La Cryptographie

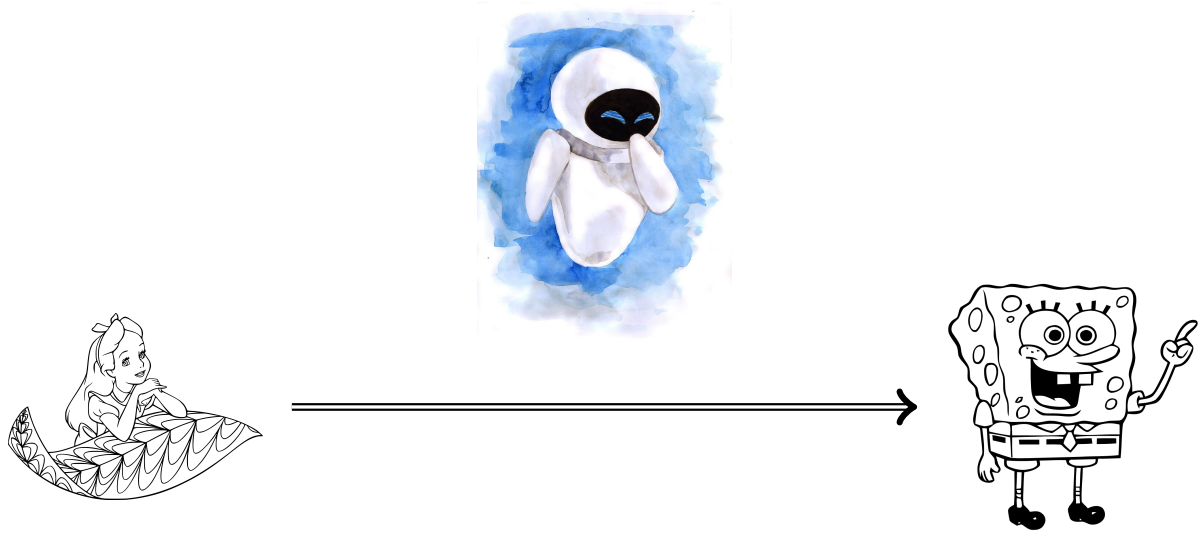
Les Mathématiques et l'Art du Secret

Yann Rotella

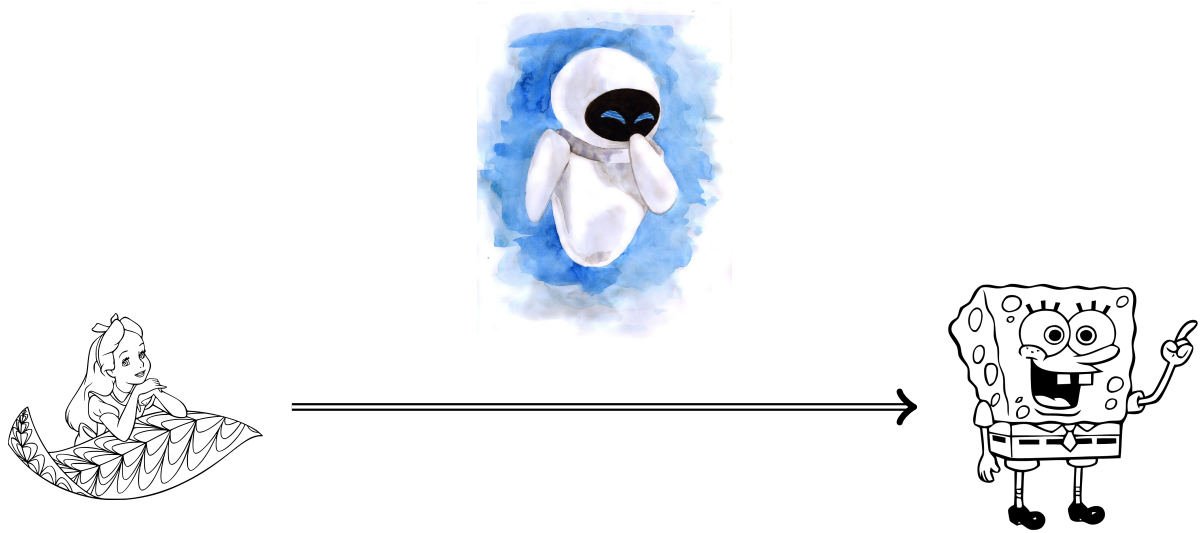
Université de Versailles Saint Quentin en Yvelines

Parlons Maths, 7 avril 2020

DÉFINITION



Définition



Enjeux

Sécurité, confidentialité et authenticité

Programme des 45 minutes

Éléments historiques

Bases de la cryptographie moderne

La Cryptographie symétrique

La cryptographie asymétrique

Éléments historiques

Bases de la cryptographie moderne

La Cryptographie symétrique

La cryptographie asymétrique

La Scytale

- Le plus ancien système cryptographique militaire (V av J-C).
- Chiffrement par transposition.
- Nombre de clefs très faibles.

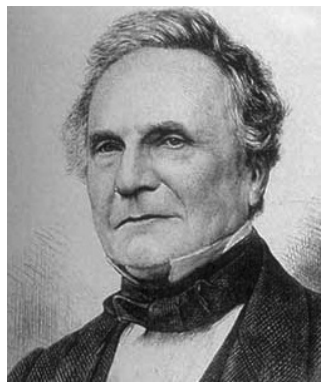
Le code de César

- décalage de l'alphabet
- chiffrement par substitution
- 25 clefs possibles

Le Chiffre de Vigenere

16ème siècle. Cassé en 1854.

Blaise de Vigenere



Charles Babbage

Idée de l'attaque :

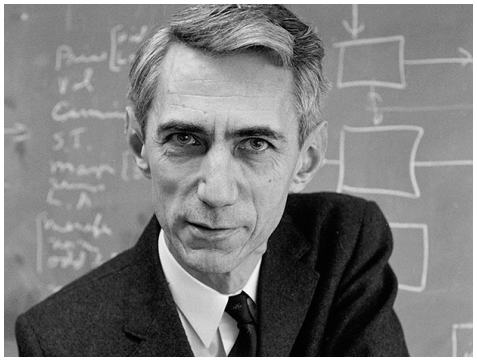
1. Trouver des motifs qui se répètent
2. En déduire des tailles de clefs possibles
3. Analyse de fréquences

Le Principe de Kerckhoffs (1883)

Auguste Kerckhoffs (1835 - 1903)

La sécurité d'un système ne doit pas exiger de secret autre que la clef.

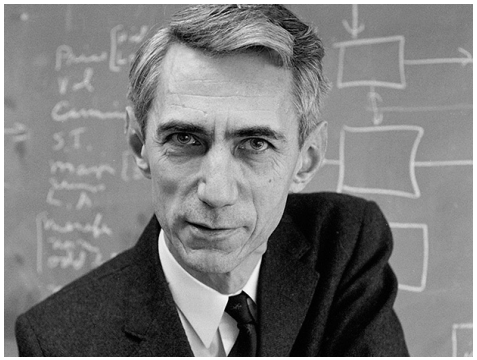
Les travaux de Claude Shannon (1949)



Sécurité inconditionnelle

La connaissance du message chiffré n'apporte aucune information sur le message clair. Pour assurer cela, la clef doit être au moins aussi longue que le message

Les travaux de Claude Shannon (1949)



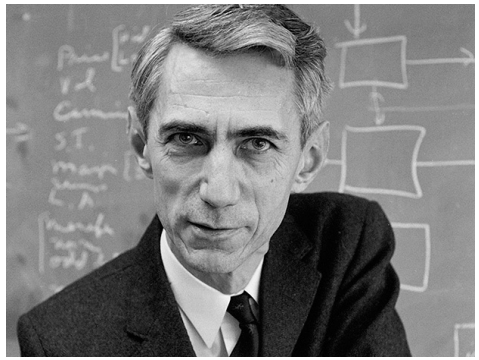
Sécurité inconditionnelle

La connaissance du message chiffré n'apporte aucune information sur le message clair. Pour assurer cela, la clef doit être au moins aussi longue que le message

Sécurité Pratique

La connaissance du message chiffré (ou de couples clairs-chiffrés ne permet de retrouver le message ou la clef en un temps raisonnable.

Les travaux de Claude Shannon (1949)



Sécurité inconditionnelle

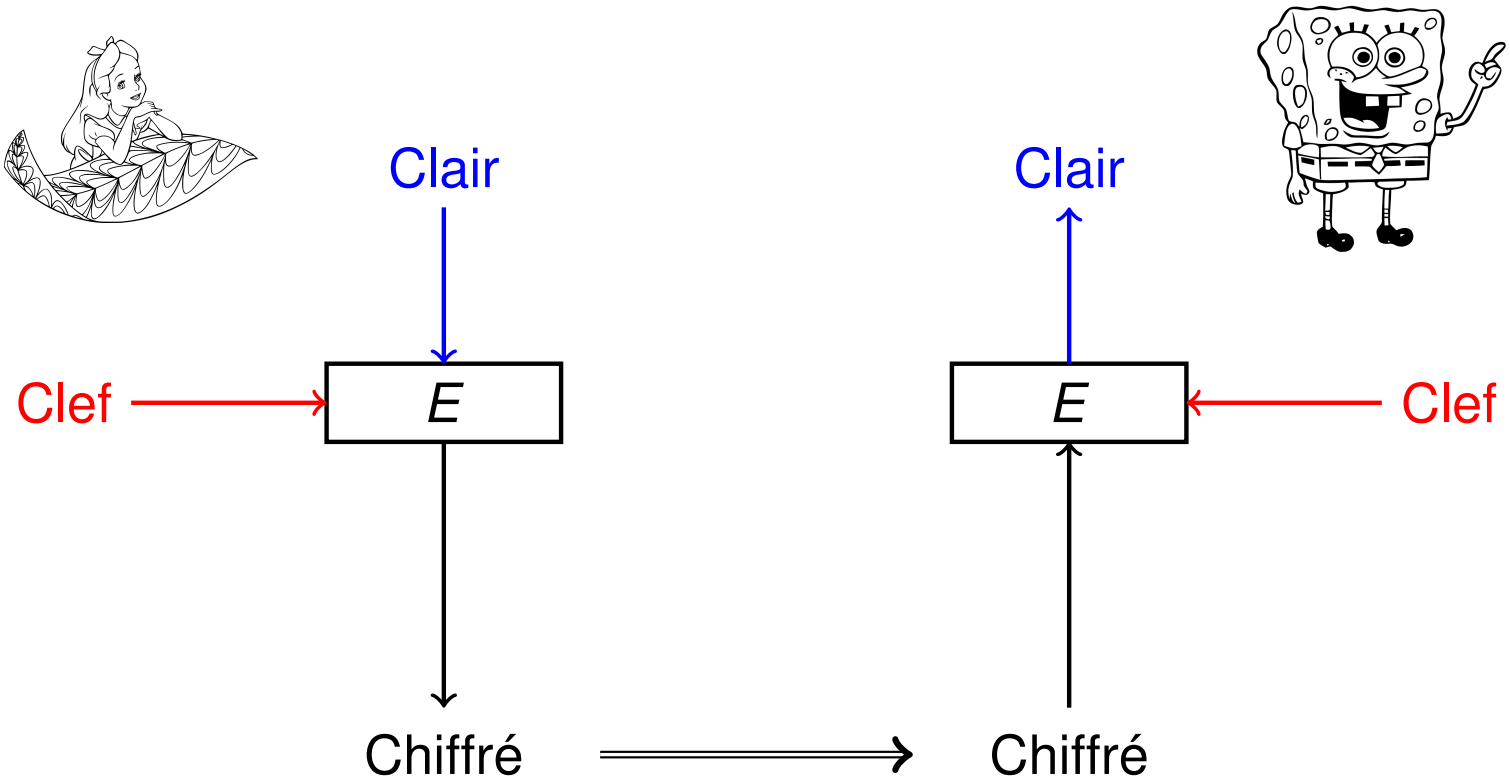
La connaissance du message chiffré n'apporte aucune information sur le message clair. Pour assurer cela, la clef doit être au moins aussi longue que le message

Sécurité Pratique

La connaissance du message chiffré (ou de couples clairs-chiffrés ne permet de retrouver le message ou la clef en un temps raisonnable.

- Diffusion
- Confusion

LE PROBLÈME



Taille des clefs

Quelques exemples

- Substitution mono-alphabétique :
  $403291461126605635584000000 \approx 4 \cdot 10^{26}$
- Enigma (1919) : $158962555217826360000 \approx 1,59 \cdot 10^{20}$
- DES (Data Encryption Standard, 1976 - 2004) : $2^{56} \approx 7 \cdot 10^{16}$

juin 97	96 jours (Deschall Project, 78 000 PC)
fev 98	39 jours (Distributed.net, 8 millions de processeurs)
juil 98	56 h (EFF, DES cracker, 250 000 $)
janv 99	22h15 (EFF DES cracker + 100 000 processeurs)
mars 07	6 jours (Copacabana, 9000 euros)

TAILLE DES CLEFS

- Age de l'univers (jours) : $4 \cdot 10^{12} = 4000000000000$
- Nombre d'atomes dans l'univers : $10^{80} =$ 100000000000000000000000000000000000000000000000000000000000000000000000000000

Taille des clefs

- Age de l'univers (jours) : $4 \cdot 10^{12} = 4000000000000$
- Nombre d'atomes dans l'univers : $10^{80} =$ 100000000000000000000000000000000000000000000000000000000000000000000000000000

Nombre de clefs éxaminées par

- une machine à un milliard d'euros en un siècle : $3 \cdot 10^{26} = 300000000000000000000000000$
- une machine à un milliard d'euros depuis la création de l'univers : $10^{33} = 1000000000000000000000000000000000$
- autant de Copacabana que d'atomes dans l'univers depuis la création de l'univers : $10^{109} =$ 10000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

Taille des clefs

- Age de l'univers (jours) : $4 \cdot 10^{12} = 4000000000000$
- Nombre d'atomes dans l'univers : $10^{80} =$ 100000000000000000000000000000000000000000000000000000000000000000000000000000

Nombre de clefs éxaminées par

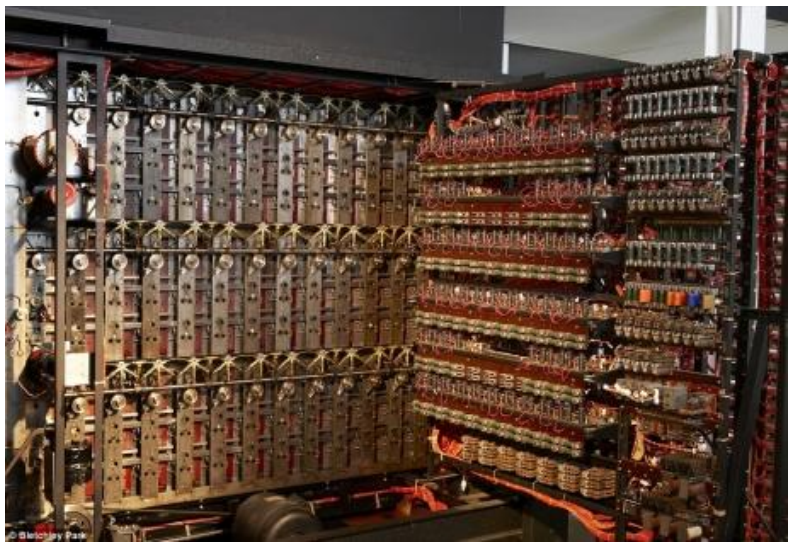
- une machine à un milliard d'euros en un siècle : $3 \cdot 10^{26} = 300000000000000000000000000$
- une machine à un milliard d'euros depuis la création de l'univers : $10^{33} = 1000000000000000000000000000000000$
- autant de Copacabana que d'atomes dans l'univers depuis la création de l'univers : $10^{109} =$ 10000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

On choisit 128 ou 256 bits, *i.e.* 10^{40} et 10^{80}

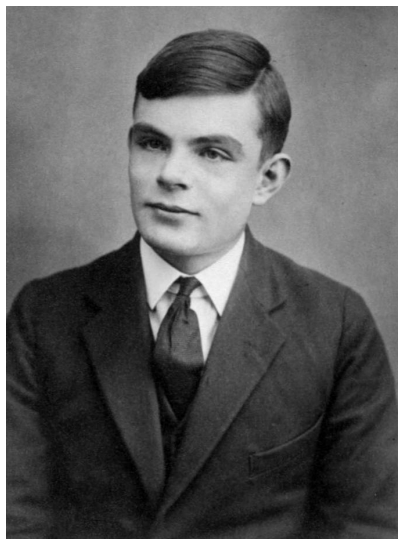
La machine Enigma (1919)

- Plusieurs substitutions poly-alphabétiques
- Nombre de clefs élevés

LES BOMBES DE TURING



La “bombe” d’A. Turing



Alan Turing

La Cryptanalyse

- Analyse fréquentielle
- Attaque par le paradoxe des anniversaires

La Cryptanalyse

- Analyse fréquentielle
- Attaque par le paradoxe des anniversaires
- Cryptanalyse différentielle (Biham, Shamir, 1990)
- Cryptanalyse linéaire (Matsui, 1993)

La Cryptanalyse

- Analyse fréquentielle
- Attaque par le paradoxe des anniversaires
- Cryptanalyse différentielle (Biham, Shamir, 1990)
- Cryptanalyse linéaire (Matsui, 1993)
- Attaques par cube (Dinur, Shamir, 2009)
- Attaques par Invariants (Leander et al., 2011)
- Et bien d'autres !

Défis actuels

- Chiffrements à bas coût
- Chiffrements plus simples
- Comprendre ce que Confusion signifie
- Définir la Sécurité Pratique ?

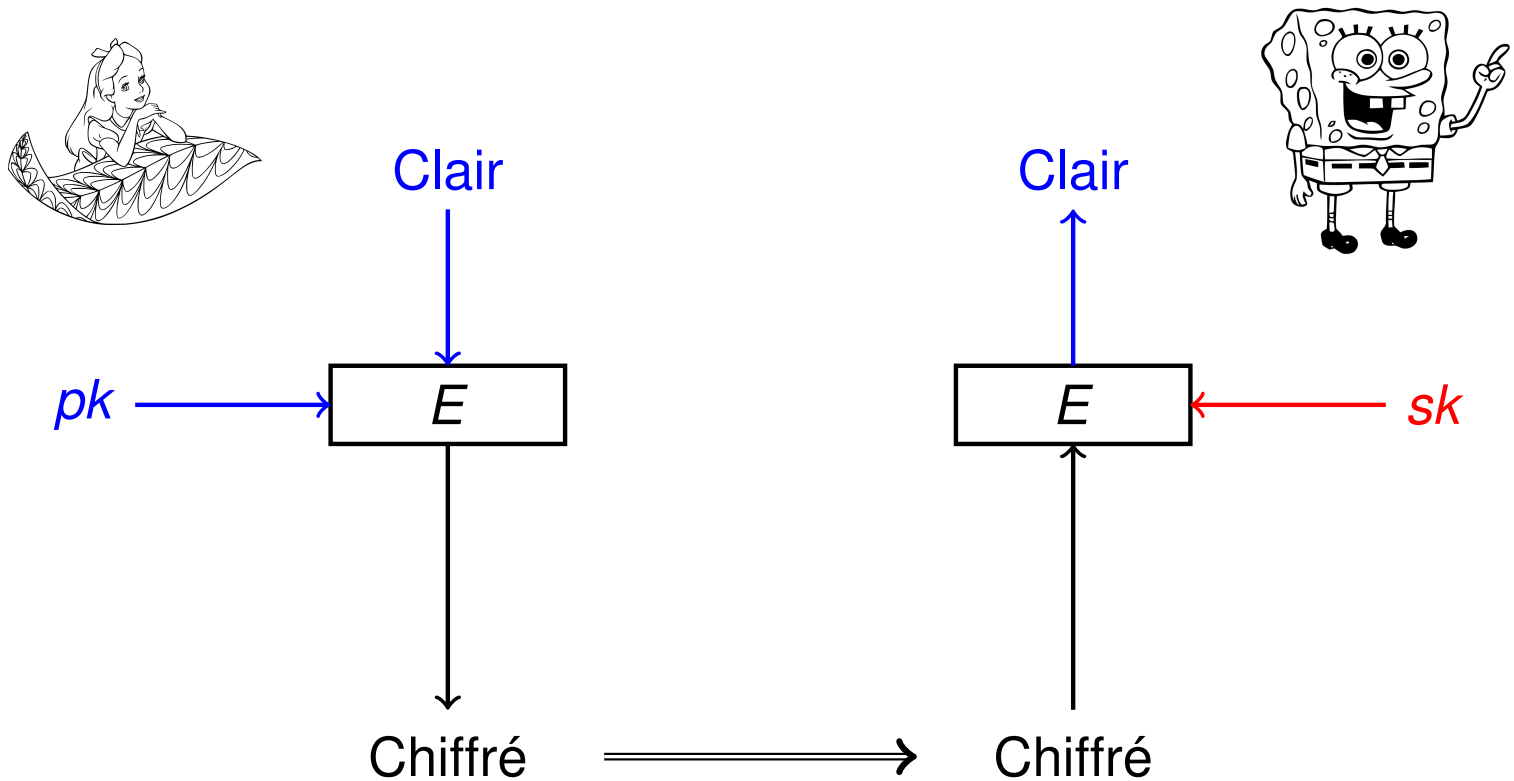
Défis actuels

- Chiffrements à bas coût
- Chiffrements plus simples
- Comprendre ce que Confusion signifie
- Définir la Sécurité Pratique ?

La cryptanalyse est le plus important !

LE PROBLÈME

Chaque utilisateur dispose d'une clef **publique** *pk* et d'une clef **privée** *sk*.



Fonctions à sens unique

$$F : x \mapsto F(x) = y$$

Propriétés

- Connaissant x, il est “facile” de calculer $y = F(x)$.
- Connaissant y, il est “très difficile” de calculer x.

UNE FONCTION À SENS UNIQUE

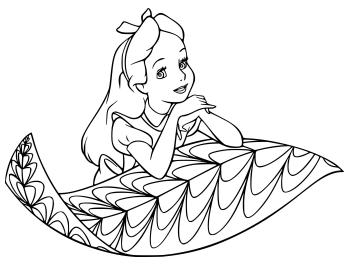
- n, e et x des entiers
- $+$ reste de la division euclidienne

$$F(x) = x^e \mod n$$

ECHANGE DE CLEFS. DIFFIE - HELLMAN (1976)

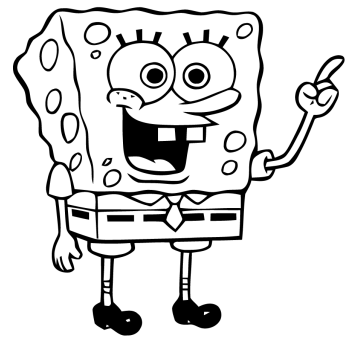
g, n et publics.

a b



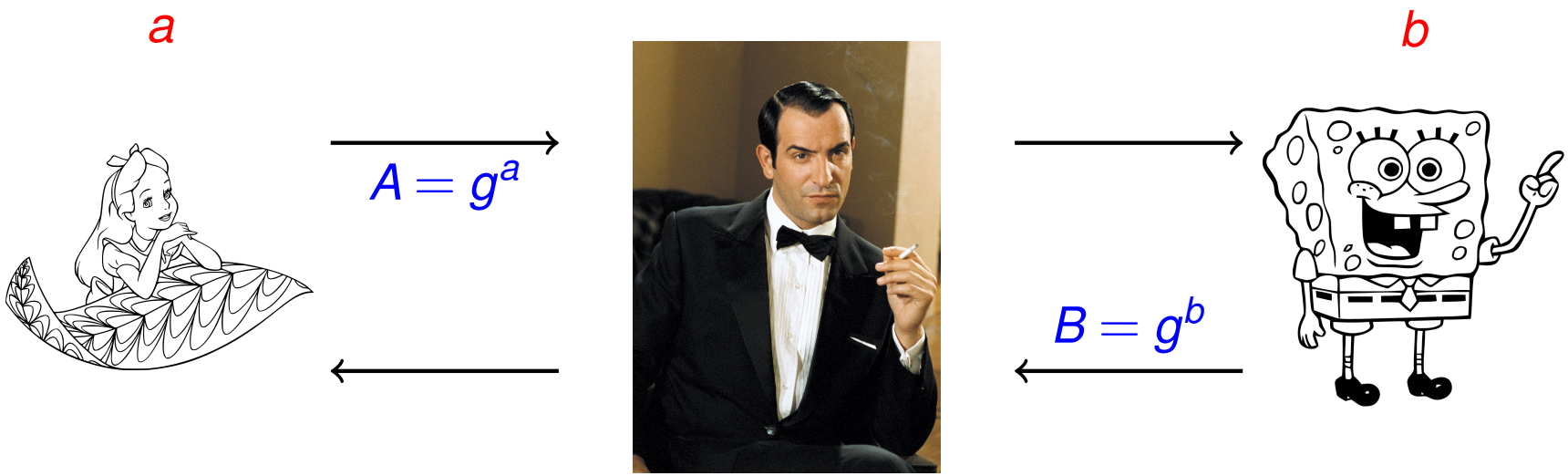
$A = g^a \mod n$

$B = g^b \mod n$

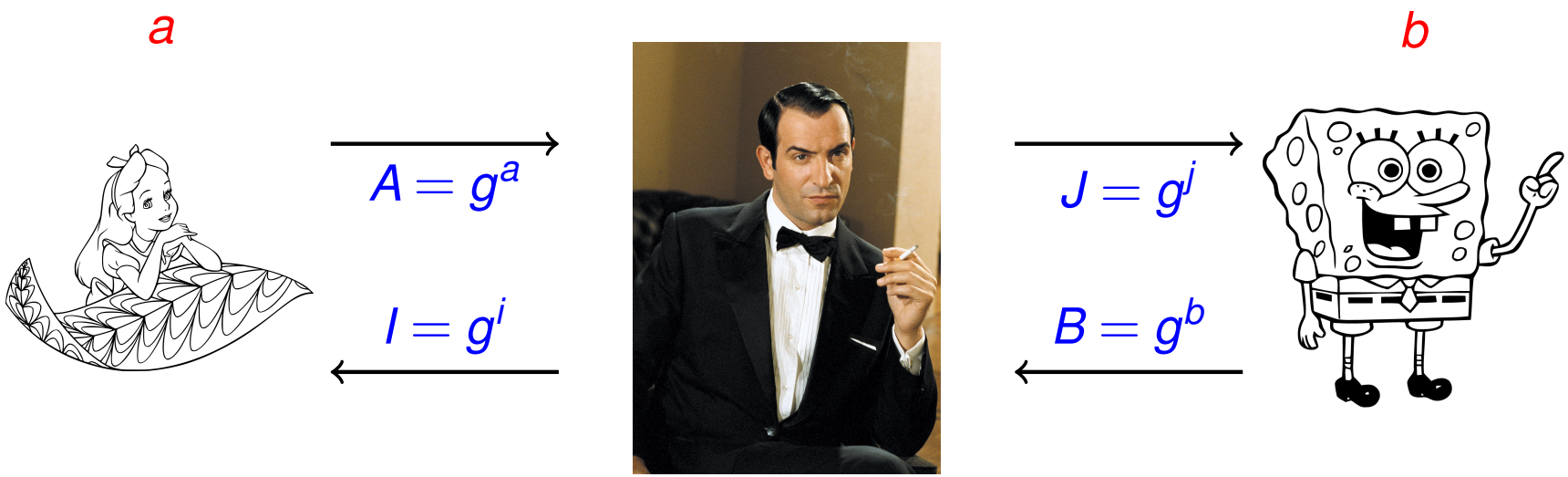


$B^a = g^{ab} \mod n$ $A^b = g^{ab} \mod n$

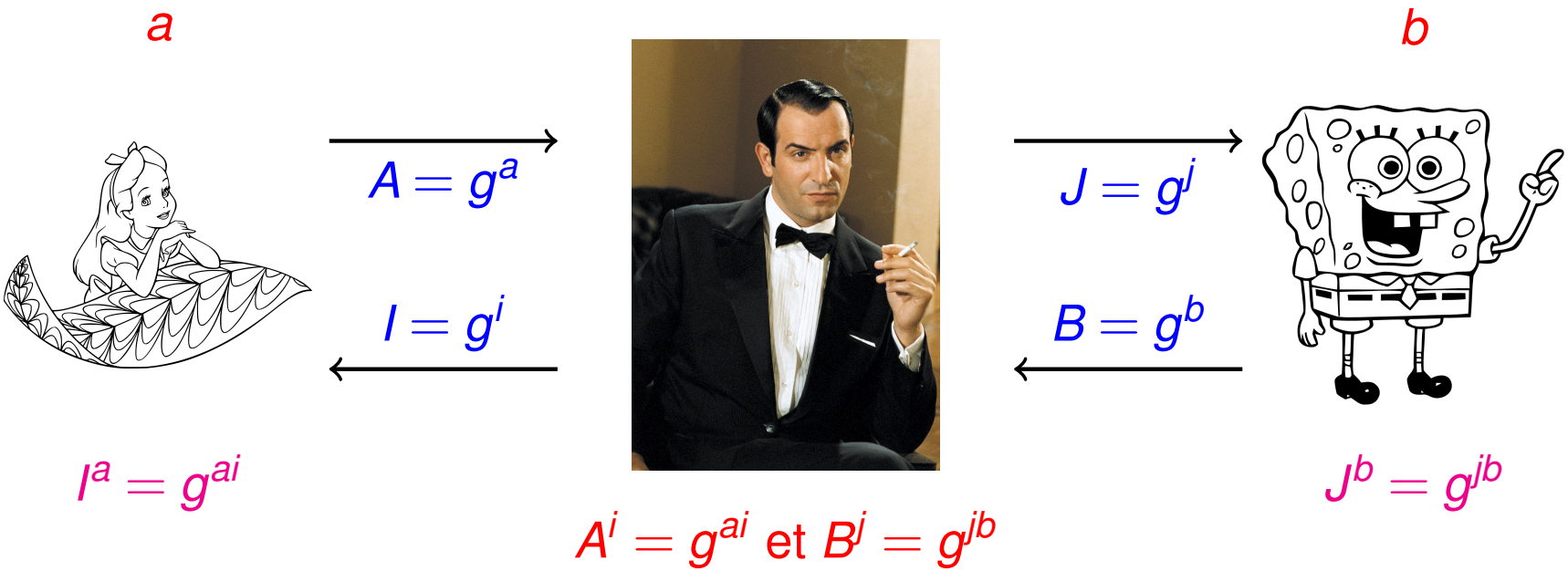
ATTAQUE DE "L'HOMME DU MILIEU"



ATTAQUE DE "L'HOMME DU MILIEU"



ATTAQUE DE "L'HOMME DU MILIEU"



Un chiffrement : El Gamal (1984)

Bob :

- pk clef publique, sk clef privée
- g public
- $pk = g^{sk}$

Chiffrement

Alice choisit r aléatoirement. Puis

$$(m, r) \longrightarrow (m \cdot pk^r, g^r)$$

Un chiffrement : El Gamal (1984)

Bob :

- pk clef publique, sk clef privée
- g public
- $pk = g^{sk}$

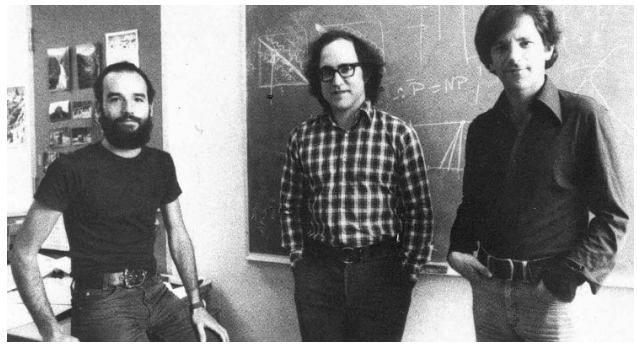
Chiffrement

Alice choisit r aléatoirement. Puis

$$(m, r) \longrightarrow (m \cdot pk^r, g^r)$$

Comment on déchiffre ?

RSA (Rivest, Shamir, Adleman (1977)



Idée

C'est facile de multiplier de nombres. C'est difficile de factoriser un nombre.

- p, q deux nombres premiers (clef privée)
- $n = p \cdot q$ (clef publique)
- e (public)

Chiffrement

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

Enjeux actuels

- La cryptographie Post-Quantique

Enjeux actuels

- La cryptographie Post-Quantique
- Les preuves

Enjeux actuels

- La cryptographie Post-Quantique
- Les preuves
- Les performances

Enjeux actuels

- La cryptographie Post-Quantique
- Les preuves
- Les performances
- La cryptanalyse