# Cryptographie

TRAN-THUONG Tien-Thinh

Lycée Hoche MP*

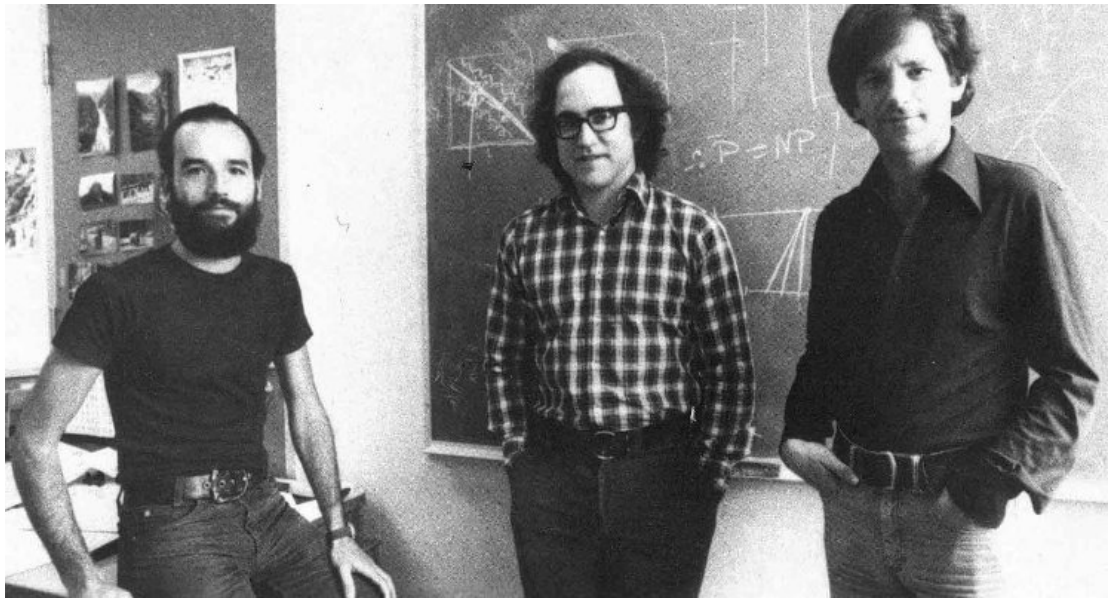
Wednesday 5th January, 2022

# Plan

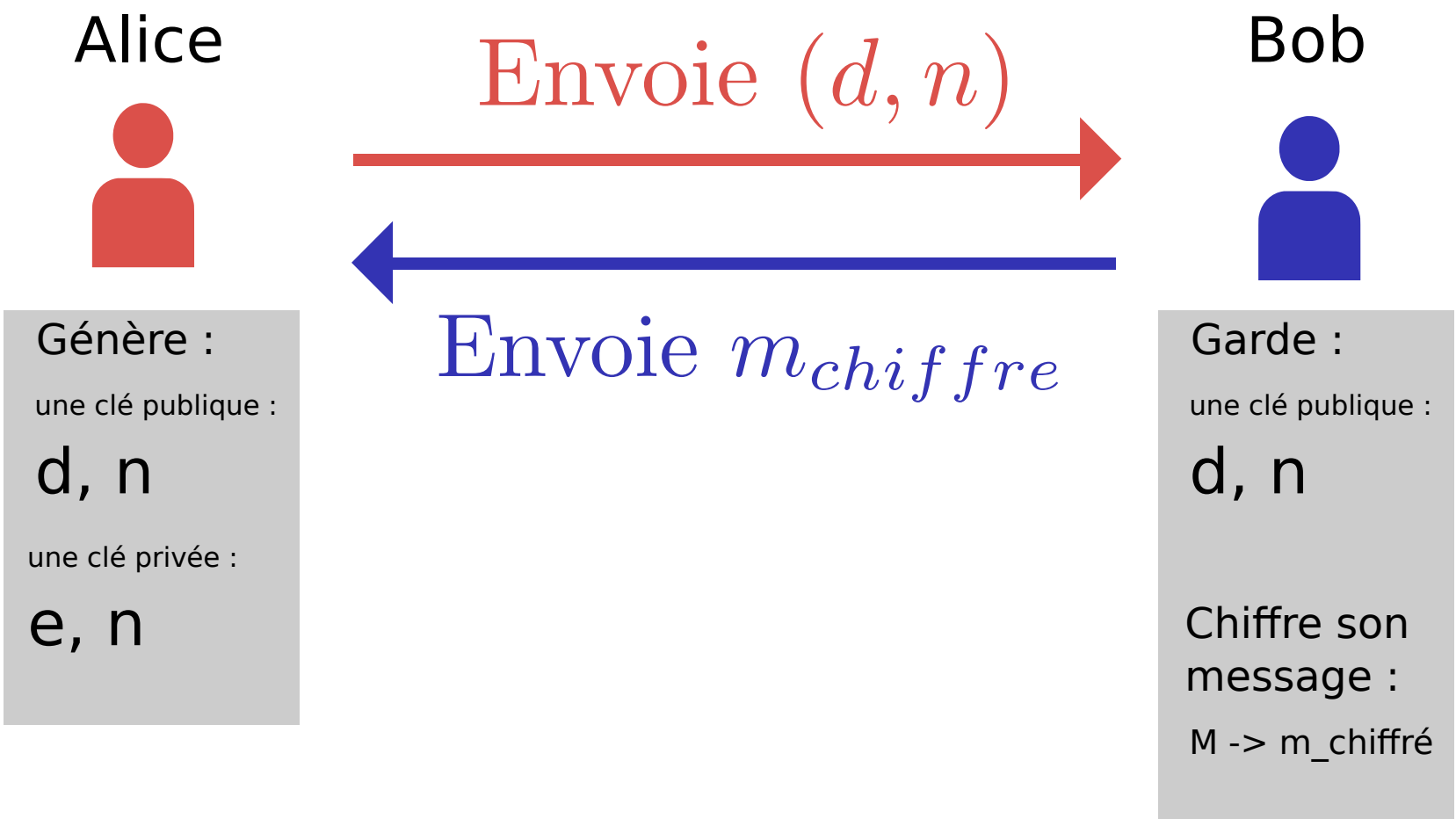
# RSA - présentation

Le chiffrement RSA est un algorithme de cryptographie asymétrique inventé en 1978. Il est nommé par les initiales de ses trois inventeurs:

- Ronald RIVEST
- Adi SHAMIR
- Leonard ADLEMAN



# RSA - clé asymétrique



# RSA - générer les clés

Alice

Bob

Génère :

2 nombres premiers :

p, q

Calcule :

$$n = p \times q$$
$$w = \varphi(n) = (p-1)(q-1)$$

Trouve :

$$e \; tel \; que \; e \wedge \varphi(n) = 1$$
$$d \; tel \; que \; e \times \; d \equiv 1[\varphi(n)]$$

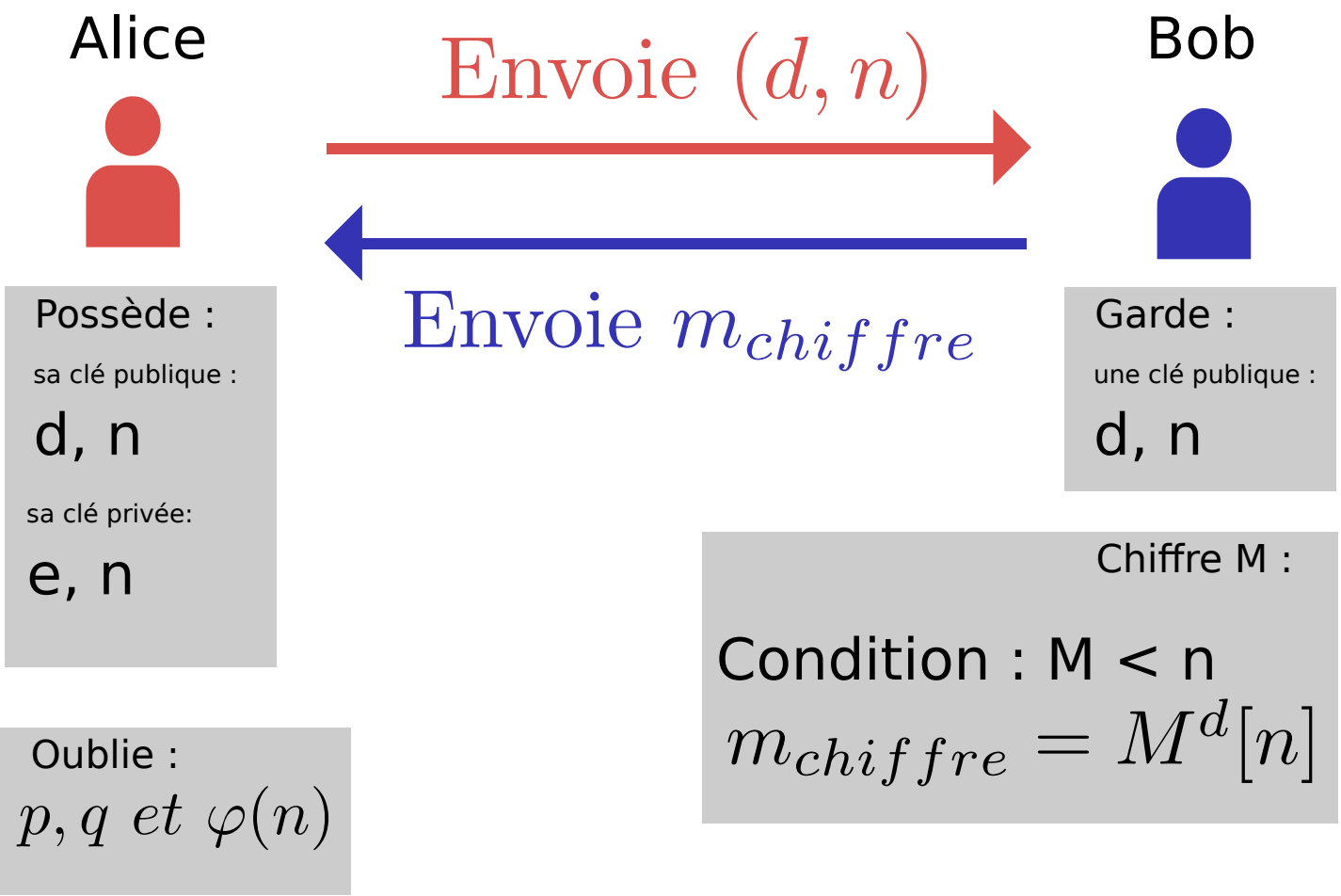
Clé publique :

d, n

Clé privée :

e, n

# RSA - chiffrer un message



# RSA - déchiffrer un message


Possède :

sa clé publique :

d, n

sa clé privée:

e, n

Garde :

une clé publique :

d, n

$m_{chiffre} = M^d[n]$

Déchiffre :

$$M \equiv M^{d \times e}[n]$$

$$M \equiv (m_{chiffre})^e[n]$$

# RSA - démonstration

Montrer que $M^{d\times e} \equiv M[p \times q]$
Revient à démontrer que $M^{d\times e} \equiv M[p]$ et $M^{d\times e} \equiv M[q]$

## Petit Théorème de Fermat

p premier, alors, $\forall a \in N$ non divisible par p, $a^{p-1} \equiv 1[p]$

## Si $M \equiv 0[p]$

$M^{d\times e} \equiv 0 \equiv M[p]$

## Si $M \not\equiv 0[p]$

On sait que $e \times d \equiv 1[\varphi(n)]$ or $\varphi(n) = (p-1)(q-1)$ d'où
$\exists k, e \times d - 1 = k \times (p-1)$

- $M^{d\times e} \equiv M \times M^{d\times e-1} \equiv M \times (M^{p-1})^k \equiv M \times 1^k \equiv M[p]$

De même pour $q$

# RSA - tentative de décryptage du message

Alice

Envoie $m_{chiffre}$

Bob

Possède :

sa clé publique : d, n

sa clé privée: e, n

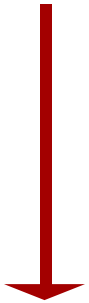
Déchiffre :

$M \equiv (m_{chiffre})^e[n]$

Garde :

une clé publique : d, n

$m_{chiffre} = M^d[n]$



Oscar

*Intercepte* $m_{chiffre}$

Oscar doit retrouver e, en connaissant d et n

$e \times d \equiv 1[\varphi(n)]$

$\varphi(n) = (p-1) \times (q-1)$

Cela revient à factoriser n

# RSA - signature d'un message

Alice

Envoie $m_{chiffre}$ et $hash_{chiffre}$

Bob

Possède :
$publique : d, n$
$privee : e, n$

Garde :
$publique : d, n$
$m_{chiffre}$

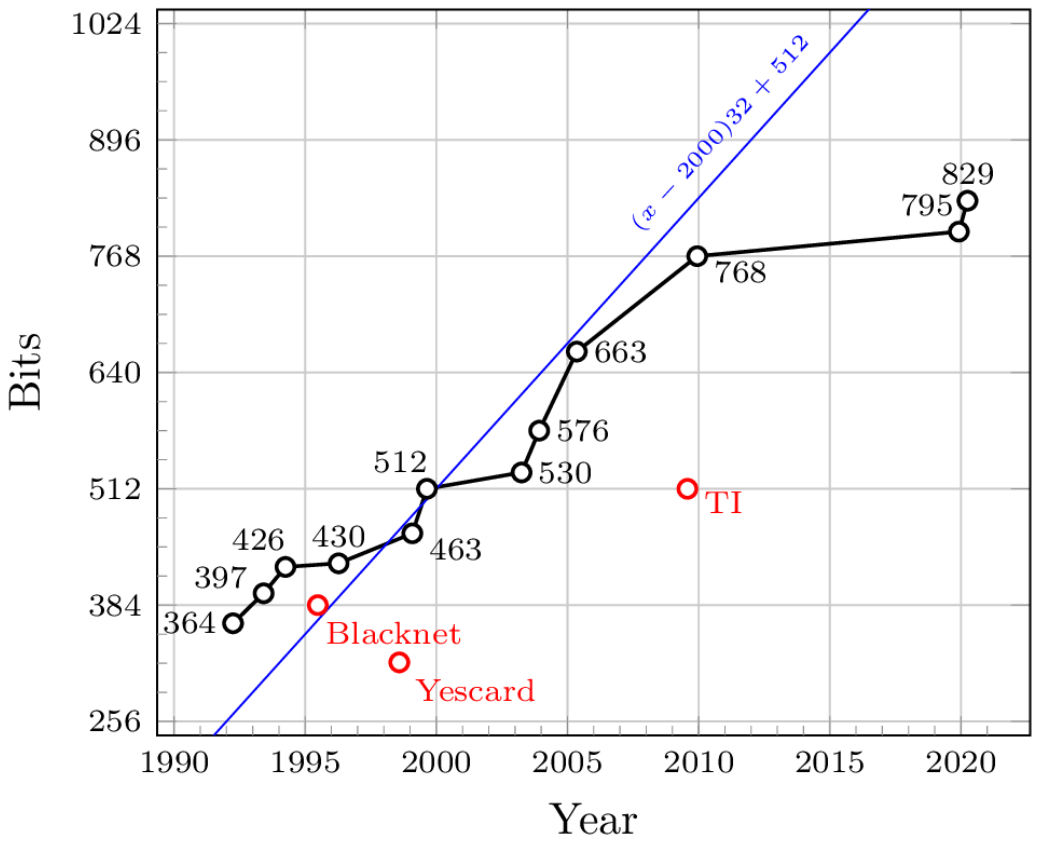
Garde :
$publique : d_{Bob}, n_{Bob}$
$m_{chiffre}$

Possède :
$publique : d_{Bob}, n_{Bob}$
$privee : e_{Bob}, n_{Bob}$

$hash = H(m_{chiffre})$
$hash = (hash_{chiffre})^{d_{Bob}}[n_{Bob}]$

$hash = H(m_{chiffre})$
$hash_{chiffre} = hash^{e_{Bob}}[n_{Bob}]$

# RSA - casser des clés (déduire la clé privée)




Les clés RSA sont, pour le moment, considérées comme sûr lorsqu'elles ont une longueur de 1 024 bits, soit en base 10, des clés d'environ $10^{310}$ .

# D'autres protocoles

D'autres protocoles existent :

- Protocole de partage Diffie-Hellman 1976 (secret commun)
- Chiffrage El Gamal 1984 (cryptographie asymétrique)
- Courbes Elliptiques

# Tests de primalité - déterministe

- Méthode naïve $O(\sqrt{n})$
- Crible d'Erathostène
- AKS Agrawal–Kayal–Saxena 2002 $O(log(n)^{12})$

# Tests de primalité de Fermat - probabiliste

## Petit Théorème de Fermat

p premier, alors, $\forall a \in N$ non divisible par p, $a^{p-1} \equiv 1[p]$

## Test de Fermat $O(k \times log(p))$

Si $n$ est premier alors il passe le test de Fermat pour toute base $a$.
Donc si n passe le test de Fermat pour un grand nombre de base a, il a de grande chance d'être un nombre premier.

## Nombre de Carmichaël

La réciproque du petit théorème de Fermat est faux.
Les nombres de Carmichaël $(561, 1105, 1729, 2465, 2821)$ sont composés pourtant pour tous nombres premiers avec le nombre le petit la congruence est vérifiée.

# Tests de primalité de Miller-Rabin - probabiliste

Une amélioration du test de Fermat.

## $p > 2$ est premier

Alors $\exists\ s, d$ tel que $p - 1 = d \times 2^s$
Ainsi, par théorème de Fermat $a^{p-1} = a^{d \times 2^s} \equiv 1[p]$
Donc p n'est pas premier si il ne vérifie pas $a^d \equiv 1[p]$ ou
$\exists\ k \in [\![0; s-1]\!], a^{d \times 2^k} \equiv -1[p]$

## Probabilité

La probabilité pour qu'un nombre $n$ non premier passe le test est inférieur à $\frac{1}{4}$.
En prenant en compte la probabilité d'un nombre impair d'être premier, on peut démontrer que si n passe k fois le test de Miller-Rabin, la probabilité qu'il soit premier est supérieur à $1 - \frac{1}{4^k}$.