FORMATIO | RESSOURCE INFORMATIQUE BUREAUTIQUE

INTRODUCTION A LA CRYPTOGRAPHIE

BIEN CHOISIR SON MOTS DE PASSES

ALAIN WAGNER B. GEST.

17 SEPTEMBRE 2020

Introduction a la cryptographie

- La sécurité informatique est assez difficile car il y a moyen d'exploiter les failles d'un système.
- Pour pouvoir exploiter les failles d'un système il faut connaitre comment fonctionne le système.
- Intervient la notion de cryptographie pour être considéré comme la boite à outils pour sécuriser le système.

- Nous allons voir comment utiliser la cryptographie pour envoyer des messages sur Internet.
  - Cryptographie signifie écrire de manière cachée. On pense donc que seul le destinataire est capable de les lires.. En réalité c'est plus compliqué que ça.

Introduction a la cryptographie

Sécurité des communications

1 - Confidentialité

Introduction a la cryptographie

Sécurité des communications

1 - Confidentialité

2 - Authenticité

Introduction a la cryptographie

Sécurité des communications

1 – Confidentialité
2 - Authenticité
3 - Intégrité

A

Prix 12.50$

Prix 1250$

B

X

Introduction a la cryptographie

Fonctionnement

c

A

B

m = Bonjour **c**

E(m) = c = laq9i/a

m = texte en clair
c = message chiffré
E = fonction de chiffrement

D(c) = m

D = Fonction de déchiffrement
m = Bonjour

Introduction a la cryptographie

Fonction de chiffrement et de déchiffrement

Chiffrement de César 

Processus extrêmement simple qui constitue à décalé les lettres d'un certain nombre de fois

Exemple:
A, B, C, D et si je prends un décalage de 3 j'obtiens pour la lettre A

A (+3) – > D

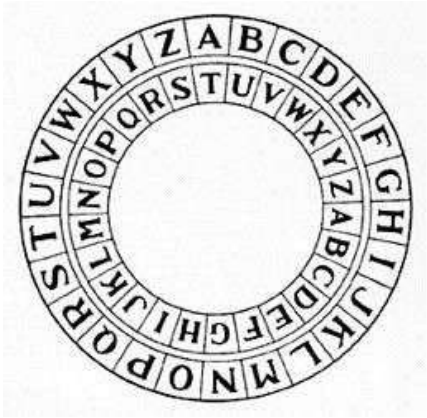
C'est également un système cyclique car si on prend Y la suite des lettres recommence au début et la chaine devient Y, Z, A, B

Exemple:
Y, Z ,A, B et si je prends un décalage de 3 j'obtiens pour la lettre Y

Y (+3) --> B

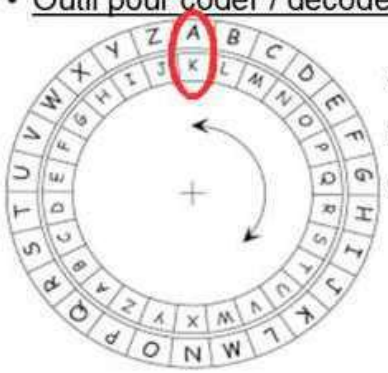
Introduction a la cryptographie

Introduction a la cryptographie



La roue CESAR

- Outil pour coder / décoder le code CESAR :



Sur cette image la clef est **A/K**

Donc le A devient K etc.

C E S A R devient **M O C K B**

Introduction a la cryptographie

Le problème est que comme nous n'avons que 26 lettres dans l'alphabet nous avons donc que 25 possibilités de décaler les lettres du mot envoyé.

C'est donc assez simple pour retrouver la clé de chiffrement

Si vous connaissez la langue qui est utilisée, on peut voir la fréquence d'apparition des lettres.

qj hmnkkwjrjsy ij hj rtz xfz xjwaz

Si nous assumons que la langue est française par exemple, la lettre **E** est la plus fréquente et si on voit dans le message chiffré beaucoup de **J** par exemple on peut présumer que **J** = **E** soit un décalage de 5

I suffit donc de reculer toutes les lettres du message codé de 5 lettres pour retrouver le message original soit: **le chiffrement de ce mot est requit**

Nous constatons qu'il est facile de trouver la clé de codage. Il faut donc trouver une autre solution qui nous permettra d'utiliser non pas une clé mais plusieurs clé et par conséquent plus de possibilité

Introduction a la cryptographie

Chiffrement de Vigenère

Blaise de Vigenère (1523-1596) était un diplomate, alchimiste et cryptographe français.

C'est d'abord son métier de diplomate qui le poussa à s'intéresser à la cryptomanie.

Il améliora le chiffre de César en utilisant des clés différentes suivant la position des lettres

Soit L'alphabet écrit normalement: A, B, C…

A chaque lettre, on associe un entier entre 0 et 25 selon l'ordre alphabétique: c'est son rang.

Cela donne le tableau suivant:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Introduction a la cryptographie

Pour un texte comme LUMIERE, on choisit alors un mot pour clé, par exemple le mot LOIRE

La lettre L est la 12ème lettre de l'alphabet et celle de rang 11: on décale alors la 1ère lettre du message de 11 lettres vers la droite.
La lettre O est la 15ème lettre de l'alphabet et celle de rang 14: on décale alors la 2ème lettre du message de 14 lettres vers la droite.
On continue ainsi cycliquement, avec les décalages des autres lettres de LOIRE: 8 pour I, 17 pour R et 4 pour E.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Exemple de chiffrement:

Message :	L	U	M	I	E	R	E
Clé :	L	O	I	R	E	L	O
Message chiffré :	W	I	U	Z	I	C	S

Codage avec table

Introduction a la cryptographie

Sa force: un chiffrement polyaphabétique

Dans cet exemple, on constate que la lettre E est chiffrée différemment suivant sa position dans le texte LUMIERE avec la clé LOIRE (une première fois en I , puis en S), et c'est exactement le but recherché: faire en sorte qu'une attaque par analyse par fréquence ne fonctionne plus, ce qui constitue un progrès par rapport au chiffre de César.

Le chiffrement de Vigenère est un chiffrement polyaphabétique par simple substitution, par opposition au chiffrement monoalphabétique de César.

Message :	L	U	M	I	**E**	R	**E**
Clé :	L	O	I	R	E	L	O
Message chiffré :	W	I	U	Z	**I**	C	**S**

Utilitaire de codage/décodage de Vigenère sur Internet: www.sindark.com/NonBlog/CR/CR.html

Introduction a la cryptographie

Quand on étudie la sécurité informatique on prend comme principe que l'intrus connais tout le mécanisme du système mais il ne connait pas la clé de chiffrement.

Ceci a été énoncé par Kerchoffs qui a stipulé que la sécurité devait dépendre uniquement de la clé et non du système.

Ceci étant dit nous constatons que les systèmes de sécurités ne suivent pas toujours ces principes.

Nous le constatons actuellement dans les sms etc.. Ou la sécurité est absolument défaillante.

Ce que nous avons vu précédemment est une **cryptographie symétrique** car il implique que l'émetteur et le receveur possède la même clé de chiffrement et de déchiffrement.

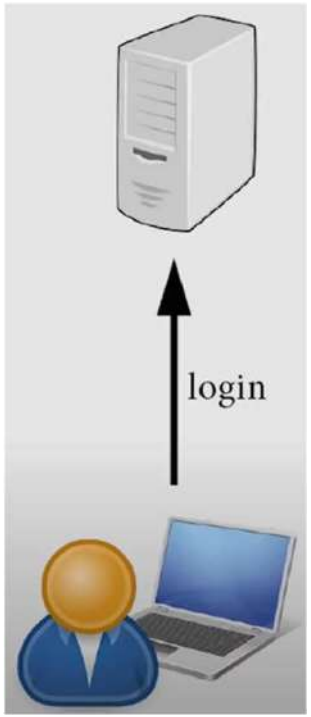
Il existe maintenant une **cryptographie asymétrique** qui demande à l'émetteur d'avoir une clé et au récepteur d'avoir une clé différente.

Fin de la première section

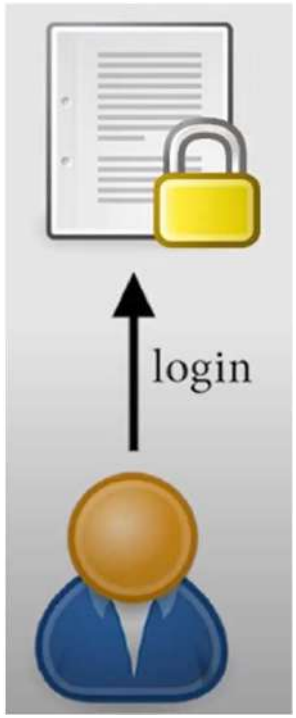
Besoin d’un mot de passe fort

Besoin d’un mot de passe pour:

Ouvrir un ordinateur



Se connecter à un réseau



Ouvrir un fichier protégé

Comment entreposer le mot de passe

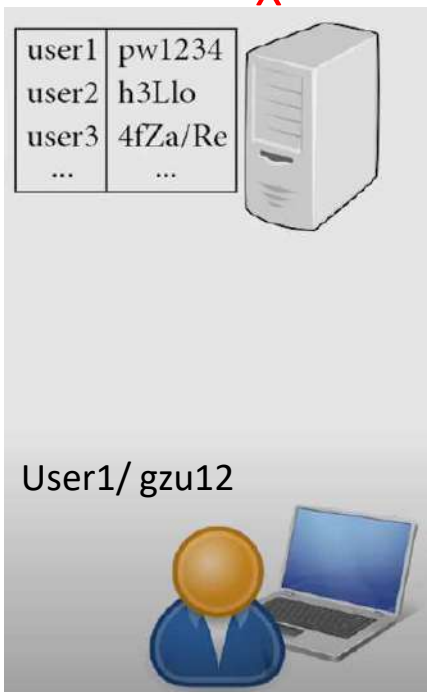
Sur le disque dur

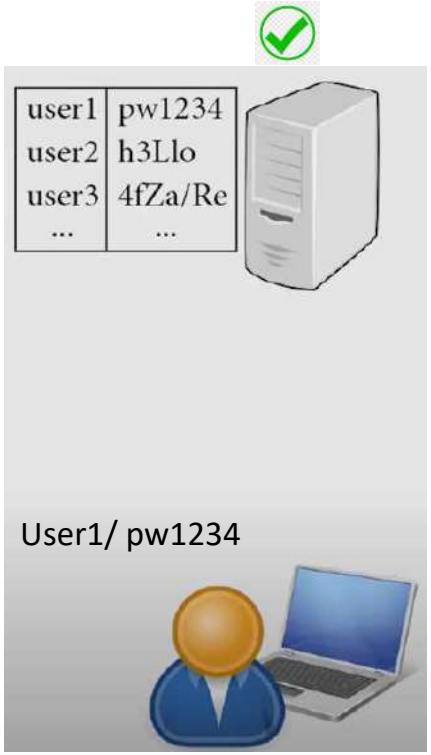
X

Comment entreposer le mot de passe

Sur un serveur

X

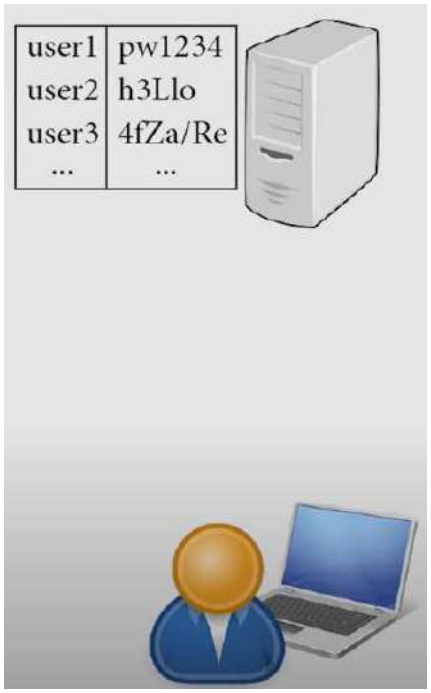




Comment entreposer le mot de passe

Le problème

Vos mots de passes sont compromis



Fonction cryptographiques de hachage

- Fonction qui a un réciproque:

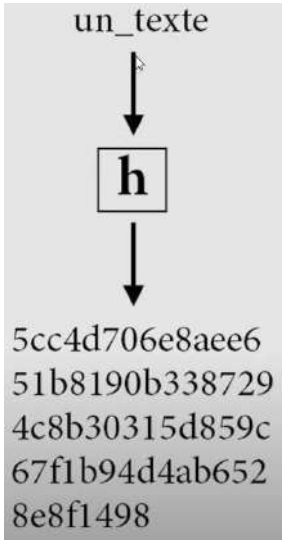
Exemple: si mon chiffre original est 5 et que je le mets au carré **5^2= 25**

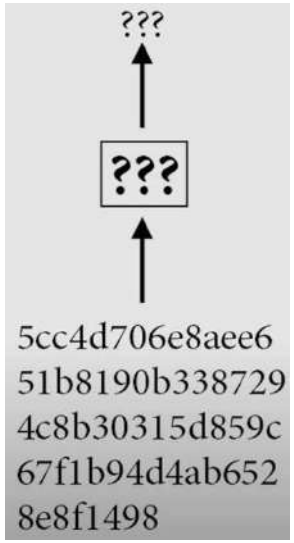
Si je veux retrouver le chiffre initial je n'ai qu'à extraire la rive carrée de 25 et je trouve 5, le chiffre original

Il y a donc une ***fonction réciproque*** qui me permet de revenir en arrière. Dans ce cas la racine carrée.

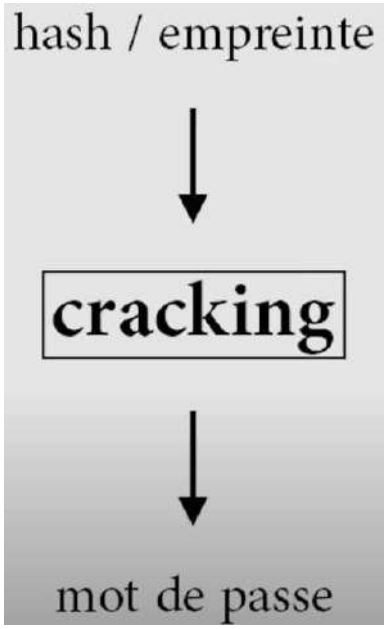
- Fonction qui n'a pas de réciproque:

Utilisation de la méthode de hachage car cette fonction n'a pas de réciproque (utilisée par exemple dans les chaines de blocs) https://emn178.github.io/online-tools/sha256.html





Cracker les mots de passes



- **Méthode de la force brute.**
  - **Essayer toutes les possibilités afin de retrouver le hash équivalent**

5 lettres minuscules = **26^5 = 2 600 000 possibilités**

aaaaa aaaab aaaac ……. zzzzy zzzzz

Si on ne connait pas le nombre de lettres mais on sait que la longueur est au max 5 lettres, on doit essayer toutes les possibilités

$26 + 26^2 + 26^3 + 26^4 + 26^5$ = 12 356 630 possibilités

Si on inclut maintenant des majuscules on obtient

$52 + 52^2 + 52^3 + 52^4 + 52^5$ = 387 659 012 possibilités

Si on inclut les chiffres on obtient

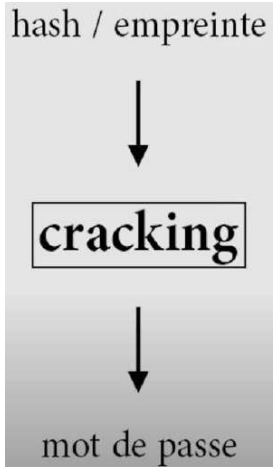
$62 + 62^2 + 62^3 + 62^4 + 62^5$ = 931 151 402 possibilités

Si on inclut les symboles on obtient

$95 + 95^2 + 95^3 + 95^4 + 95^5$ = 7 820 126 495 possibilités

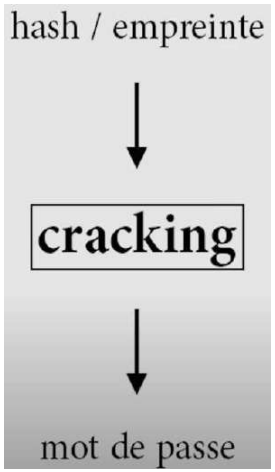
Exemple de logiciel qui calcule le nombre de possibilités et du temps de réponse:
https://www.grc.com/haystack.htm

Cracker les mots de passes



- **Méthode du dictionnaire**
  - les personnes utilisent souvent des mots standards qui se trouvent dans le dictionnaire.
  - On compose donc des tables avec des mots les plus fréquemment utiliser et on calcul leur hash.
  - Il suffit de comparer le hash a cracker et le hash de la table pour retrouver le mot de passe
  - Demo avec utilisation du logiciel HashKracker qui se trouve à l'adresse:
    - https://securityxploded.com/hash-kracker.php

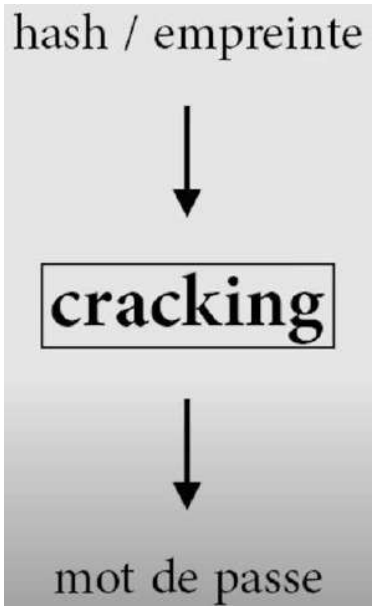
Cracker les mots de passes



- Méthode du dictionnaire avec remplacement
  - les personnes utilisent souvent des mots standards qui se trouvent dans le dictionnaire mais substitue des lettres avec des chiffres.
    - Exemples: soleil par s0le1l ce mot de passe n'est donc pas reconnu par la base de données.
  - On compose donc des tables avec des mots les plus fréquemment utiliser et les possibilités de remplacements puis on calcul leur hash.
  - Il suffit de comparer le hash a cracker et le hash de la table pour retrouver le mot de passe
  - Évidemment le temps requis pour la recherche est beaucoup plus long

Exemple de remplacement:
Maison devient ma1son – mais0n – ma1s0n
il faut donc dans ce cas essayer trois possibilités du mot.

Cracker les mots de passes



- **Méthode de l'attaque ciblée**
  - les personnes utilisent souvent des mots qui leurs sont propres et qui reflètent d'une manière ou l'autre leur personnalité.
  - On compose donc des tables avec des mots les plus fréquemment utiliser en consultant l'utilisation des milieux sociaux (Facebook etc..) puis on calcul leur hash.
  - Il suffit de comparer le hash a cracker et le hash de la table pour retrouver le mot de passe

Informations sur la cible

- John Smith
- 45 ans
- Vit à New York
- Marié à Alice Smith

Composition d'une table avec par exemple:

John
Smith
Date de naissance et 45
New York et NYC
Alice
Marié

Cracker les mots de passes

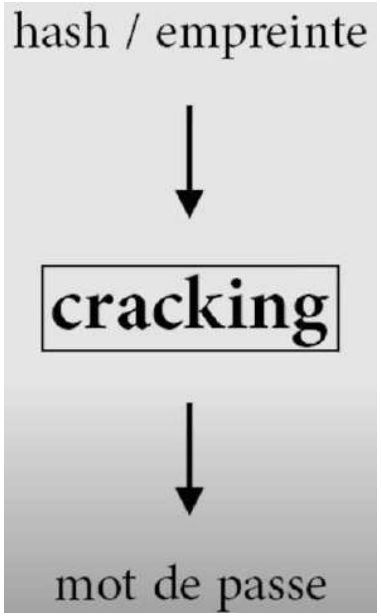
Combien de temps faut-il pour craquer un mot de passe ?

Longueur du mot de passe	Chiffres uniquement	Lettres minuscules & majuscules	Chiffres, lettres minuscules & majuscules	Chiffres, lettres min & maj, symboles
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

Cracker les mots de passes

- **Demonstration**
  - **Composition d'un hash :** https://emn178.github.io/online-tools/sha256.html
  - **Recherche inverse d'un hash avec utilisation du logiciel HashKracker (méthode force brut):** https://securityxploded.com/hash-kracker.php
  - **Recherche inverse d'un Hash avec logiciel en ligne (utilisation de fichier arc-en-ciel (Rainbow file):**
    - https://hashtoolkit.com/decrypt-hash/?hash=ed45d626b07112a8a501d9672f3b92796a6754b8d8d9cb4c617fec9774889220
    - **ou un logiciel payant:** https://gpuhash.me/
  - **Calcul de la complexité d'un mot de passe:**
    - https://www.grc.com/haystack.htm

Cracker les mots de passes



Il existe beaucoup d'autres méthodes sophistiquées mais, pour aujourd'hui cela devrait suffire.

Vous réaliser maintenant l'importance d'avoir un mot de passe sécuritaire.

Un peu d’humour