5nb0uKN47teyxkGyGYw2IStEtwKjng2Be6D3FIAJPXxG
clZUtcSPA7BfzE09t1hw1N1m5istdn9dTnoUAhA8B6R1JZCQPFHPEmBC0MXLxfys
yoRMhTYhMQqQU38cJDmxkrXieShg4N0aSYDtsfolLsu8sQ1D7AD1/vur9L6/UfFc
D5sX28KfhViB9vV5L1Bgvs5o6CvvvbEEoNzDSPkOaEj+/R5MHkArGYDplk03IIHH
YDg//5wJ4tiQyjsh+HF7WudUzzIaq4rXlWAHrinjItZZILM7+I6ajclF3qStj8kG
Mjd9pzoGJKLxuB8AEQEAAbQrdGVzdDEgPG1hdGh5cy5kb21lcmd1ZUBldHUudW1v
bnRwZWxsaWVyLmZyPokB1AQTAQoAPhYhBNMVhWaCerCbT6l9aADRJ55UCDZCBQJm
EARXAhsDBQkDwmcABQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEADRJ55UCDZC
4vQMALh8jII9rsu1lRwgx7WTsbexktZ4fkKjpifxoPNUWatzDX5khNRwn25QJN2U
O1nHdh5VrF+oEWEO+eFoBMmiQR0/3WqexBjflZclFDFc6w9wr6lRIJQT1WoMEA0D
QTMHGiJN5MGy1oWc3PsCEBj0f3EJL6cdhSS5ORp1Y7KQr5PenkTUKpylTHBfXRDD
xsayBXshrndBcgGbhbHmJ+XI4Hi2K1Hic7es3zLStXVIebE7bJy7j5BOEgSo9Koi
xfXF/w2qXMFXLtG9ATkkDgMkQjf3le0dvk4WRXukOL2N7FwIX+owGNLNvSJE5PxP
2bPFWyH+/4vlnFKt3wNkv23ydqkc9htDz7G48JvGC3747beiw66GOtdJOIkFBjd6
N6o2ypWCdGcVdKbIdNchUEKOIc7lpbM40uk/iegFhnncVUMeh4lzh6p3tOjoOLLQ
GwHlWIwyVu7N0tbu1Knf/Q0ENL+4AU4IGynlpp9FudpkVZ2UgoVAeBR5MLWaaB98
qQ2RU7kBjQRmEARXAQwAyOkPrejAmtqapg4DhF+IBGKBbIF8h00+k4qJCikDv15u
fGUTRHYO/vO1wxhIKJH9bvTw21ew0zUWnJ2jkjAGg0DVQvnWqcAlfeFJAvGgxPBq
psw5tR/Ns9VhtpESHcrKFKJkFzNAlMLFJjv9prcH+Ie+rBcR/GTS3Wb/VBx5WpY3
WjJPSxdpHBc6t/UX8uNhsTGr/JJokvmcj7xtf1TAanYv28NE3nX/cZPuXVd70gVb
YbMM5rxcemaI+mDFQ4UsiJerobsi6dETIjLaNpQ7V0dDVDw0qm0oyyCWY7fmTLuc
pdIgkGL8j/YEyhuTN6LFdYkwZN2kVoqgmnHsJDOHNLbfr1v3mcmewogjE+W4VAXg
sENLNdo4DvJkCn5lN01dwNxRsPR64VlwMRxAJSnyr/nLElVguS7MmbJBcnQobOMl
4jcpKy4Fd2boLKSfJxi9ubYisUJAR2iaKO3hHbxr5ce5e8tWpc+n2P+DXYdtW9gy
u2GhKjSbmz3kU6DdfKSXABEBAAGJAbwEGAEKACYWIQTTFYVmgnqwm0+pfWgA0See
VAg2QgUCZhAEVwIbDAUJA8JnAAAKCRAA0SeeVAg2Qq8AC/wNrbZjpdK7QcOh24EL
eLfzXqQTRJSMieVSDDR0CjMN2tTk9xe9nEbfSYrTdW+o9bB9u6reyklJP/0r0zft
HOXbS9picGPJEnOkWHYNEnM4MumXZA7PYYR4RA2X9C6UET1SSCJ6ClPTWFiP0BXQ
NqbUziTLBHrbfvWOAbBDVM8jMEYQYhgTkJcNsNsMHIR0jE6oMyDcLsUjD76t/RI/
```

```
b0s2Hc2cQx2nBCVHhDht5lYQCkZGkBGDC/uaR96YXpBnMQiONdYYPAaF884K2HTK
v09q8WI6Sc6o+Q/MIo8Nh//WZJhWdqZQiPfpBn25AGvrm2NnsdF9RW8NY+VFEOz/
q/BTe7yo9UzxFN4tqolMsH6Kk6iXagTQ6yQMshXnzL5EnDRA89PeuwFOoYUV8/bs
UYDD9oMEBuMOCaE2kLcR5kogY9NY59Q0k1i8fNivKTazcPaiuLMF6zYvtu+HXFAr
FPtLlfSWrj2ZuJNSHBHV82Sz0JWrj5P8zu9Wm6XpjSXyYi0=
=o585
-----END PGP PUBLIC KEY BLOCK-----
```

10.
```
gpg --export-secret-keys --armor > testsec.key
```

3 Chiffrage d’un fichier

11. Pour pouvoir envoyer un message, il faut crypter avec sa clé publique.

12. Voici le résultat:

```
/home/lucky/.gnupg/pubring.kbx
------------------------------
pub   rsa3072 2024-04-05 [SC] [expires: 2026-04-05]
     D3158566827AB09B4FA97D6800D1279E54083642
uid           [ultimate] test1 <mathys.domergue@etu.umontpellier.fr>
sub   rsa3072 2024-04-05 [E] [expires: 2026-04-05]

pub   rsa3072 2024-04-05 [SC] [expires: 2026-04-05]
     953C70C9A87D0D752C8E9914EB3BD79BE624AE5A
uid           [ unknown] Thibault
<thibault.garcia@etu.umontpellier.fr>
sub   rsa3072 2024-04-05 [E] [expires: 2026-04-05]
```

On constate que la clef de Thibault est bien dans mes clefs publiques.

```
gpg --armor --recipient thibault.garcia@etu.umontpellier.fr --encrypt
test.txt
```

Voici le décryptage du fichier:

```
lucky@lucky-the-one:~/Desktop/IUT-cours/R401/TP1$ cat truc.txt
    top secret mathys... j'ai encrypté mon fichier !
```

13. Le fichier est bien identique.

4 Signature numérique

4.1 Signature d'un fichier

15. Voici le résultat:

```
gpg: encrypted with 3072-bit RSA key, ID C7153A85672F42FC, created
2024-04-05
  "test1 <mathys.domergue@etu.umontpellier.fr>"
mathys, j'ai encrypté mon fochoer ET ne l'ai figné !!!
gpg: Signature made ven. 05 avril 2024 17:12:10 CEST
gpg:                using RSA key
953C70C9A87D0D752C8E9914EB3BD79BE624AE5A
gpg:                issuer "thibault.garcia@etu.umontpellier.fr"
gpg: Good signature from "Thibault
<thibault.garcia@etu.umontpellier.fr>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the
owner.
Primary key fingerprint: 953C 70C9 A87D 0D75 2C8E  9914 EB3B D79B E624
AE5A
```

4.2 Signature d’une clef publique

17. Voici le résultat:

```
lucky@lucky-the-one:~/Desktop/IUT-cours/R401/TP1$ gpg --sign-key
953C70C9A87D0D752C8E9914EB3BD79BE624AE5A

pub  rsa3072/EB3BD79BE624AE5A
     created: 2024-04-05  expires: 2026-04-05  usage: SC
     trust: unknown       validity: unknown
sub  rsa3072/864EEF76CF4AD13C
     created: 2024-04-05  expires: 2026-04-05  usage: E
[ unknown] (1). Thibault <thibault.garcia@etu.umontpellier.fr>


pub  rsa3072/EB3BD79BE624AE5A
     created: 2024-04-05  expires: 2026-04-05  usage: SC
     trust: unknown       validity: unknown
 Primary key fingerprint: 953C 70C9 A87D 0D75 2C8E  9914 EB3B D79B
E624 AE5A

     Thibault <thibault.garcia@etu.umontpellier.fr>

This key is due to expire on 2026-04-05.
Are you sure that you want to sign this key with your
key "test1 <mathys.domergue@etu.umontpellier.fr>" (00D1279E54083642)

Really sign? (y/N) y
```

5 Utilisation d’un certificat