

Réseaux ?

Cryptographie

Gaétan RICHARD

6 juillet 2020

DiU EIL

Université de Caen Normandie



Cryptographie

Cryptologie : science du secret et de la confiance

Cryptographie :

- conception de systèmes cryptographiques
- étude (preuve) de leur sécurité
- amélioration des performances

Cryptanalyse :

- mise en défaut des systèmes cryptographiques
- attaque des problèmes algorithmiques sous-jacents
- observation des “canaux auxiliaires”

Objectifs

- **confidentialité** : garantir que le contenu d'une communication (ou d'un fichier) n'est pas accessible à tout autre personne que le destinataire légitime.
- **authenticité** : s'assurer de l'identité d'une entité donnée ou de l'origine d'une communication (ou d'un fichier).
- **intégrité** : s'assurer que le contenu d'une communication (ou d'un fichier) n'a pas été modifié de façon malveillante.
- **non répudiation** : s'assurer que l'expéditeur/signataire ne peut nier avoir envoyé/signé un message

Objectifs

- **confidentialité** : garantir que le contenu d'une communication (ou d'un fichier) n'est pas accessible à tout autre personne que le destinataire légitime.

↪ *chiffrement*

- **authenticité** : s'assurer de l'identité d'une entité donnée ou de l'origine d'une communication (ou d'un fichier).
- **intégrité** : s'assurer que le contenu d'une communication (ou d'un fichier) n'a pas été modifié de façon malveillante.
- **non répudiation** : s'assurer que l'expéditeur/signataire ne peut nier avoir envoyé/signé un message

Objectifs

- **confidentialité** : garantir que le contenu d'une communication (ou d'un fichier) n'est pas accessible à tout autre personne que le destinataire légitime.

↪ *chiffrement*

- **authenticité** : s'assurer de l'identité d'une entité donnée ou de l'origine d'une communication (ou d'un fichier).

↪ *identification/signature*

- **intégrité** : s'assurer que le contenu d'une communication (ou d'un fichier) n'a pas été modifié de façon malveillante.

- **non répudiation** : s'assurer que l'expéditeur/signataire ne peut nier avoir envoyé/signé un message

Objectifs

- **confidentialité** : garantir que le contenu d'une communication (ou d'un fichier) n'est pas accessible à tout autre personne que le destinataire légitime.

↪ *chiffrement*

- **authenticité** : s'assurer de l'identité d'une entité donnée ou de l'origine d'une communication (ou d'un fichier).

↪ *identification/signature*

- **intégrité** : s'assurer que le contenu d'une communication (ou d'un fichier) n'a pas été modifié de façon malveillante.

↪ *hachage/signature*

- **non répudiation** : s'assurer que l'expéditeur/signataire ne peut nier avoir envoyé/signé un message

Objectifs

- **confidentialité** : garantir que le contenu d'une communication (ou d'un fichier) n'est pas accessible à tout autre personne que le destinataire légitime.

↪ *chiffrement*

- **authenticité** : s'assurer de l'identité d'une entité donnée ou de l'origine d'une communication (ou d'un fichier).

↪ *identification/signature*

- **intégrité** : s'assurer que le contenu d'une communication (ou d'un fichier) n'a pas été modifié de façon malveillante.

↪ *hachage/signature*

- **non répudiation** : s'assurer que l'expéditeur/signataire ne peut nier avoir envoyé/signé un message

↪ *hachage/signature*

L'âge artisanal

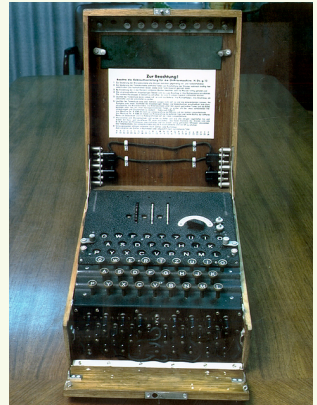
- IRAK XVIème avant JC : potier → recette secrète sur une tablette d'argile : suppression des consonnes et modification de l'orthographe
- -600 : Nabuchodonosor (Babylone) tatouage sur le cuir chevelu



- VIIème avant JC : scytale
- Ier avant JC : chiffrement de César
- transposition, substitution (mono/poly-alphabétique, homophonique,...) - Vigénère,

L'âge technique

- machine à chiffrer (Enigma)
~> automatisatisation
- naissance de l'informatique
~> Turing, Colossus à Bletchley Park
- **Data Encryption Standard**
~> du militaire au civil, prémices de la théorie



L'âge paradoxal

- naissance de la

cryptographie à clé publique

on ne s'échange plus de clé : on la publie !

↪ chaque utilisateur possède un **couple**

$$(sk, pk)$$

où pk est publique et sk est gardée secrète

$$sk \mathcal{R} pk$$

il est “*difficile*” de retrouver sk à partir de pk .



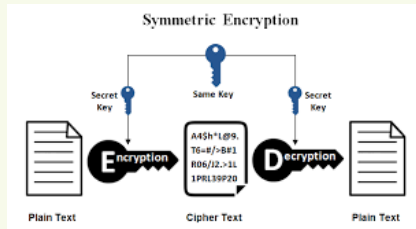
New Directions in Cryptography. W. Diffie and M. E. Hellman,
IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, pp 644–654.

Cryptographie

Chiffrement symétrique

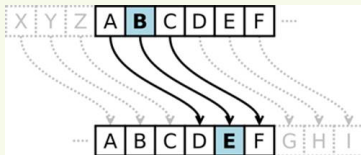
Principe du chiffrement symétrique

- Un secret commun (clé secrète) ;
- Utilisé pour le chiffrement et le déchiffrement.



Chiffre de César (vers 50 av JC)

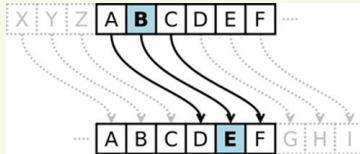
Principe : on décale les lettres d'une valeur fixée.



Clair Un enfant assez sage
Chiffré

Chiffre de César (vers 50 av JC)

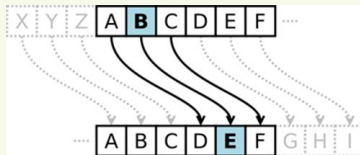
Principe : on décale les lettres d'une valeur fixée.



Clair	Un enfant assez sage
Chiffré	d

Chiffre de César (vers 50 av JC)

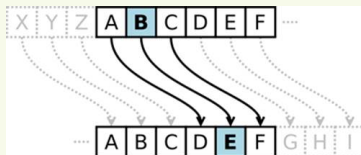
Principe : on décale les lettres d'une valeur fixée.



Clair	Un enfant assez sage
Chiffré	Xq hqidqw dvvhc vdjh

Chiffre de César (vers 50 av JC)

Principe : on décale les lettres d'une valeur fixée.



Clair Un enfant assez sage

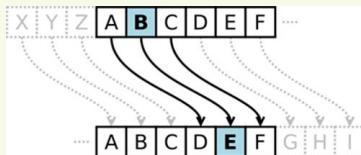
Chiffré Xq hqidqw dvvhc vdjh

Chiffré Rx sdv!

Clair

Chiffre de César (vers 50 av JC)

Principe : on décale les lettres d'une valeur fixée.



Clair	Un enfant assez sage
Chiffré	Xq hqidqw dvvhc vdjh

Chiffré	Rx sdv!
Clair	Ou pas!

Décrypter le chiffre de César

Od Iudqfh hvw xqh Uhsxeoltxh lqglylvleoh, odltxh,
ghprfudwltxh hw vrfldoh. Hooh dvvxuh o'hjdolwh ghydqw od
orl gh wrxv ohv flwrbhqv vdqv glvwlqfwlrq g'ruljqlh, gh
udfh rx gh uholjlrq. Hooh uhvshfwh wrxwhv ohv furbdqfhv.
Vrq rujdqlvdwlrq hvw ghfhqwudolvhh.

Décrypter le chiffre de César

Od Iudqfh hvw xqh Uhsxeoltxh lqglylvleoh, odltxh,
ghprfudwltxh hw vrfldoh. HooH dvvxuh o'hjdolwh ghydqw od
orl gh wrxv ohv flwrbbhqv vdqv glvwlqfwlrq g'ruljllqh, gh
udfh rx gh uholjllrq. HooH uhvshfwh wrxwhv ohv furbdqfhv.
Vrq rujdqlvdwlrq hvw ghfhqwudolvhh.

Décrypter le chiffre de César

La France est une République indivisible, laïque,
démocratique et sociale. Elle assure l'égalité devant la
loi de tous les citoyens sans distinction d'origine, de
race ou de religion. Elle respecte toutes les croyances.
Son organisation est décentralisée.

Chiffre de Vigenère (1586)

Principe : On effectue plusieurs chiffre de César (basé sur un mot).

clair : WIKIPEDIA L'ENCYCLOPEDIE LIBRE

clef : CLEFCLEFC L EFCLEFCLEFCL EFCLE

chiffré : YTONRPHNC W'ISEJGQQAIKP PNDCI

Site Web : <https://www.dcode.fr/chiffre-vigenere>

Création :

- Concours organisés par le NIST ;
- concours public et visible ;
- Algorithmes connus et distribués.

Quelques chiffrements :

- **DES** (1970) *deprecated* ;
- **3-DES** (1998) *plus vraiment au jour* ;
- **AES** (1998) ([lien vidéo](#))
- **Autres** : Blowfish, Serpent, Twofish.

Cryptographie

Fonction de hashage

Principe : Réduire un gros document à une petite empreinte de façon à ce que :

- calculer l'empreinte soit facile ;
- construire un document avec une empreinte donnée soit difficile ;
- construire deux documents avec la même empreinte soit difficile ;

L'empreinte *caractérise* le document.

Des exemples :

- MD4 MD5
- SHA0 SHA-1
- RIPEMD
- SHA-256
- SHA-3
- Whirlpool
- AES

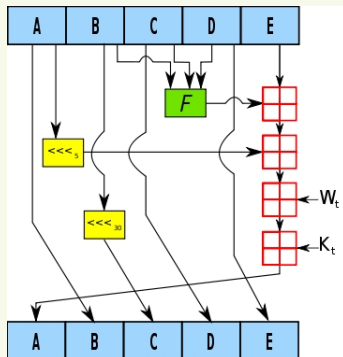
Fonctions de hachage

Des exemples :

- MD4  MD5 
- SHA0  SHA-1 presque 
- RIPEMD 
- SHA-256
- SHA-3
- Whirlpool
- AES

Fonctions de hachage

Une itération de SHA1



Stockage des mots de passe

Bonne pratique : On stocke l'empreinte du mot de passe avec une graine spécifique (*salt and hash*).

Résultat : Le site ne possède pas le mot de passe, juste un moyen de vérifier que la personne donnant le mot de passe le connaît.

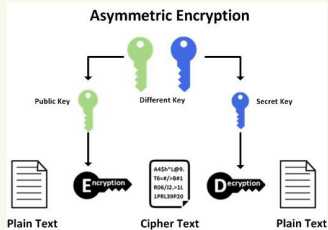
Conséquence : aucun site web raisonnable ne doit être capable de vous renvoyer un mot de passe.

Cryptographie

Chiffrement asymétrique

Principe

- Un couple de clés (clé publique / clé privée) ;
- ce qui est chiffré avec la clé publique se déchiffre avec la clé privée ;
- et inversement (signature).



- La paire de clés :
 - p et q sont deux grands premiers (1024 bits)
 - $N = pq$ (2048 bits)
 - e et d sont deux entiers premiers à $\varphi(N) = (p-1)(q-1)$ tels que

$$ed \equiv 1 \pmod{\varphi(N)}$$

- Finalement
 - (N, e) est la clé publique (pk)
 - (d, p, q) est la clé secrète (sk)

- La paire de clés :
 - p et q sont deux grands premiers (1024 bits)
 - $N = pq$ (2048 bits)
 - e et d sont deux entiers premiers à $\varphi(N) = (p-1)(q-1)$ tels que

$$ed \equiv 1 \pmod{\varphi(N)}$$

- Finalement
 - (N, e) est la clé publique (pk)
 - (d, p, q) est la clé secrète (sk)
- Pour chiffrer $m \in \mathbb{Z}/N\mathbb{Z}$:

Protocole RSA

- La paire de clés :
 - p et q sont deux grands premiers (1024 bits)
 - $N = pq$ (2048 bits)
 - e et d sont deux entiers premiers à $\varphi(N) = (p-1)(q-1)$ tels que

$$ed \equiv 1 \pmod{\varphi(N)}$$

- Finalement
 - (N, e) est la clé publique (pk)
 - (d, p, q) est la clé secrète (sk)
- Pour chiffrer $m \in \mathbb{Z}/N\mathbb{Z}$:

$$c \equiv m^e \pmod{N}$$

- Pour déchiffrer $c \in \mathbb{Z}/N\mathbb{Z}$

$$m \equiv c^d \pmod{N}$$

En effet :

$$\begin{aligned} c^d \pmod{N} &\equiv m^{ed} \pmod{N} \\ &\equiv m^{1+k\varphi(N)} \pmod{N} \\ &\equiv m \times (m^{\varphi(N)})^k \pmod{N} \\ &\equiv m \end{aligned}$$

Exemple numérique

Génération des clés :

- $p = 7919, \quad q = 17389$
- $n = pq = 137703491$
- $\varphi(n) = (p - 1)(q - 1) = 137678184$
- $e = 5$ (on a bien $\text{pgcd}(e, \varphi(n)) = 1$)
- $d = e^{-1} \bmod n = 27535637$ (Euclide étendu)

clé publique : (n, e) clé privée : $(d, p, q, \varphi(n))$

Chiffrement d'un message :

- $m = 123456$ (on a bien $\text{pgcd}(m, n) = 1$)
- $c = m^e \bmod n = 36218866$

Déchiffrement d'un message :

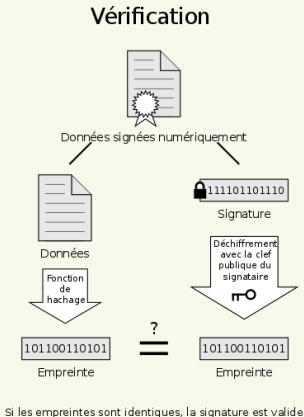
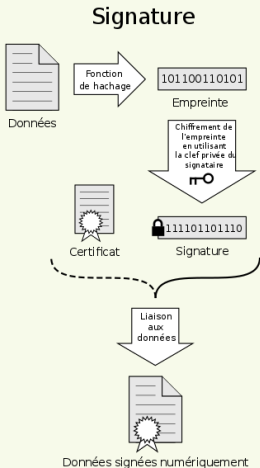
- $m' = c^d \bmod n = 123456$ (on a bien $m' = m$)

Avantages et inconvénients

- Chiffrement à clé publique lent
 - ⇒ Chiffrer des messages courts
 - ⇒ on combine les deux types de cryptographie
- Chiffrement déterministe
 - ⇒ Même message chiffré toujours de la même manière
 - ⇒ On ajoute du prétraitement probabiliste

Signature

Principe : On chiffre avec la clé privée une empreinte du document.



Cryptographie

PKI

Un certificat contient :

- une clé publique
- un nom associé
- une période de validité
- l'adresse (URL) du centre de révocation
- la signature de ce certificat par l'autorité de certification

Structure de X.509 :

- Certificate
 - Version
 - Serial Number
 - Algorithm ID
 - Issuer
 - Validity
 - Not Before
 - Not After
 - Subject
 - Subject Public Key Info
 - Public Key Algorithm
 - Subject Public Key
 - Issuer Unique Identifier (Optional)
 - Subject Unique Identifier (Optional)
 - Extensions (Optional)
- Certificate Signature Algorithm
- Certificate Signature

Apparté : les certificats

Exemple de X.509 :

Certificate:

Data:

Version: 1 (0x0)

Serial Number: 7829 (0x1e95)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,

OU=Certification Services Division,

CN=Thawte Server CA/emailAddress=server-certs@thawte.com

Validity

Not Before: Jul 9 16:04:02 1998 GMT

Not After : Jul 9 16:04:02 1999 GMT

Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,

OU=FreeSoft, CN=www.freesoft.org/emailAddress=baccala@freesoft.org

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:

33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:

66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:

70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:

16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:

c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:

8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:

d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:

e8:35:1c:9e:27:52:7e:41:8f

Exponent: 65537 (0x10001)

Exemple de X.509 (fin) :

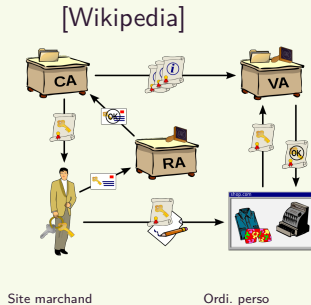
Signature Algorithm: md5WithRSAEncryption

```
93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:
68:9f
```

Infrastructure de gestion de clés

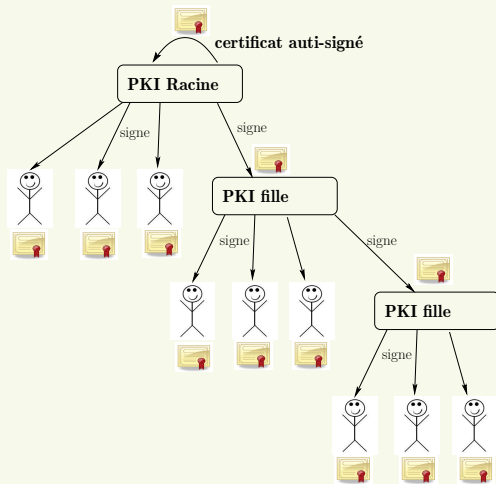
Une infrastructure de gestion de clés publiques (PKI en anglais) est un ensemble de procédures visant à **mettre en place des communications sécurisées à l'aide de certificats**.

- Autorité de certification (CA) : signe les certificats et les listes de révocation (CRL)
- Autorité d'enregistrement (RA) : vérifie l'identité de l'utilisateur final
- Autorité de dépôt/validation (VA) : stocke les certificats et les CRL
- Utilisateur final (EE) : par exemple le webmail Unicaen



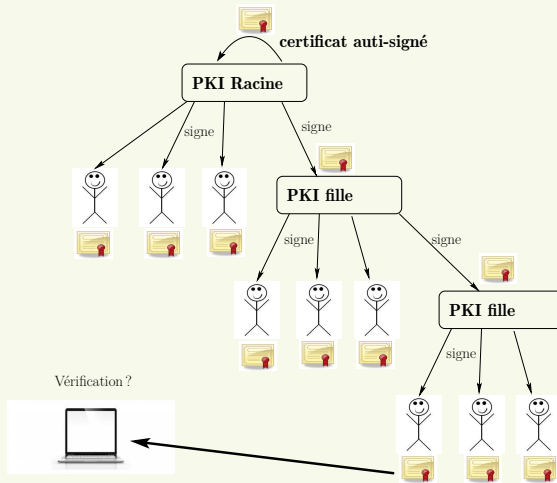
Infrastructure de gestion de clés

Le plus souvent, les PKI ont une structure hiérarchique



Infrastructure de gestion de clés

Le plus souvent, les PKI ont une structure hiérarchique



Cryptographie

Blockchain

Principe technique :

- Une base de donnée **distribuée, transparente et robuste** ;
- Repose sur une chaine d'éléments ;
- Créer un élément est complexe ;
- Le travail est partagé.

Monnaie virtuelle :

- Les blocs enregistrent des opérations ;
- La création de bloc donne droit à un bonus ;
- Des plateformes échangent ces valeurs contre de l'argent.