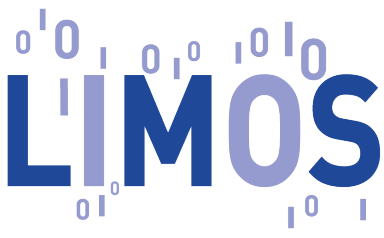
Chiffrement à clé publique

Pascal Lafourcade



2022-2023

Chiffrement à Clé publique

Exemples

- RSA : $c = m^e \mod n$
- ElGamal : $c \equiv (g^r, h^r \cdot m)$

Plan

Plan

Fonction à sens unique (One-way function)

Définition

Une fonction à sens unique si :

- elle est facile à calculer
- son inverse est difficile à calculer :

$$\Pr[m \xleftarrow{r} \{0,1\}^*; y := f(m) : f(A(y, f)) = y]$$

est negligeable.

Trappe (Trapdoor):

- L'inverse devient facile à calculer avec la connaissance d'une information additionnelle.

Factorisation

Factorisation

- $p, q \mapsto n = p.q$ facile (quadratique)
- $n = p.q \mapsto p, q$ difficile

Exemple :

$$633074497293458013329878397376016798042565813844911$$

Factorisation

Factorisation

- $p, q \mapsto n = p.q$ facile (quadratique)
- $n = p.q \mapsto p, q$ difficile

Exemple :

$$633074497293458013329878397376016798042565813844911$$

$$= 80406619138040667977 \times 787341271253560435407513019474 3$$

Logarithme Discret

Soit G un groupe cyclique engendré par g d'ordre n :

$$G = \{1, g, g^2, \ldots, g^{n-1}\}$$

Logarithme discret

- $g, n, x \mapsto y = g^x \mod n$ facile (quadratique)
- $g, n, y = g^x \mod n \mapsto x$ difficile

Exemple :
$n = 7, g = 3$

$$3^5 \mod 7 \equiv 243 \mod 7 \equiv 5$$

Plan

Rappel : Petit théorème de Fermat

Petit théorème de Fermat

Soit p premier et a entier. Alors $a^p \equiv a \mod p$.

Remarque : $(k+1)^p \equiv k^p + 1 \mod p$ coefficiet binomiaux sont tous multiples de p

Preuve d'Euler (par récurrence)

- **Cas de base :**
  Pour $a = 1$ on a bien $a^p \equiv a \mod p$.
- **Hypothèse de récurrence :**
  Pour a, $a^p \equiv a \mod p$.
- **Induction :**
  Montrons que $(a+1)^p \equiv (a+1) \mod p$.
  $(a+1)^p \equiv a^p + 1 \equiv (a+1) \mod p$. □

Corrolaire : Soit p premier et a entier, alors $a^{p-1} \equiv 1 \mod p$.

Généralisation : Théorème d'Euler

Théorème d'Euler

Pour tout entier $n > 0$ et tout entier a premier avec n

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

où φ est la fonction indicatrice d'Euler.

Pour tout entier naturel n non nul, la fonction φ associe le nombre d'entiers compris entre 1 et n (inclus) et premiers avec n.
Par exemple, si p et q premiers alors $\varphi(p \times q) = (p-1)(q-1)$

Généralisation : Théorème d'Euler (Preuve)

Soit $A = \{a_1, a_2, \ldots, a_{\varphi(n)}\}$ l'ensemble des entiers qui sont premiers avec n.

$$A = \{aa_1, aa_2, \ldots, aa_{\varphi(n)}\}$$

Car

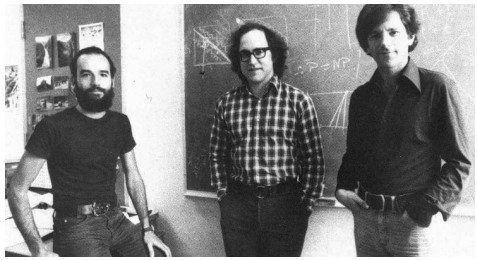
- $pgcd(a_j, n) = 1$ implique $pgcd(aa_j, n) = 1$, donc $aa_j \in A$.
- $a_i \neq a_j$ implique $aa_i \neq aa_j$

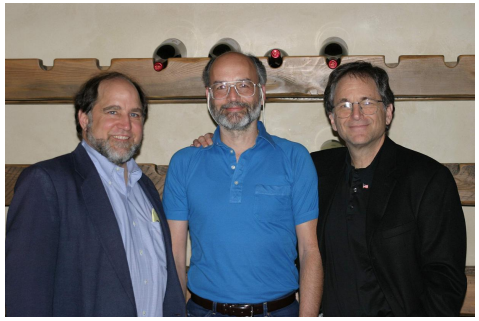
$$\prod_{i=1}^{i=\varphi(n)} a_i = \prod_{i=1}^{i=\varphi(n)} aa_i = a^{\varphi(n)} \prod_{i=1}^{i=\varphi(n)} a_i$$

Ainsi

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Rivest Shamir Adelmann (RSA 1978)





Soit $n = pq$, p et$q$ deux nombres premiers.

Clé Publique : (e, n)

Clé Secrète : d où $d = e^{-1} \mod \phi(n)$
et $pgcd(e, \phi(n)) = 1$

Chiffrement : $c = m^e \mod n$

Déchiffrement: $m = c^d \mod n$

Correction

$c^d = m^{de} = m.m^{k\phi(n)} \mod n$

Rappel : Théorème d'Euler $\forall x \in (Z/nZ)^*, x^{\phi(n)} = 1 \mod n$

Example RSA

Example

- $p = 61$
- $q = 53$
- $n = pq = 3233$
- $e = 17$
- $d = 2753$

Clé publique est (e, n) et la clé privée est d.
$Chiffrer(T) = (T^e) \bmod n = (T^{17}) \bmod 3233$
$Dechiffrer(C) = (C^d) \bmod n (C^{2753}) \bmod 3233$

- $Chiffrer(123) = 123^{17} \bmod 3233$
  $= 337587917446653715596592958817679803 \bmod 3233$
  $= 855$
- $Dechiffrer(855) = 855^{2753} \bmod 3233$

Calculs

```
855^1 = 855 (mod 3233)
855^2 = 367 (mod 3233)
855^4 = 367^2 (mod 3233) = 2136 (mod 3233)
855^8 = 2136^2 (mod 3233) = 733 (mod 3233)
855^16 = 733^2 (mod 3233) = 611 (mod 3233)
855^32 = 611^2 (mod 3233) = 1526 (mod 3233)
855^64 = 1526^2 (mod 3233) = 916 (mod 3233)
855^128 = 916^2 (mod 3233) = 1709 (mod 3233)
855^256 = 1709^2 (mod 3233) = 1282 (mod 3233)
855^512 = 1282^2 (mod 3233) = 1160 (mod 3233)
855^1024 = 1160^2 (mod 3233) = 672 (mod 3233)
855^2048 = 672^2 (mod 3233) = 2197 (mod 3233)
```

Calculs

```
855^2753 (mod 3233)
= 855^(1 + 64  + 128 + 512 + 2048) (mod 3233)
= 855^1 * 855^64 * 855^128 * 855^512 * 855^2048 (mod 3233)
= 855 * 916 * 1709 * 1160 * 2197 (mod 3233)
= 794 * 1709 * 1160 * 2197 (mod 3233)
= 2319 * 1160 * 2197 (mod 3233)
= 184 * 2197 (mod 3233)
= 123 (mod 3233)
= 123
```

Complexité de la factorisation

Lenstra-Verheul 2000

Modulus (bits)	Operations ($\log_2$)
512	58
1024	80
2048	111
4096	149
8192	156

Chiffrement d'ElGamal

Génération de clé: Choisir un premier p et un générateur g de $(Z/pZ)^*$ et $a \in (Z/(p-1)Z)^*$.

Clé Publique : (p, g, h), où $h = g^a \mod p$.

Clé Privée : a

Chiffrement : Choisir $r \in_R (Z/(p-1)Z)^*$ et calculer $(u, v) = (g^r, Mh^r)$

Déchiffrement : Avec (u, v), calculer $M \equiv_p \frac{v}{u^a}$

Justification: $\frac{v}{u^a} = \frac{Mh^r}{g^{ra}} \equiv_p M$

Optimal Asymmetric Encryption Padding : OAEP -RSA

Soit deux fonctions de hachage :

$$G : \{0,1\}^{k_0} \rightarrow \{0,1\}^{k-k_0}$$

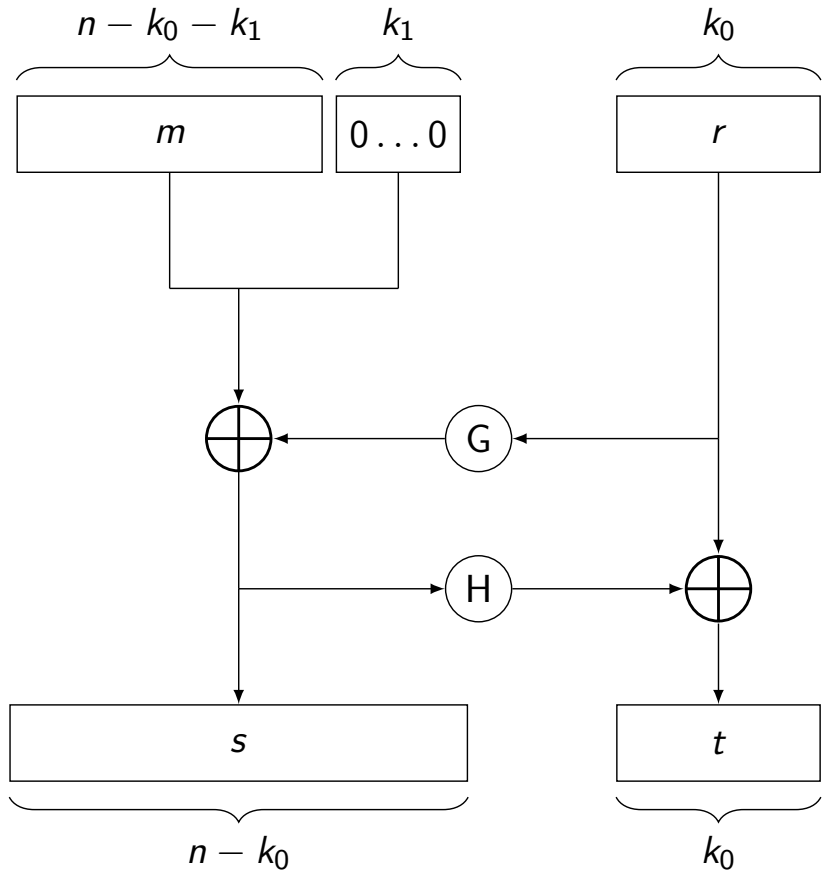
$$H : \{0,1\}^{k-k_0} \rightarrow \{0,1\}^{k_0}$$

Le chiffrement c de m avec la clef RSA pk est noté $RSA_{pk}(m)$
Le déchiffrement de c avec la clé privée sk est noté $RSA_{pk}^{-1}(m)$

OAEP: Encryption

$E_{pk}(m, r) = c = RSA_{pk}(s, t)$ avec $m \in \{0,1\}^n$, et $r \leftarrow \{0,1\}^{k_0}$

$$s = (m||0^{k_1}) \oplus G(r), t = r \oplus H(s)$$



OAEP: Déchiffrement

$D_{sk}(c)$

$$RSA_{sk}^{-1}(c) = (s, t)$$

$$r = t \oplus H(s)$$

$$M = s \oplus G(r)$$

Si $[M]_{k_1} = 0^{k_1}$, alors on renvoie $[M]^n$, sinon "Reject"

- $[M]_{k_1}$ dénote les k_1 dernier bits de M
- $[M]^n$ dénote les n premiers bits of M

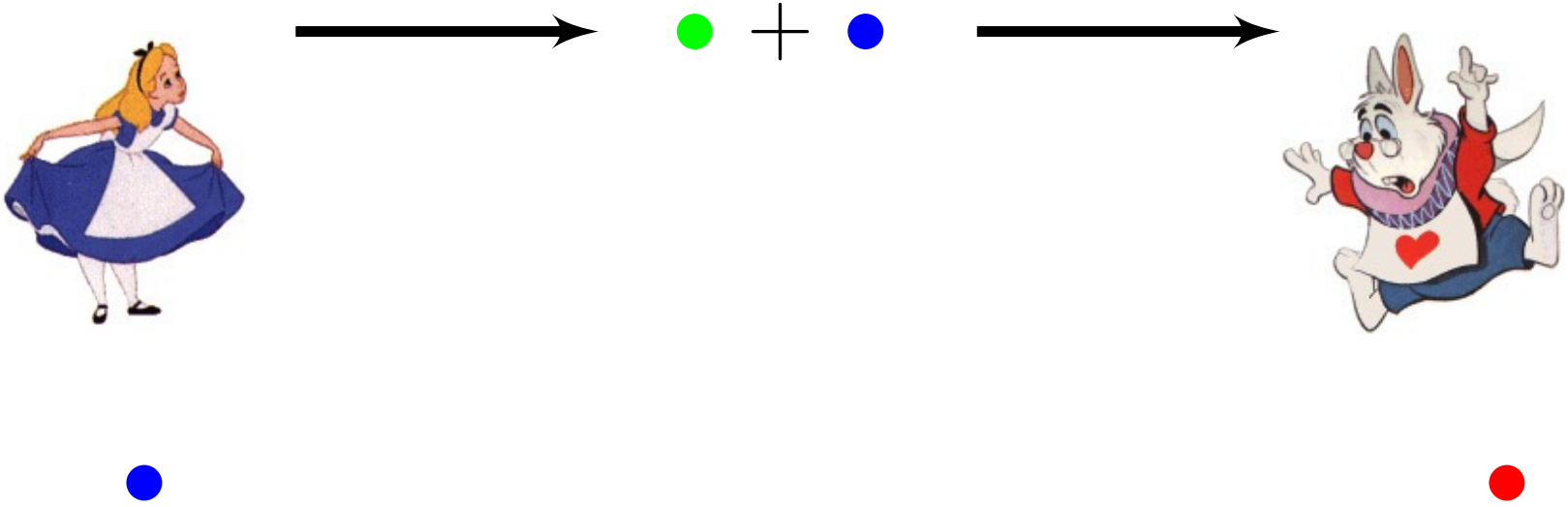
Plan

Diffie Hellman (1976)

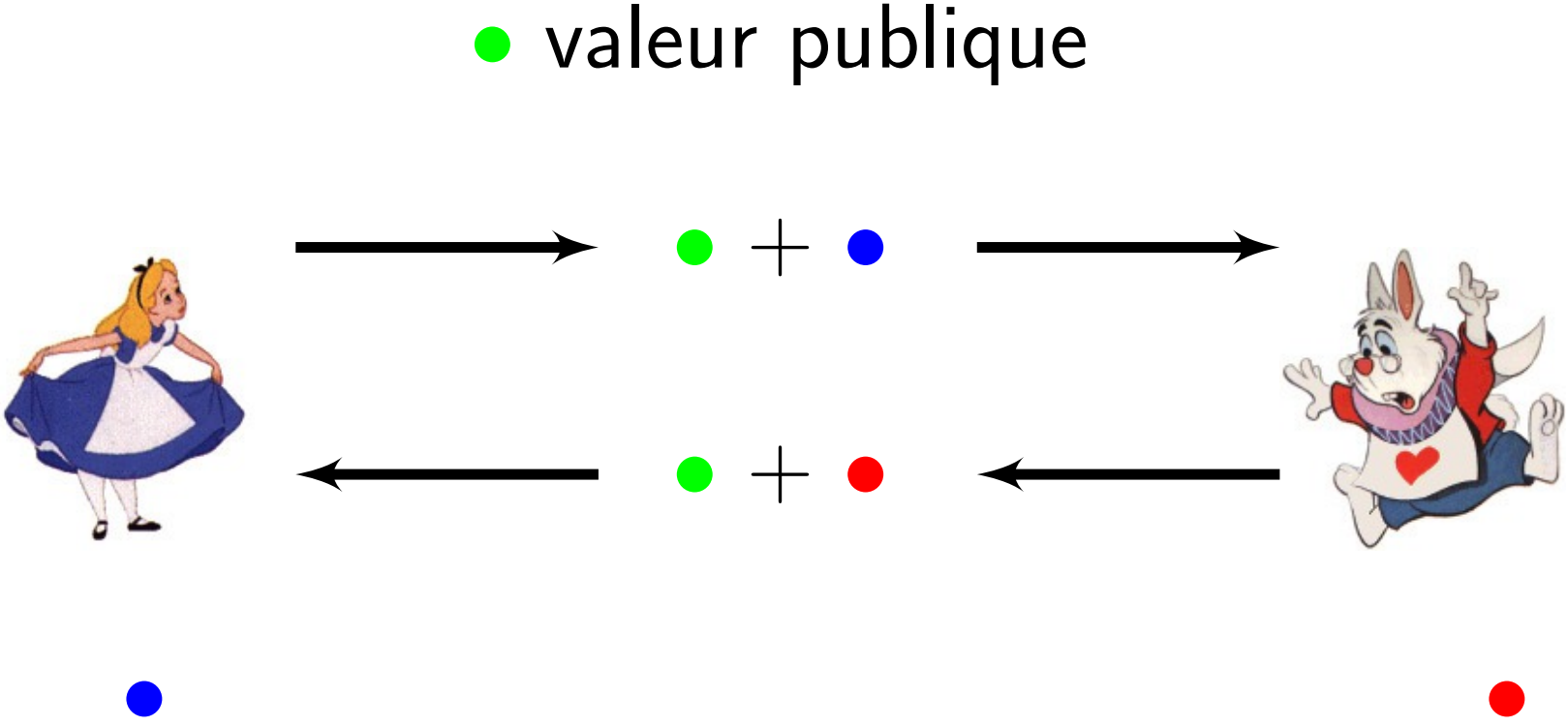
- valeur publique

Diffie Hellman (1976)

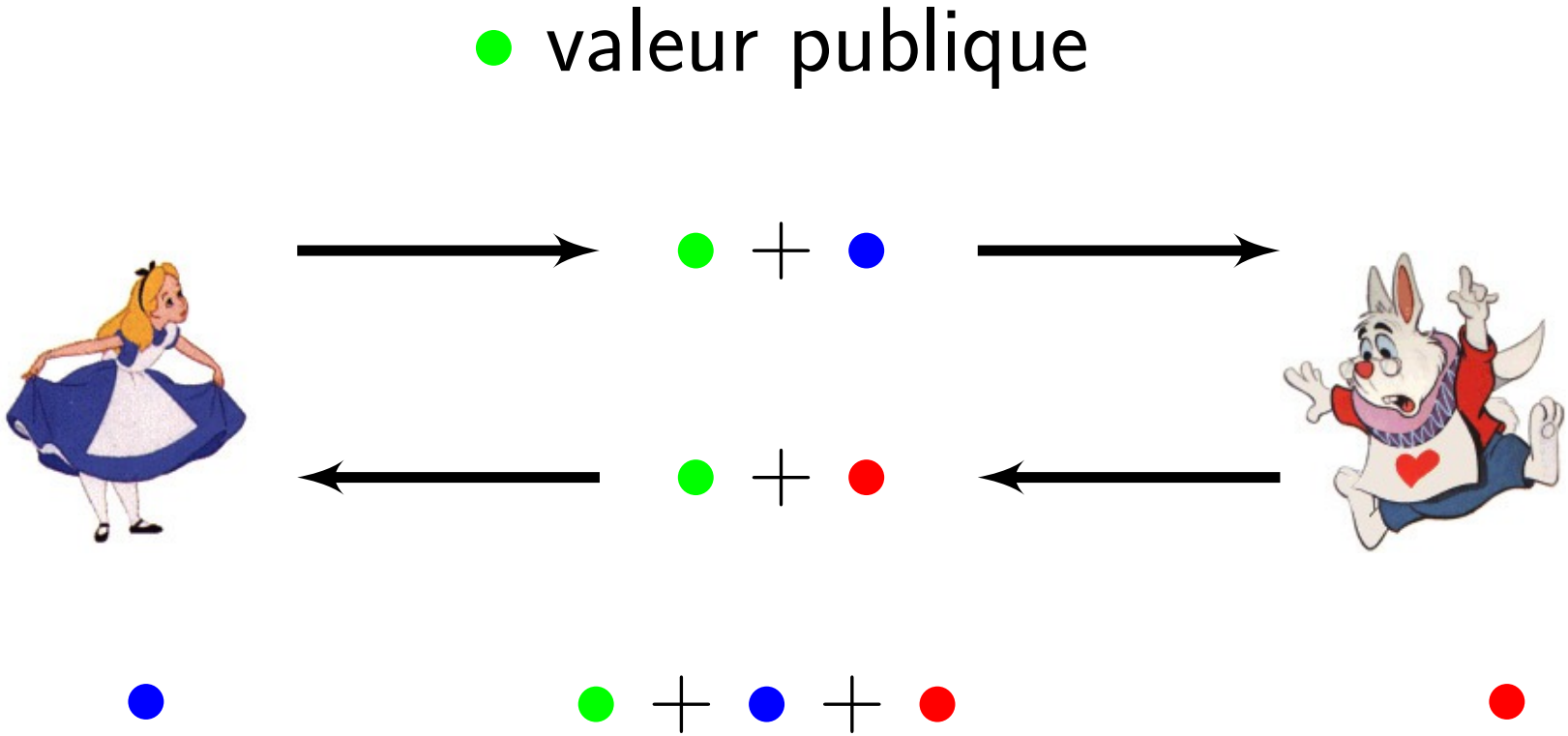
- valeur publique



Diffie Hellman (1976)



Diffie Hellman (1976)



Diffie Hellman (1976)

valeur publique

- $g =$
- $a =$
- $b =$

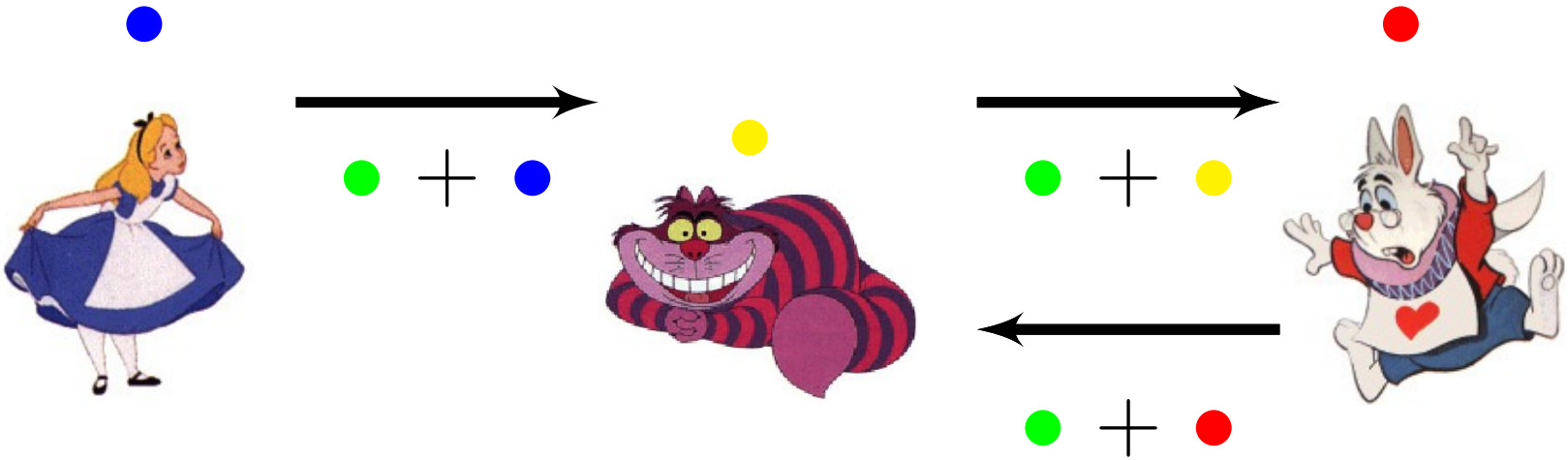
$$(g^a)^b = g^{ab} = (g^b)^a$$

Attaque “Man in the middle”

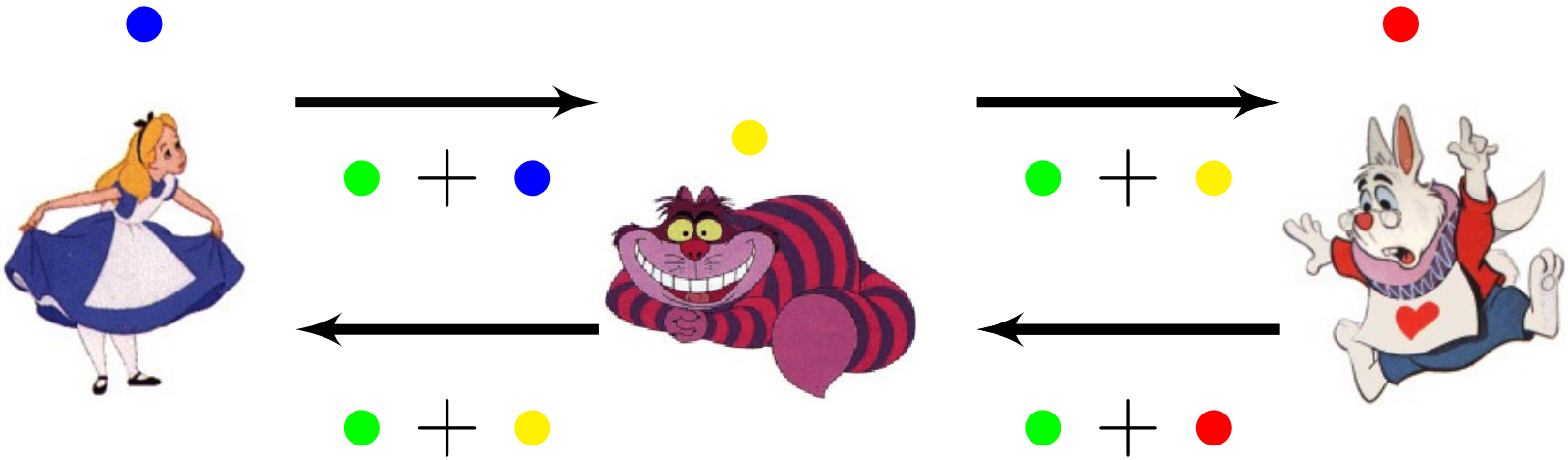
Attaque “Man in the middle”

Attaque “Man in the middle”

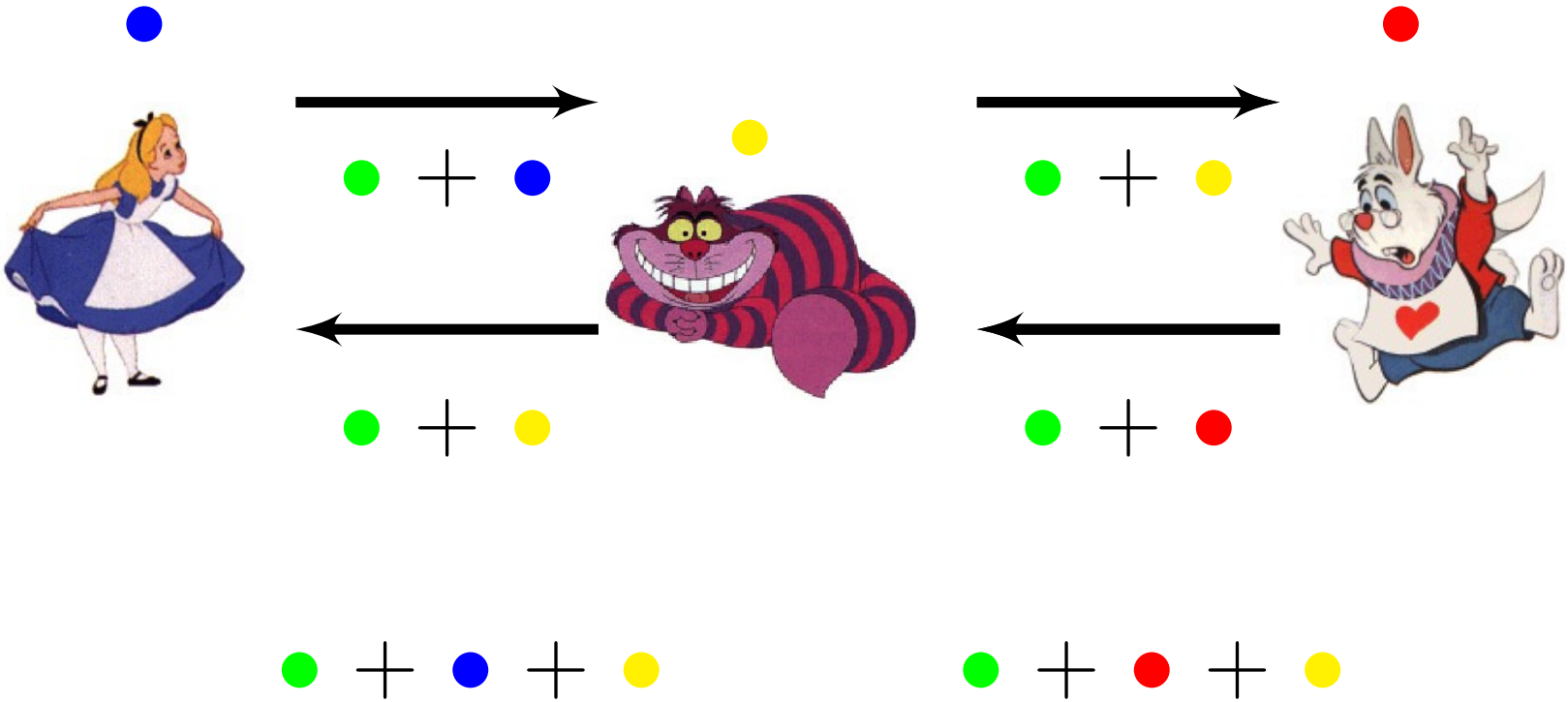
Attaque “Man in the middle”



Attaque “Man in the middle”



Attaque “Man in the middle”



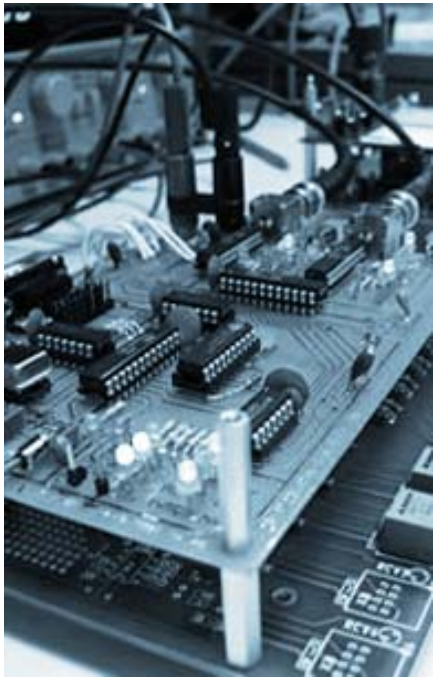
Plan

Exemple du Digicode

- Digicode avec 10 nombres possibles (0..9)
- Un code composé de 4 nombres
- A chaque erreur du moindre chiffre une lumière rouge s'allume, sinon une lumière verte s'allume.

Combien d'essais sont nécessaires pour ouvrir la porte protégée avec ce digicode ?

Differents types de Canaux Cachés



But obtenir des information sur un secret ou une clé par l'observation :

- Temps
- Énergie
- Cache
- Injection de fautes
- Émission électromagnetique ...

Timing Attacks on Implementations of Diffie–Hellman, RSA, DSS, and Other System... Paul Kocher - CRYPTO - 1996

Code Pin à l'épreuve du temps

Pour un 8 bytes code PIN, il y a $(2^8)^8 = 256^8$ possibilités par attaque par Brute Force.

Programme

```
for ( i = 0 ; i <= 7; i++)
      if ( pinCarte[i] != pinPresente[i] ) return false;
return true ;
```

Combien faut-il d'essais pour trouver le code PIN vérifé par ce programme ?

Code correct

Program

```
boolean test = true ;
for ( i = 0 ; i <= 7; i++)
    test = test && ( pinCarte[i] == pinPresente[i]);
return test ;
```

Pourquoi ce code est plus sûr ?

Calcul naïf

Écrire un programme Python qui calcule $x^n \mod p$?

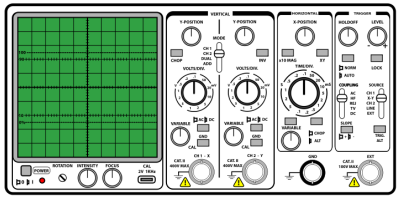
Exponentielle rapide

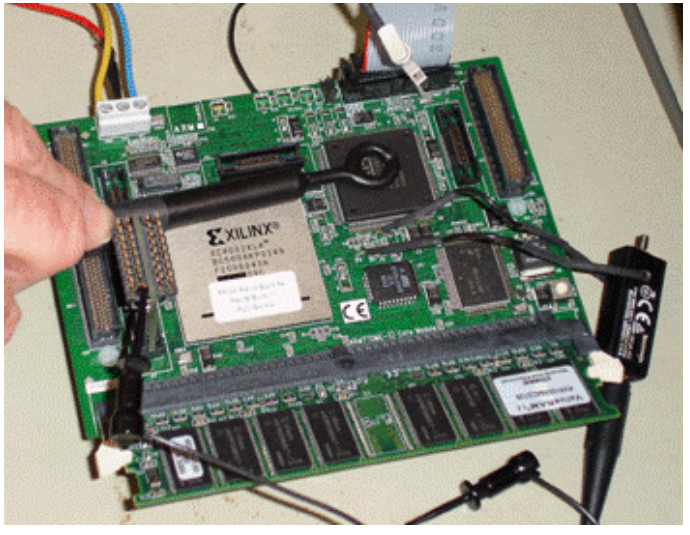
L'algorithme d'**exponentiation rapide** calcule plus vite $x^n \bmod p$

$$\text{expo}(x, n, p) =$$

$$\begin{cases} 1, & \text{si } n = 0 \\ \text{expo}(x^2 \bmod p,\ n/2, p), & \text{si } n \text{ est pair} \\ x \cdot \text{expo}(x^2 \bmod p,\ (n-1)/2, p) \bmod p, & \text{si n est impair} \end{cases}$$

Messurer la consomation électrique



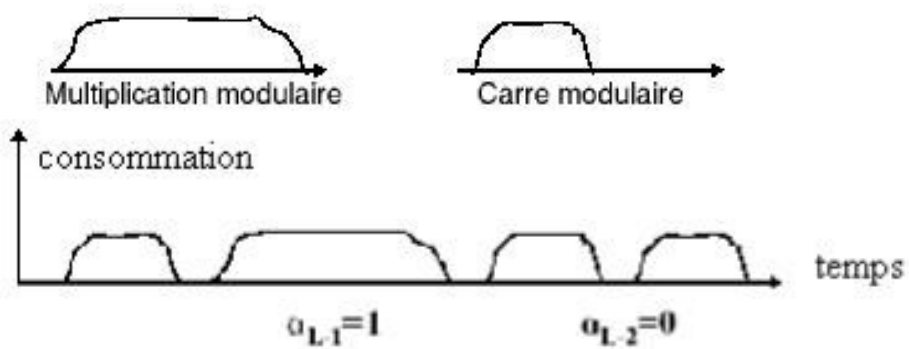


Attaque par consommation électrique sur le déchiffrement de RSA

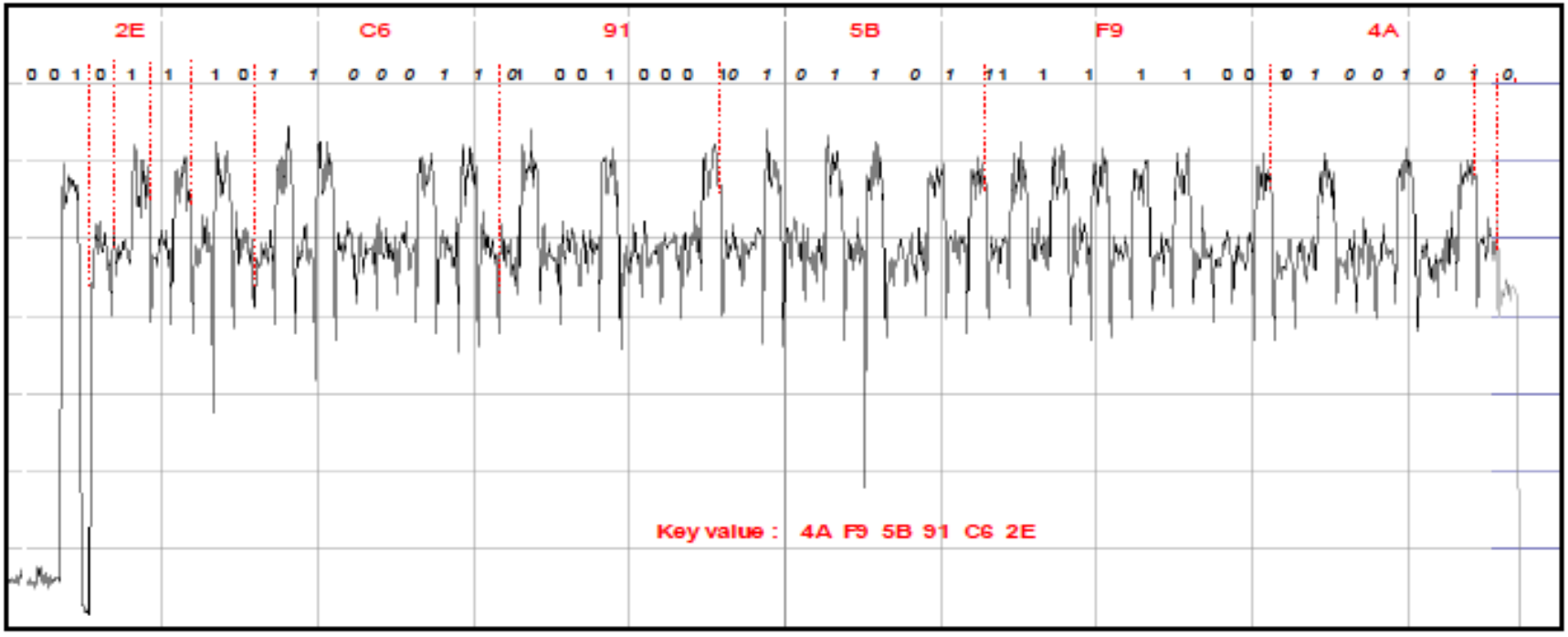
Pour déchiffré il faut calculer $y^d \mod n$, où y est le chiffré, n est publique et d est la clé secrète.

Programme d'exponentielle rapide

```
s = 1 ;
for ( i = L-1 ; i >= 0; i --) {
      s = s*s mod n ;
      if ( d [ i ] == 1)
            s = s*y mod n ;
}
return s
```



In reality



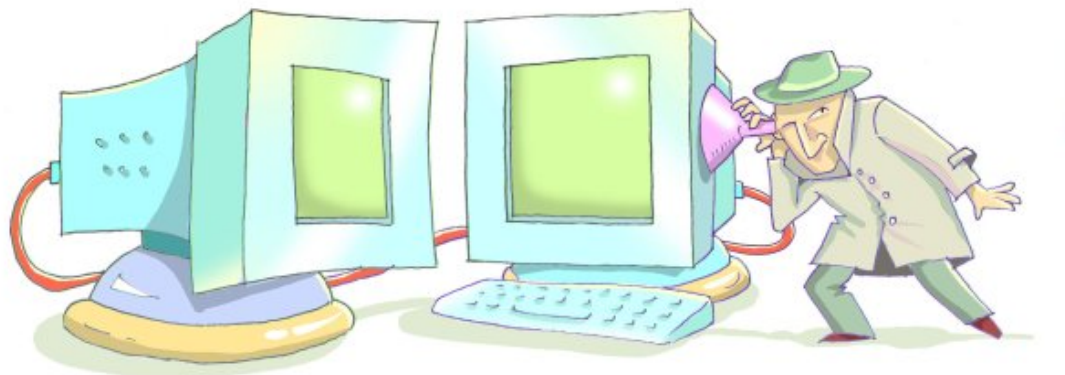
Acoustic cryptanalyse I

Dans son livre Spycatcher, l'ancien agent du MI5 Peter Wright décrit une attaque acoustique contre le chiffrement mécanique Egyptien Hagelin en 1956, sous le nom de code "ENGULF".

HAGELIN M-209 CIPHER MACHINE (GVG / PD)

Acoustic cryptanalyse II

En 2004, Dmitri Asonov et Rakesh Agrawal d'IBM que les claviers sont vulnerables à une attaque sur les sons émis par les touches.



Plan

Aujourd'hui

1. Chiffrement à clé publique
2. Diffie Hellman
3. Attaques par canaux auxilliaires

Merci pour votre attention.

Questions ?

Adi Shamir

“Fully secure systems don’t exist today and they won’t exist in the future.”