# Introduction à la Securité,

Licence IUT R & T 2015-2016
pascal.lafourcade@udamail.fr

## 1 Pour le cours 2

**Exercise 1 (RSA)**
Nous rappelons le chiffrement RSA.

- Clef publique : $(n, e)$, où $n = pq$, $\Phi(n) = (p-1)(q-1)$ et $pgcd(e, \Phi(n)) = 1$.
- Clef privée : $d$, tel que $d.e = 1 \mod \Phi(n)$
- Chiffrement : Pour chiffrer $M$ Bob calcule $c = M^e \mod n$
- Déchiffrement : $M = c^d \mod n$

1. Soit $p = 3$, $q = 7$, calculer $n$ et $\Phi(n)$.
2. Soit $e = 5$, chiffrer le message $M = 2$.
3. Soit la clef privée $d = 5$ déchiffrer le message $c = 3$.

***Solution :***

1. $n = 21$, $\Phi(n) = 12$
2. $c = M^e \mod n = 2^5 \mod 21 = 32 \mod 21 = 11$
3. $M = c^d \mod n = 3^5 \mod 21 = 3.3.3.3.3 \mod 21 = 27.9 \mod 21 = 6.9 \mod 21 = 54 \mod 21 = 12$
4. $n = pq \rightarrow p$ *et* $q$
5. *on retrouve* $d$ *connaissant* $p$ *et* $q$

**Exercise 2 (ElGamal (5 points))**
Nous rappelons le chiffrement d'ElGamal, où la clef privée est $a$ et la clef publique et $(p, g, h)$, avec $h = g^a \mod p$.

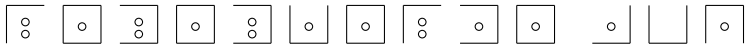
- Chiffrement : Pour chiffrer $M$ Bob choisit un nombre aléatoire $r$ et calcule $(u, v) = (g^r \mod p, Mh^r \mod p)$
- Déchiffrement : $M \equiv_p \frac{v}{u^a}$

1. (3 point) Soit $a = 2$ et $(p, g) = (5, 3)$, calculer $h$ et déchiffré le message $c = (4, 2)$.
2. (2 points) Le nombre aléatoire $r = 2$ a servi à calculer le message $c$. Vérifier que le chiffré du message trouvé à la question précédente correspond bien à $c$.

***Solution :***

1. *(3 points) Soit* $a = 2$ *et* $(p, g) = (5, 3)$ *les paramètres privé et publique d'un chiffrement d'Elgamal.*
   $4 = h = g^a \mod p = 3^2 \mod 5 = 9 \mod 5$ .
   $r = 2$, $M = 2$ $(u, v) = (g^r, Mh^r) = (3^2 \mod 5, 2 \times 4^2 \mod 5) = (4, 2)$
   $\frac{v}{u^a} = \frac{2}{4^2} = \frac{2}{1} = 2$

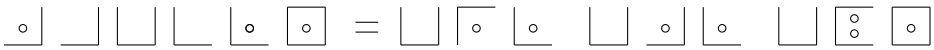
**Exercise 3 (Chiffrement de Churchyard (10 points))**



**Histoire:** Ce message chiffré est gravé sur une tombe dans le cimetière de Trinity Churchyard (New York) depuis 1794. Of course le texte chiffré est écrit en anglais. Il fut déchiffré en 1896.

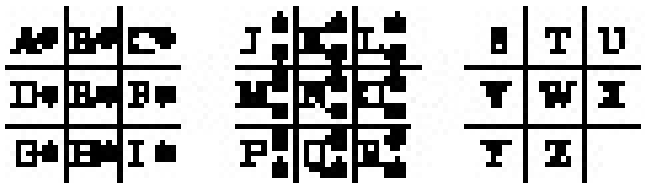
1. (6 points) En utilisant l'astuce (hint en anglais) retrouvez le message original ?
2. (4 points) Comment fonctionne ce chiffrement ?

ASTUCE = TIC TAC TOE



***Solution :***

1. *Substitution.*
2. *Not enought cipher text to perform a frequency analysis.*
3. *REMEMBER DEATH*
4. *The substitution is designed by this scheme:*



## 2 Pour le cours 3

**Exercise 4 (Chiffrement symétrique)**

1. Donner les avantages d'un chiffrement symétrique.
2. Donner les désavantages d'un chiffrement symétrique.

***Solution :***

1. *Rapide, clef courtes, temps réel, hardware implementations.*

2. *Echange des clefs, gestion des clefs une par contact, taille des messages fixes, ne permet pas de signer.*

**Exercise 5 (Fonctions de Hachage)**
Pour chaque fonction de hachage naïves suivante donner des attaques de écurité si possible :

1. Pour les humains, la fonction de hachage retourne le genre de la personne
2. Pour les humains, la fonction de hachage retourne la couleur des yeux
3. Pour les humains, la fonction de hachage retourne les empreintes digitales
4. La fonction de hachage retourne le poids de Hamming
5. La fonction de hachage retourne le nombre de 0 suivit du nombre de 1

***Solution :***

1. *Pour les humains, la fonction de hachage retourne le genre de la personne.*
   *Il est facile de trouver deux humains ayant le même genre (non collision resitant).*
2. *Pour les humains, la fonction de hachage retourne la couleur des yeux*
   *Il est facile de trouver deux humains ayant la même couleur des yeux. (non collision resitant).*
3. *Pour les humains, la fonction de hachage retourne les empreintes digitales.*
   *Il n'est pas facile de trouver deux humains ayant la même couleur des yeux. (collision resitant).*
4. *La fonction de hachage retourne le poids de Hamming.*
   *Il est facile de trouver deux nombres ayant le même poids de Hamming.(non collision resitant).*
5. *La fonction de hachage retourne le nombre de 0 suivit du nombre de 1*
   *Il est facile de trouver deux nombres ayant le même nombre de 0 et de 1.(non collision resitant).*

# 3 Pour le cours 4

**Exercise 6 (Chiffrement déterministique)**

1. Montrer qu'un chiffrement déterministique n'est pas IND-CPA.

***Solution :***

1.

**Exercise 7 (Shamir 3-Pass protocole)**
En utilisant le chiffrement OTP, c'est-à-dire $c = m \oplus m$, voici le protocole de Shamir :

1. A $\rightarrow$ B : $m \oplus KA$
2. B $\rightarrow$ A : $(m \oplus KA) \oplus KB$
3. A $\rightarrow$ B : $m \oplus KB$

1. Trouver une attaque passive contre ce protocole
2. Trouver une attaque par rejeu contre ce protocole

***Solution :***

1.
2.

# 4 Pour le cours 5

**Exercise 8 (Side channel)**
Soit une digicode à 4 chiffres, qui allume une lumière verte par défaut et une lumière rouge dès qu'un des chiffres n'est pas correct.

1. Combien existe-t-il de code possibles pour un tel digicode?
2. En combien d'essai est-il possible de trouver le code?

***Solution :***

*1.*

*2.*

**Exercise 9 (E-vote)**

- Identifier les acteurs d'un système de vote en ligne
- Donner les propriétés de sécurité de ce système.

***Solution :***

*1.*

*2.*