Introduction

La cybersécurité est devenu un branche importante du monde informatique et civique moderne, que ce soit dans le monde des assurances ou le monde publique.

La cybersécurité est tellement importante qu'une attaque contre une entreprise doit être déclarée par celle-ci et que d'éventuelles attaques doivent être prévenu.

Dans la sécurité, il y un petit chapitre dédié à la cryptographie. Dans les années 80, la cryptographie était à usage militaire seulement.

La cryptographie, c'est le code secret dans le monde militaire et preuve de confiance dans le monde civile.

La cryptographie peut être simple, par exemple le code César, un simple décalage de 3.

Cependant, cette méthode peut être contré par un repérage des mots de peu de lettres ou à l'aide d'un calcul statisque des lettres utilisées.

Une des méthodes utilisées par la suite est la création de machines complexes de chiffrement, mais celles-ci peuvent être volé et comprises.

Une autre méthode est la création d'algo de chiffrement à l'aide du message.

```
1       K
2  M ->[f]->C
3
4  M = le message "en clair"
5  K = la clé
6  C = le message "chiffré"
```

Les algos de chiffrages publics sont l'AES, le RSA, etc..

En chiffrement, M est secret et C est chiffré. En authentification, M connu et C est secret.

Exemple: Lors d'un achat en ligne, type Amazon, la banque a confiance dans le document envoyé par Amazon pour demander le débitement de l'achat. C'est de l'authentification. On s'aide pour cela de la clé de chiffrement pour signer la transaction.

On a deux niveaux dans la cryptographie:

1. Quels sont les algos pour chiffrer des messages de taille fixe / limitée ?
2. Avec l'AES ou le RSA, comment chiffer des messages de très grandes longueurs.

Deux obstacles dans la conception d'algorithme de chiffrement, nommée algorithme de base, par exemple pour 1024 bits:

- Le mode de chiffrement: on veut chiffrer des bits, pas des caractères, de plus l'addition et la multiplication ne sont pas stables car trop long et lourd.
- Le protocole de chiffrement

Dans ce cours, on va étudier l'arithmétique modulaire et le RSA.

Arithmétique modulaire

L'arithmétique date de la Grèce antique et c'est la science de l'addition et de la multiplication sur les nombres.

Addition et multiplication dans Z/nZ

a $\equiv$ b (mod n), a - b divisible par n. Dire que a et b sont congruant permet d'avoir une relation de quasi équalité.

Classe de a: $\bar{a}$ = {u $\in$ Z, u $\equiv$ a (mod n)} = { a + kn, k $\in$ Z}

Classe de m ~ classe de la division de m par n

Z/nZ = $\{\bar{0}, \bar{1}, \ldots, \bar{n-1}\}$

La modulation permet de diminuer et d'atténuer la grandeur des nombres en cryptographie.

Valeur = un nombre entre 0 et n-1 Module = n

L'addition

n = 10, 7 et 4

Une addition modulaire est une addition des classes modulaires.

$a \bar{+} b$ = (a + b) % n

Exemple : 7 + 4 = 11, 17 + 24 = 41

$\bar{7} + \bar{4} = \bar{1}$

4 propriétés:

1. La commutativité
2. L'associativité
3. L'élèment neutre = 0
4. Tout élèment a son opposé tel que a + b = 0, avec b = -a

(Z/nZ, +), *Groupe commutatif*, Elèment neutre *0*

$\bar{-a}$ = n - a, - a = n - a $\bar{a}$ - $\bar{b}$ = $a \bar{-} b$ a - b = (a - b) % n

La multiplication

$\bar{a}, \bar{b} \in$ Z/nZ

$\bar{a}$ * $\bar{b}$ = $\bar{ab}$

a * b = ab % n

(a + kn)(b + ln) = ab + (kb + al + kln)n

4 propriétés:

- La commutativité
- L'associativité
- L'élèment neutre = 1
- L'élèment absorbant = 0

Ici, le produit de deux nombres peut donner 0.

Exemple: en table de 4: 2 * 2 = 4 % 4 = 0

2 situations:

1. (Z/nZ, +, *) : Anneau commutatif, unitaire
2. (Z/nZ, +, *) : Corps commutatif

On a un corps ssi le nombre du modulo est premier.

Théorème de Bézout:

Soient a et n deux entiers ($\in$ Z), a et n premiers entre eux ssi $\exists$(s, t) $\in Z^2$, as + nt = 1

Algorithme d'Euclide (étendu): A chercher

Dans Z/nZ, Bezout s'écrit as $\equiv$ 1 (n)

a inversible modulo n ssi a premier avec n

s $equiv$ a^{-1} (mod n)

Résumé

1. La cryptographie est un chapitre de la sécurité
2. La cryptographie c'est savoir faire du chiffrement

3. La cryptographie se déroule dans l'arithmétique modulaire, se comportant à une propriété près comme l'arithmétique classique