

# Introduction à la cryptographie – Chapitre I

## Systemes à clef publique



25/01/2010

# Plan du cours

- 0. Courte introduction.
- I. Systèmes à clef publique.
- II. Systèmes à clef secrète.
- III. Authentification.
- IV. Exemples.

- 1.1. Quelques notions d'arithmétique.
- 1.2. Le protocole Diffie & Hellman.
- 1.3. Le protocole RSA.
- 1.4. Autres protocoles.
- 1.5. Conclusion.



- 1.1. Quelques notions d'arithmétique.
- 1.2. Le protocole Diffie & Hellman.
- 1.3. Le protocole RSA.
- 1.4. Autres protocoles.
- 1.5. Conclusion.



La présentation des protocoles à clef publique utilise, hélas, beaucoup de calculs arithmétiques. Nous allons revoir quelques définitions sur les nombres premiers et les calculs modulo un entier  $n$ .

- Les nombres dont nous allons parler sont tous des entiers.

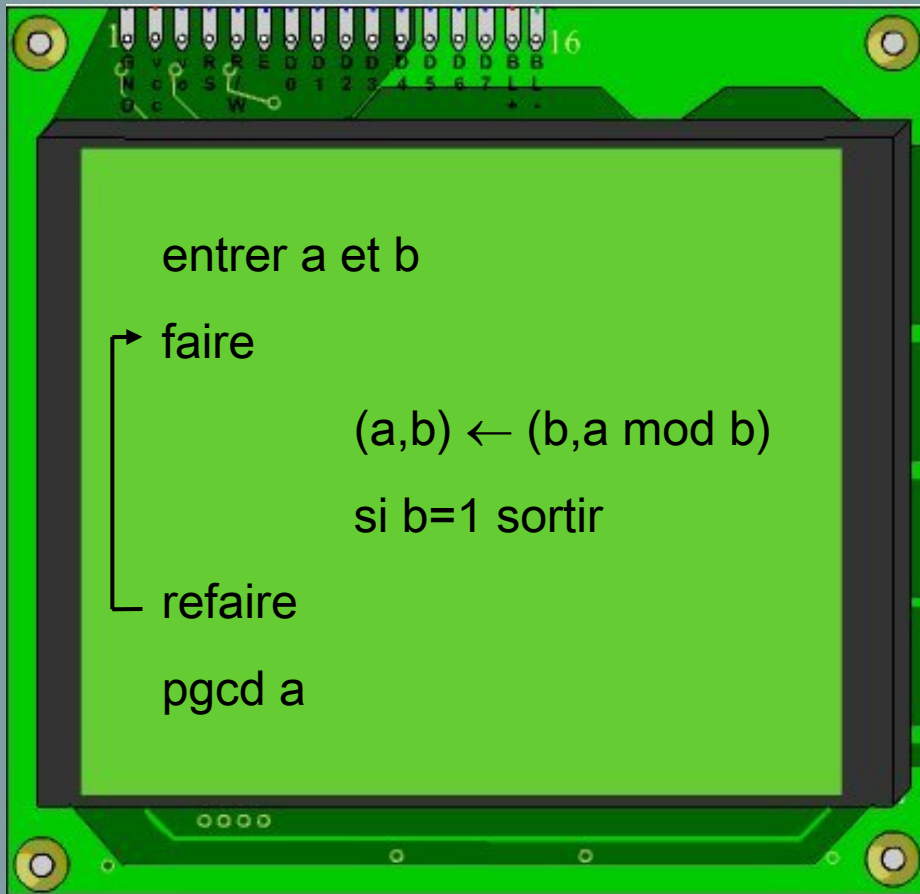
## DÉFINITION 3

|| On dit que  $a$  divise  $b$  et l'on note  $a/b$  s'il existe  $d$  tel que  $b = ad$   
|| On dit alors que  $b$  est un multiple de  $a$ .

- Ex: 3 divise 12 car  $12 = 3 \times 4$
- Le *pgcd* de deux entiers est leur plus grand diviseur commun.
- Ex:  $\text{pgcd}(24, 18) = 6$  car  $24 = 2 \times 2 \times 2 \times 3$  et  $18 = 2 \times 3 \times 3$
- Ex:  $\text{pgcd}(15, 28) = 1$  car  $15 = 3 \times 5$  et  $28 = 2 \times 2 \times 7$

- Lorsque le pgcd de deux nombres est égal à 1, on dit qu'ils sont **premiers entre eux**.
- Pour calculer le pgcd de deux nombres, on utilise l'algorithme d'Euclide. Vous l'utilisez aussi lorsque vous faites une division euclidienne.
- Cet algorithme a plus de 2500 ans et est déjà présent dans les éléments d'Euclide. Les historiens pensent qu'il antérieur de 200 ans à Euclide. C'est sans doute le plus vieil algorithme informatique connu au monde.

$$\begin{array}{r|l} 250 & 3 \\ 10 & \\ \hline 1 & 83 \end{array}$$





```
void euclide (int a,int b,int u,int v,int d)
{
    int u1=1,v1=0,d1=a,u2=0,v2=1,d2=b,u3,v3,d3,q;
    while(d2!=0)
    {
        q=d1/d2;
        u3=u1-u2*q;v3=v1-v2*q;d3=d1-d2*q;
        u1=u2;v1=v2;d1=d2;
        u2=u3;v2=v3;d2=d3;
    }
    u=u1;v=v1;d=d1
}
```

## DÉFINITION 5

|| Un nombre est premier s'il est supérieur à 1 et si ses seuls diviseurs sont 1 et lui-même.

- Exemples: **2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59,**
- Les nombres premiers vont en se raréfiant (rapport avec la conjecture de Riemann), mais il en existe quand même une infinité.
- Le théorème fondamental de l'arithmétique dit que:  
**Tout nombre entier se décompose de façon unique en produit de facteurs premiers.**
- Exemples:

$$12 = 2^2 \times 3^1$$

$$4200 = 2^3 \times 3^1 \times 5^2 \times 7^1$$

$$175 = 2^0 \times 3^0 \times 5^2 \times 7^1$$

- Pour un entier  $n$ , la fonction  $\Phi(n)$  calcule le nombre d'entiers inférieurs à  $n$  et premiers avec  $n$ . Autrement dit,

## DÉFINITION 6

$$\left\| \begin{array}{l} \Phi(n) = \text{Card}\{k / 1 \leq k < n \text{ et } \text{pgcd}(k, n) = 1\} \\ \Phi(1) = 1 \end{array} \right.$$

$k$	1	2	3	4	5	6	7	8	9
$\Phi(k)$	1	1	2	2	4	2	6	4	6

- De façon générale, on calcule  $\Phi(n)$  à partir de la décomposition en facteurs premiers de  $n$ .

Afin de pouvoir exposer l'algorithme de la méthode RSA, nous aurons juste besoin de connaître les deux propriétés suivantes :

- Si  $p$  est un nombre premier,  $\Phi(p) = p - 1$

- $\text{pgcd}(m, n) = 1 \Rightarrow \Phi(m \times n) = \Phi(m) \times \Phi(n)$

- Exemple:

$$\Phi(77) = \Phi(7)\Phi(11) = 6 \times 10 = 60$$

- On dit que deux entiers sont égaux *modulo*  $n$  si  $n$  divise leur différence :

$$a \equiv b \pmod{n} \iff n \mid (b - a) \iff \exists k \in \mathbb{N} / a = b + k \times n$$

$b$  est appelé résidu de  $a$  modulo  $n$

- Exemples :

$$19 \equiv 7 \pmod{12} \text{ car } 19 = 7 + 1 \times 12$$

$$4 \equiv 14 \pmod{5} \text{ car } 14 = 4 + 2 \times 5$$

- En particulier :

$$a \equiv 0 \pmod{n} \text{ ssi } a \text{ est un multiple de } n$$

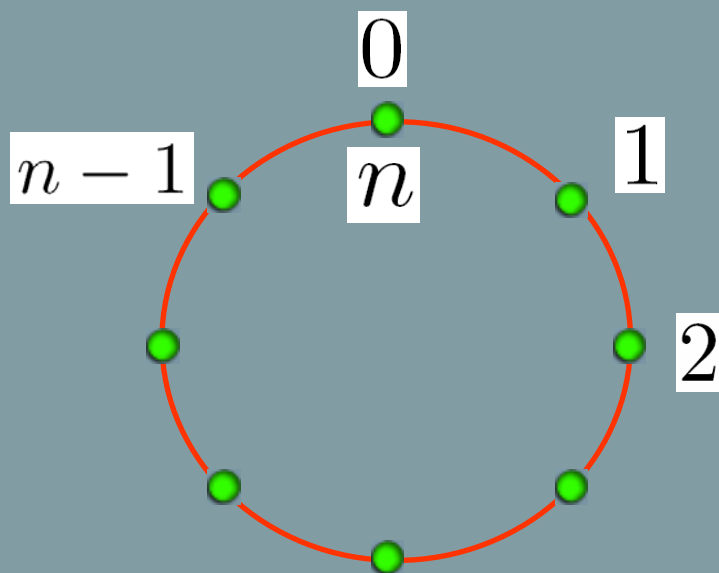
- Exemple:

$$36 \equiv 0 \pmod{12} \text{ car } 36 = 3 \times 12$$

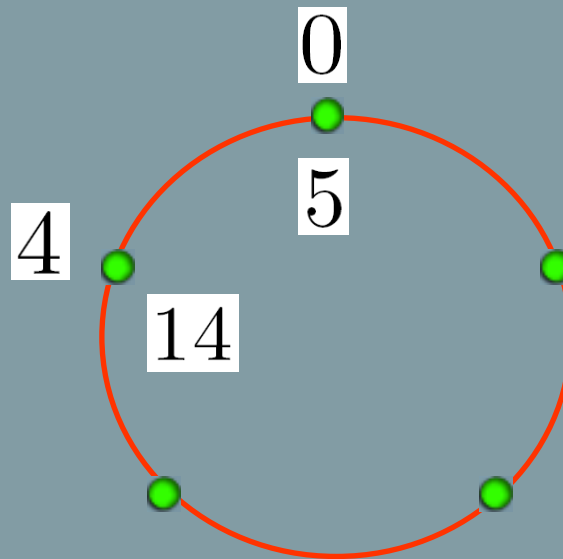
- Calculer *modulo*  $n$  revient à ne considérer que le reste d'un entier dans la division par  $n$  :

$$4 \equiv 14 \pmod{5} \text{ car } 14 = 4 + 2 \times 5$$

- Travailler modulo  $n$  revient à travailler sur un cercle de  $n$  points régulièrement espacés. Lorsque l'on a fait un tour complet, on revient en  $0$  :



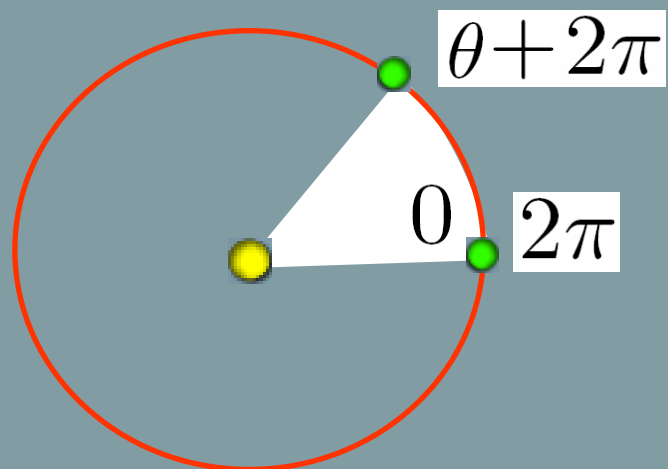
- $4 \equiv 14 \pmod{5}$  car  $14 = 4 + 2 \times 5$



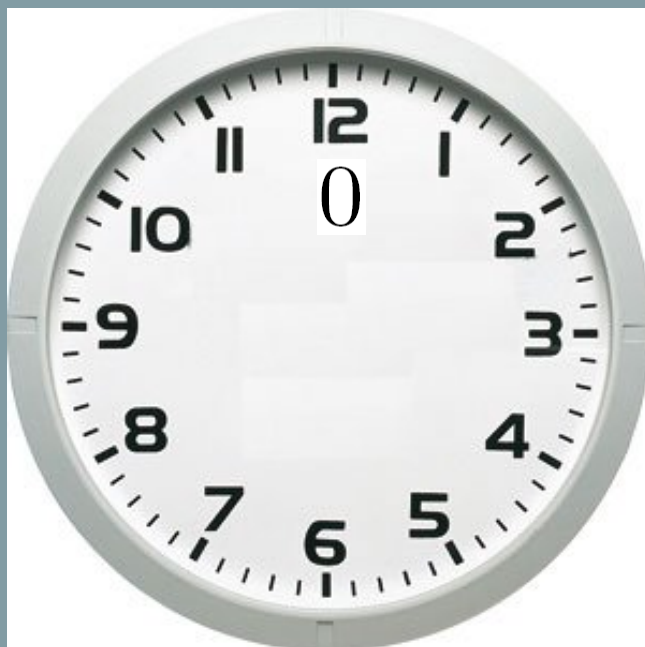
25/01/2010



- Finalement vous savez déjà travailler modulo  $n$  : Les calculs trigonométriques (*Deux Souvenirs*) se font modulo  $2\pi$ .



- Et puis vous savez aussi lire l'heure : Les calculs horaires se font modulo *12*.



25/01/2010

- Exemple de calcul :

$$(9 + 11) \bmod 7 = 20 \bmod 7 = 6 \bmod 7$$

ou

$$(9 + 11) \bmod 7 = (2 + 4) \bmod 7 = 6$$

- Autre Exemple :

$$(9 \times 11) \bmod 7 = 99 \bmod 7 = (14 \times 7 + 1) \bmod 7 = 1 \bmod 7$$

ou

$$(9 \times 11) \bmod 7 = (2 \times 4) \bmod 7 = 1 \bmod 7$$

- *Un élément  $a$  est inversible modulo  $n$  s'il existe  $b$  tel que  $ab \equiv 1 \pmod{n}$*

- Exemple :

$$(9 \times 11) \pmod{7} = (2 \times 4) \pmod{7} = 1 \pmod{7}$$

- Autre exemple :

$$3 \times 2 = 6 \equiv 1 \pmod{5}$$

- Mais modulo  $4$ ,  $2$  n'a pas d'inverse... En fait,

$$a \text{ est inversible modulo } n \text{ ssi } \text{pgcd}(a, n) = 1$$

## THÉORÈME (PETIT THÉORÈME DE FERMAT)

||| *Si  $p$  est un nombre premier et  $a$  non multiple de  $p$ ,*  
|||  $a^{p-1} \equiv 1 \pmod{p}$

- Exemple :  $2^4 \equiv 1 \pmod{5}$

## THÉORÈME (THÉORÈME DE FERMAT-EULER)

|| Si  $\text{pgcd}(a, n) = 1$ , on a  $a^{\Phi(n)} \equiv 1 \pmod{n}$

- Qui sert à calculer l'inverse modulo  $n$  :

$$a \times a^{\Phi(n)-1} \equiv 1 \pmod{n}$$

- On peut calculer très efficacement les puissances modulo  $n$  :

$$a^x \pmod{p}$$

$x$	1	2	3	4	5	6
$3^x$	3	9	27	81	243	729
$3^x \pmod{7}$	3	2	6	4	5	1

- $3^{1234567890} \pmod{7826348737} = 7590405247$

- Le calcul par ordinateur se fait (rapidement) grâce à la « squaring method »

- L'opération inverse est par contre très difficile à réaliser (problème du logarithme discret).

- Connaissant  $f(x) = a^x \pmod p$  il faut retrouver  $x$

$x$	1	2	3	4	5	6
$3^x$	3	9	27	81	243	729
$3^x \pmod 7$	3	2	6	4	5	1

- $3^{1234567890} \pmod{7826348737} = 7590405247$



- 1.1. Quelques notions d'arithmétique.
- 1.2. Le protocole Diffie & Hellman.
- 1.3. Le protocole RSA.
- 1.4. Autres protocoles.
- 1.5. Conclusion.


$$\begin{aligned} & (y f(x) + 40) y_1 + e_2(x) y_2 + e_3(x) y_3 \\ (x+1) & = \left( \frac{x(x-2)}{2} \right) 1 + (x(x-1)) 0 + \left( \frac{x(x-1)}{2} \right) \\ & = \left( \frac{x-1}{2} \right) 1 + (x(x-1)) 0 + \left( \frac{x(x-1)}{2} \right) \\ & (y + 6x + 7)^4 (y + 7x + 8)^4 (y + 9x + 6)^4 (y + 8x + 7)^4 \\ & 1) (x+6)^4 (x+9)^4 \quad x(x+6)^4 (x+2)^4 \\ & -9b + \sqrt{3} \sqrt{4a^3 + 27b^2} / 3 \quad 6x)^2 (y + 10x + 11) x + 1 \\ & \frac{2^{11} 3^{2/3}}{x(x+6)^2} \quad (y+9x+ \\ & \frac{(y+8x)^2}{(1-i\sqrt{3})(-9b + \sqrt{3} \sqrt{4a^3 + 27b^2})^{1/3}} \quad (y+8x+ \\ & \frac{1/3}{(y+8x)^2 (y+7x+4)^4 (y+} \end{aligned}$$

## 1.2. Le protocole Diffie & Hellman.

- Whitfield Diffie, Martin Hellman et Ralph Merkle se rencontrent en 1974 à Stanford.
- Leurs recherches portent sur le problème de la **distribution des clefs** en cryptographie.



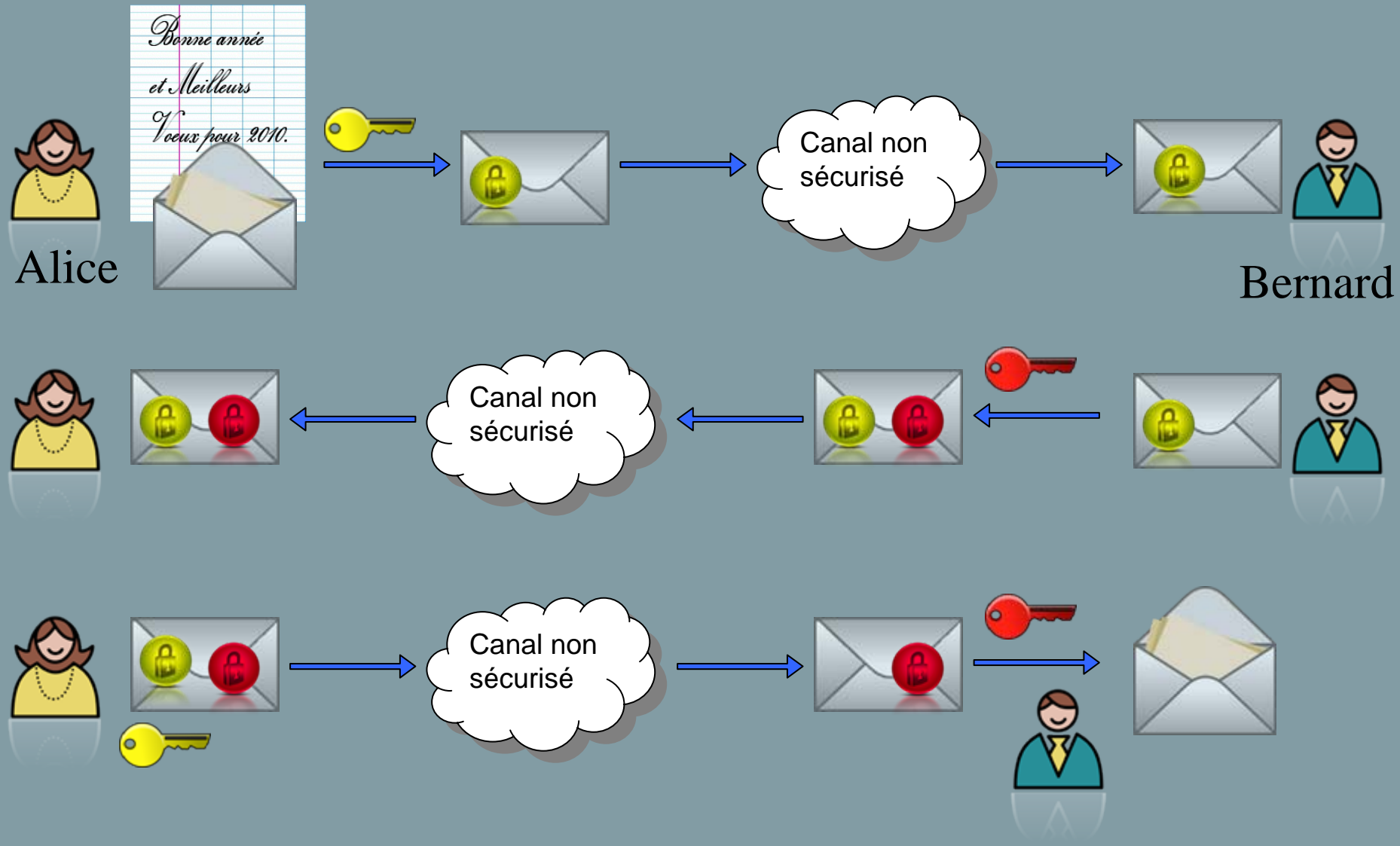
25/01/2010

- Question fondamentale :  
Est-il possible de trouver un système cryptographique dans lequel aucun échange de clef entre l'expéditeur (Alice) et le destinataire (Bernard) ne serait nécessaire ?



25/01/2010

# Première piste : l'idée du double cadenas.



25/01/2010

28



- Une fonction à sens unique est facile à calculer, mais sa réciproque est très difficile à exprimer.



25/01/2010

29



- Mathématiquement, que peut être une fonction à sens unique ?
- Diffie et Hellman ont l'idée d'utiliser l'arithmétique modulaire : on a vu qu'il était très facile d'élever un entier à une certaine puissance, modulo un autre entier.
- L'opération inverse s'appelle le calcul d'un **logarithme discret**. C'est une opération très difficile (c-à-d très longue) à effectuer, même avec un ordinateur, pour peu que les nombres en jeu soient « grands ».

- On choisit deux nombres  $a$  et  $p$ .
- La fonction à sens unique est :

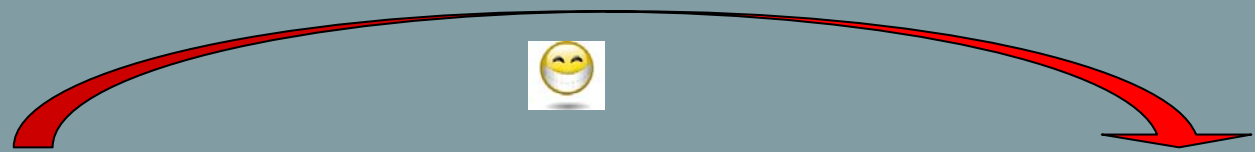
$$f(x) = a^x \pmod{p}$$

- Sa réciproque est :

$$f^{-1}(y) = x$$



$x$	1	2	3	4	5	6
$3^x$	3	9	27	81	243	729
$3^x \bmod 7$	3	2	6	4	5	1



$$3^{1234567890} \bmod 7826348737 = 7590405247$$





- Alice et Bernard choisissent un nombre premier  $p$ , très grand, et un nombre  $a$  premier avec  $p$ .
- $a$  et  $p$  forment la partie publique de leur clef.
- Alice choisit un nombre  $x$  compris entre  $1$  et  $p-1$  qui forme la partie privée de sa clef.
- Bernard choisit un nombre  $y$  compris entre  $1$  et  $p-1$  qui forme la partie privée de sa clef.



- Alice calcule :  $b = a^x \pmod{p}$

- Bernard calcule :  $c = a^y \pmod{p}$



$x$

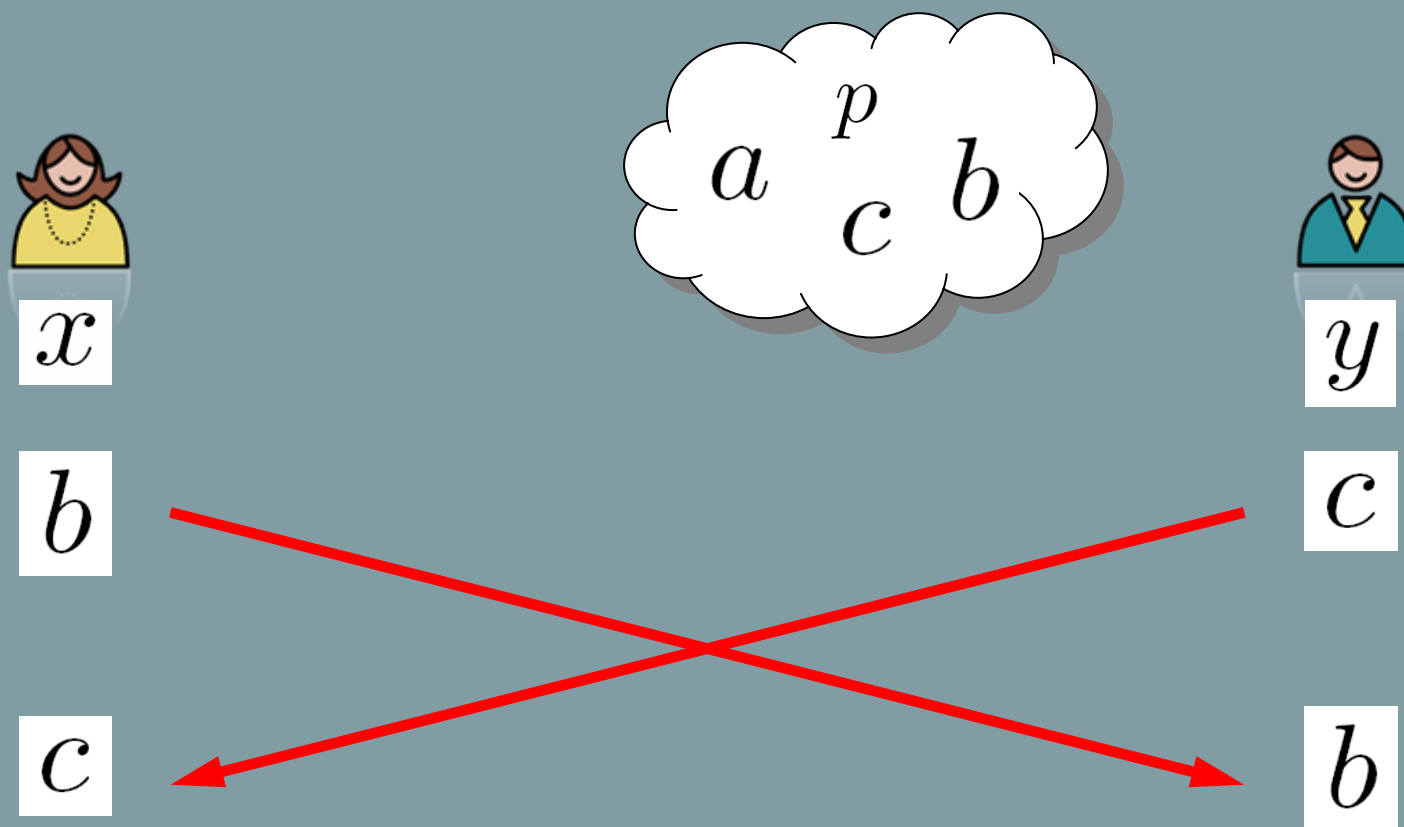
$b$



$y$

$c$

- Alice et Bernard s'échangent  $b$  et  $c$



25/01/2010

35



- Alice calcule :  $c^x \pmod p$
- Bernard calcule :  $b^y \pmod p$

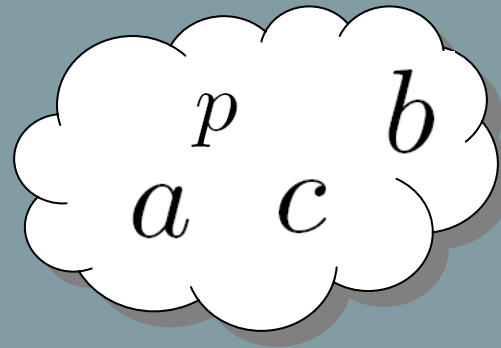


$x$

$b$

$c$

$c^x \pmod p$



$y$

$c$

$b$

$b^y \pmod p$

- $b^y \pmod p = (a^x)^y \pmod p = a^{xy} \pmod p = k$
- $a^x \pmod p = (a^y)^x \pmod p = a^{yx} \pmod p = k$



$x$

$b$

$c$

$$c^x \pmod p =$$

$$= k =$$

$$b^y \pmod p$$

Finalemment,  $k$  est une valeur secrète partagée par Alice et Bernard, sans qu'ils aient eu besoin de se rencontrer.



$y$

$c$

$b$

- Exemple :

Sont publics :

$$p = 17$$

$$a = 3$$

$$b \quad c$$



$$x = 6$$

$$b = 3^6 \pmod{17} = 15$$

$$k = 8^6 \pmod{17} = 4$$



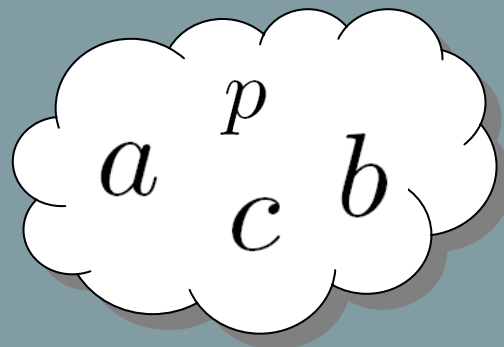
$$y = 10$$

$$c = 3^{10} \pmod{17} = 8$$

$$k = 15^{10} \pmod{17} = 4$$

- Connaissant  $a$   $p$   $b$   $c$

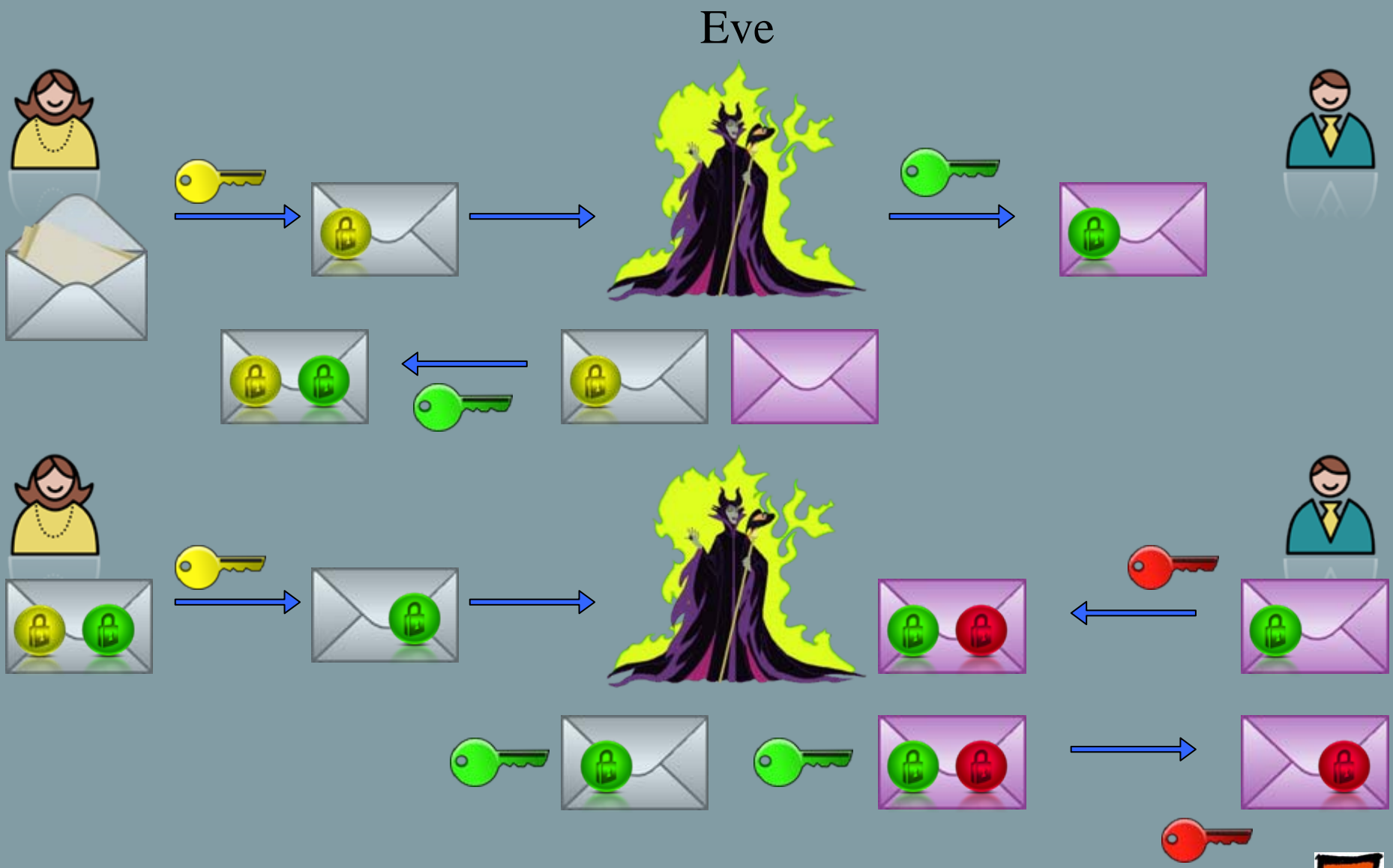
on ne peut pas en déduire  $k$  car le calcul d'un logarithme discret est impossible si  $p$  est très grand.



- L'article de Diffie & Hellman paraît en 1976. C'est le premier protocole utilisant la notion de clef publique et clef privée.
- C'est un protocole d'échange de clefs. Une fois qu'Alice et Bernard partagent la même clef secrète, ils peuvent chiffrer leur message avec n'importe quel algorithme à clef secrète.
- Ce protocole ne permet pas d'assurer l'authentification et le non-désavoeu, comme le montre l'attaque « man in the middle ».



# L'attaque « man in the middle ».



25/01/2010

41



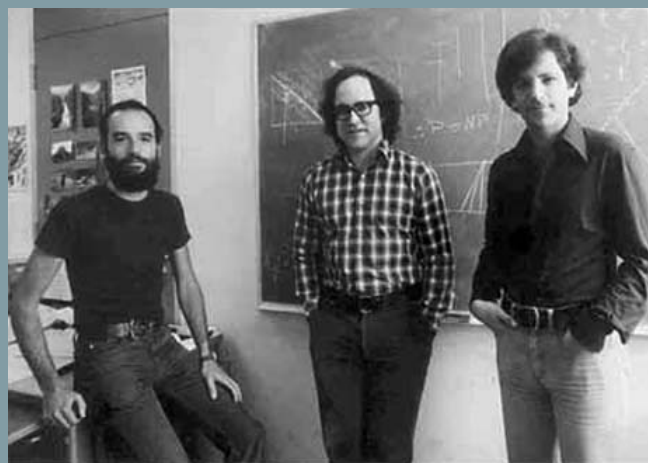
- 1.1. Quelques notions d'arithmétique.
- 1.2. Le protocole Diffie & Hellman.
- 1.3. Le protocole RSA.
- 1.4. Autres protocoles.
- 1.5. Conclusion.



The image shows a large black padlock in the center, symbolizing security or encryption. The background is filled with various mathematical formulas, including polynomials, fractions, and square roots, representing the underlying mathematics of public key cryptography.

## 1.3. Le protocole RSA.

- En 1977, **Ronald Rivest**, **Adi Shamir** et **Leonard Adleman** travaillent ensemble au MIT de Boston sur le protocole de Diffie et Hellman.
- Le système **RSA** va être le premier système de chiffrement à clef publique permettant en même temps la confidentialité, l'authentification et le non-désavoeu.



25/01/2010

- La fonction à sens unique qu'ils découvrent repose sur la difficulté de la factorisation des grands nombres premiers.
- Il est très facile de multiplier deux grands nombres premiers (même à la main). Moins d'une seconde suffit à un PC pour calculer le produit de deux nombres de plusieurs milliers de bits.

$$p = 28934793874928374982374984331$$

$$q = 109038493824092387983749872399$$

$$n = p \times q$$

$n = 3155006343232763871224373627959492603597202806590874380069$

- Fonction à sens unique qu'ils découvrent repose sur la difficulté de la factorisation des grands nombres premiers.
- Il est très facile de multiplier deux grands nombres premiers (même à la main). Moins d'une seconde suffit à un PC pour calculer le produit de deux nombres de plusieurs milliers de bits.

$$p = 2893479387492837498235974984331$$

$$q = 10903849382409238798374923399$$

$$n = p \times q$$

- Et encore, ce sont de petits nombres...
- La taille d'un nombre se mesure en bits. Le nombre de bits nécessaire pour écrire un nombre décimal  $n$  est égal à :

$$\lfloor \log_2 n \rfloor + 1$$

- $p = 28934793874928374982374984331$  95 bits

- $q = 109038493824092387983749872$  97 bits

- $n = 315500634323276387122437362795$   
 $9492603597202806590874380069$  192 bits

- Les plus petites clefs RSA font actuellement 768 bits

- Maintenant, ne connaissant que  $n$ , il est impossible de retrouver  $p$  et  $q$ . C'est la fonction à sens unique.
- Martin Gardner, dans sa rubrique jeux mathématiques de la revue « pour la science », écrit en août 1977 « **New kind of cipher that would take millions of years to break** ». Le nombre suivant est le produit de deux entiers. Lesquels ?

$n = 114381625757888867669235779976$   
 $14661201021829672124236256256184293$   
 $57069352457338978305971235639587050$   
 $58989075147599290026879543541$

100 \$

- 16 ans plus tard, en avril 1994, Leyland, Graff et Atkins...

$$p = 349052951084765094914784961990$$
$$3898133417764638493387843990820577$$
$$q = 327691329932667095499619881908$$
$$34461413177642967992942539798288533$$

- 600 volontaires participèrent au calcul en formant un cluster d'ordinateurs via internet.
- Taille de  $n = p \times q$  **129 bits**



- Alice et Bernard vont chacun construire une clef en deux parties. Nous nous intéressons pour l'instant à Alice.
- Alice choisit deux (très) grands nombres premiers :  $p$   $q$
- Alice calcule  $n = p \times q$



$p$   $q$

$$n = p \times q$$



- Alice calcule  $\phi(n) = (p - 1)(q - 1)$
- Alice choisit un nombre  $e$  premier avec  $\phi(n)$
- Alice calcule  $d = e^{-1} \text{ mod } \phi(n)$



$p$   $q$

$$n = p \times q$$

$$\phi(n) = (p - 1)(q - 1)$$

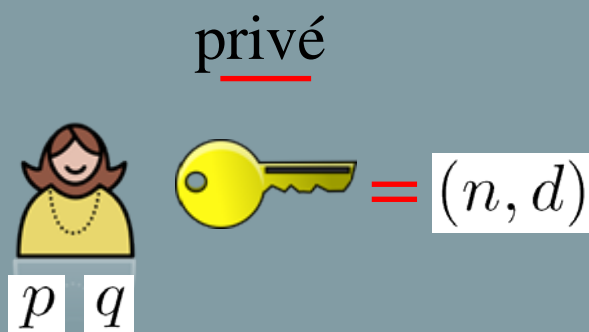
$e$

$$d = e^{-1} \text{ mod } \phi(n)$$

Canal non  
sécurisé



- Alice détruit  $p$   $q$
- Sa clef privée sera le couple  $(n, d)$
- Sa clef publique sera le couple  $(n, e)$

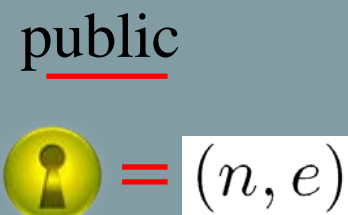




$$n = p \times q$$

$$\phi(n) = (p - 1)(q - 1)$$

$e$

$$d = e^{-1} \text{ mod } \phi(n)$$




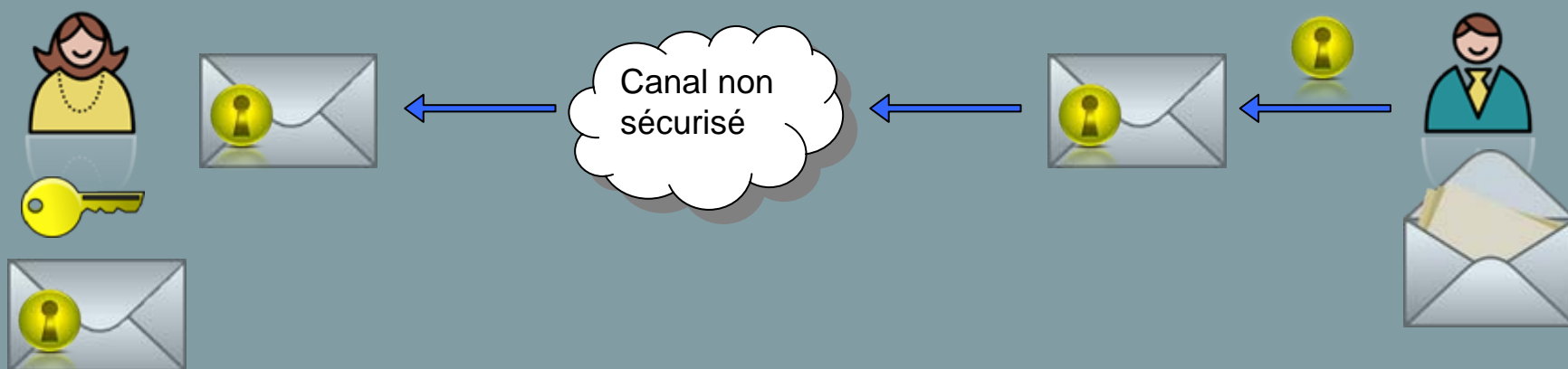
- Alice possède une clef en deux parties :
- La partie privée   $(n, d)$  (c'est la clef de sa boîte aux lettres)
- La partie publique   $(n, e)$  (c'est son adresse)



Canal non sécurisé

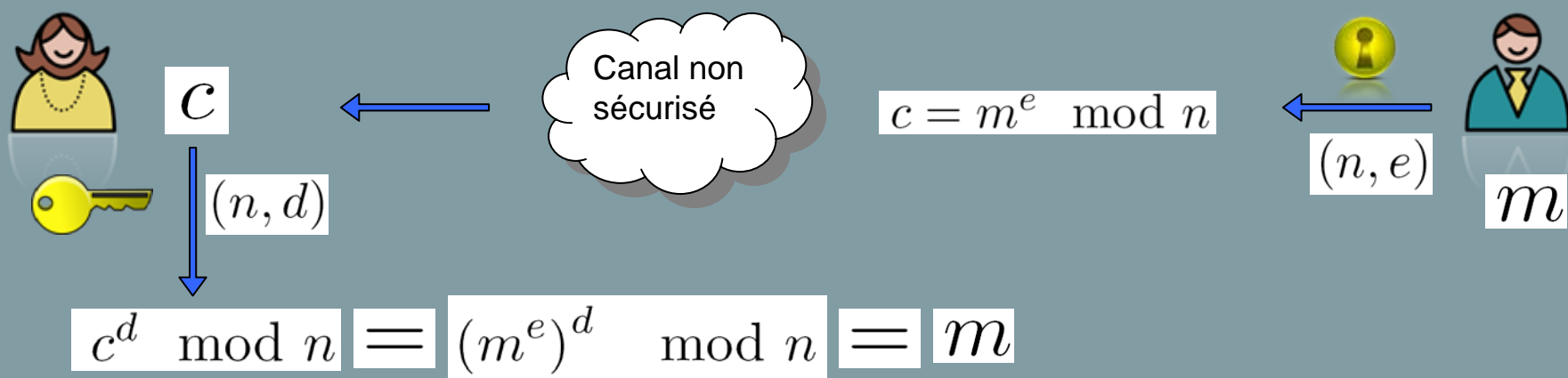


- Bernard veut envoyer un message à Alice.
- Il récupère sa clef publique sur un annuaire. 
- Il chiffre son message avec.
- Alice est la seule à posséder la clef privée correspondante.



- Bernard chiffre le message  $m$  en calculant  $c = m^e \pmod n$
- Alice déchiffre le message  $c$  en calculant  $c^d \pmod n$
- Oui mais :

$$c^d \pmod n = (m^e)^d \pmod n = m^{e \times d} \pmod n = m$$



$$c^d \pmod n = (m^e)^d \pmod n = m^{e \times d} \pmod n = m$$

$$\begin{aligned} m^{ed} &\equiv m^{1+k \times \phi(n)} \\ &\equiv m \times m^{k \times \phi(n)} \\ &\equiv m \times (m^k)^{\phi(n)} \\ &\equiv m \end{aligned}$$

car  $d = e^{-1} \pmod{\phi(n)}$

$$\iff ed = 1 \pmod{\phi(n)}$$

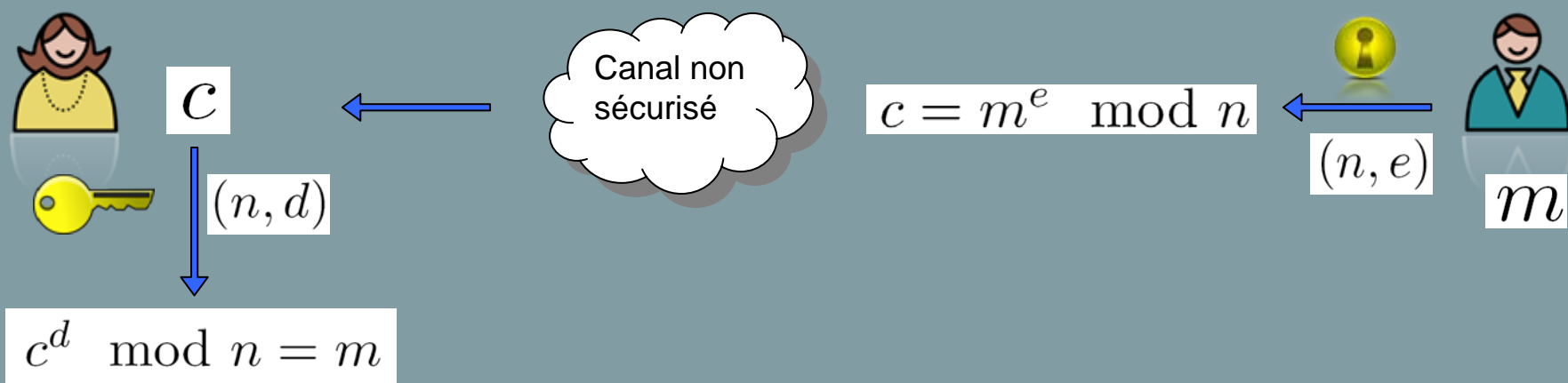
$$\iff ed = 1 + k \times \phi(n)$$

Théorème de Fermat

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

- Bernard chiffre le message  $m$  en calculant  $c = m^e \pmod n$
- Alice déchiffre le message  $c$  en calculant  $c^d \pmod n$
- Oui mais :

$$c^d \pmod n = (m^e)^d \pmod n = m^{e \times d} \pmod n = m$$





## Exemple simple.



$$p = 11047 \quad q = 19501$$

$$n = p \times q = 215427547$$

$$\phi(n) = (p - 1) \times (q - 1) = 215397000$$

$$e = 65537$$



$$d = 65537^{-1} \pmod{215397000} \quad d = 160194473$$



- Bernard veut chiffrer « **BON** » dont le tableau des codes ascii est [66,78,79]. Il le transforme en nombre :

$$x = 78 + 79 \times 128 + 66 \times 128^2 \quad x = 1091534$$

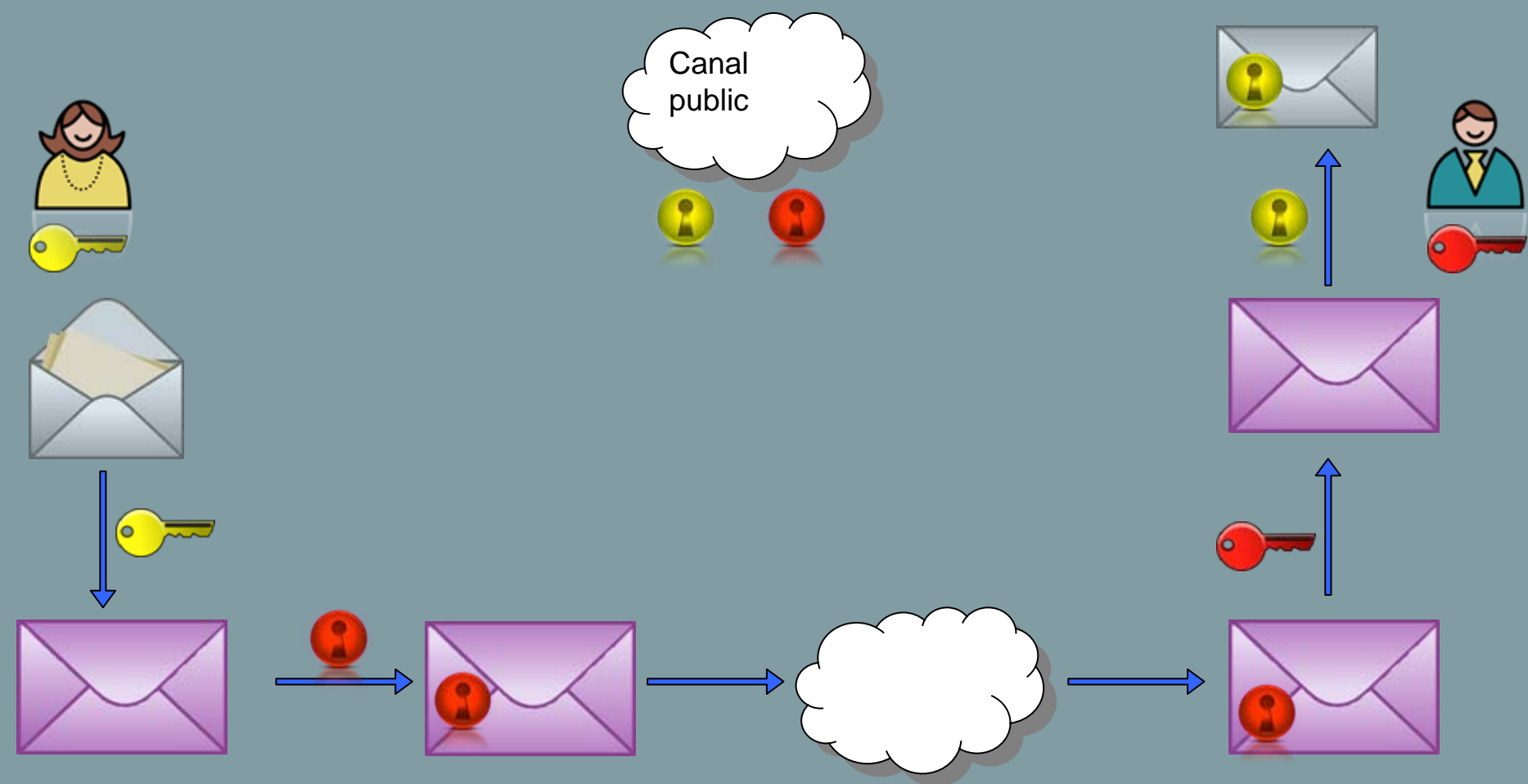
$$y = x^e \pmod{n} \quad y = 109466891$$



$$y^d \pmod{n} = 1091534$$

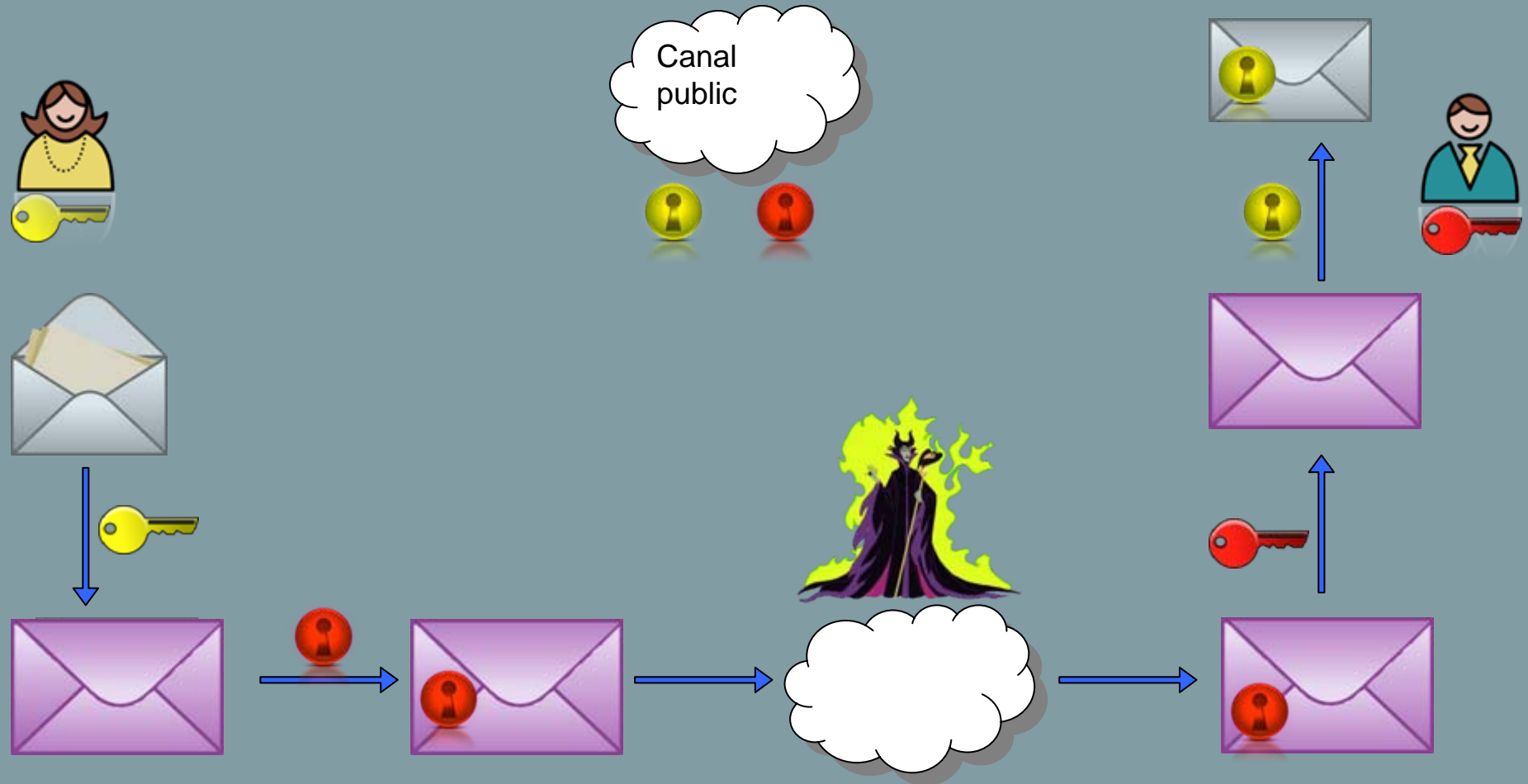


# Authentification par la méthode RSA.



25/01/2010

# « Man in the middle » devient impossible.



25/01/2010

59



- Résiste depuis 30 ans à toutes les tentatives de cryptanalyse.
- Système considéré comme fiable si l'on prend quelques précautions avec le choix et la longueur des clefs ( $n > 1024$  bits).
- Résoud à la fois le problème de confidentialité, d'authentification et de non désavoeu.
- Utilisé dans près de 500 millions de logiciels.

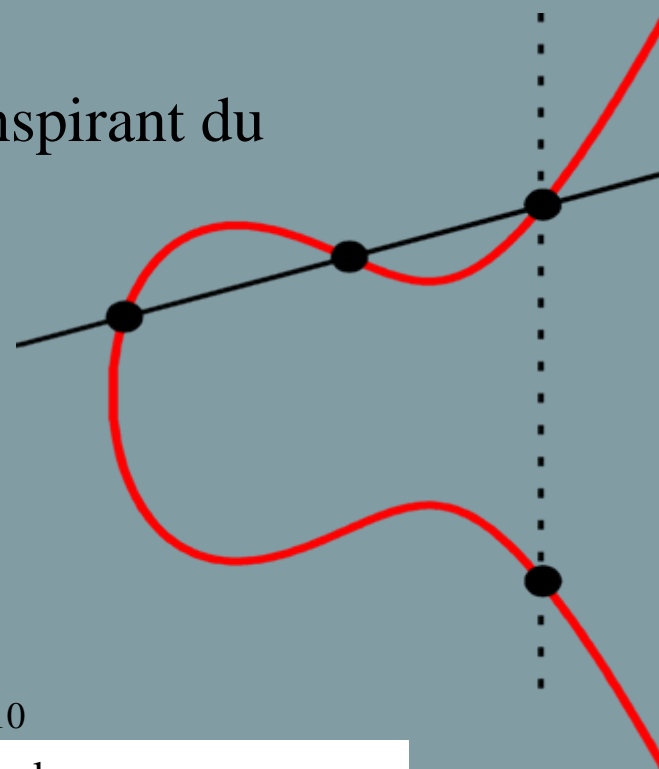


- 1.1. Quelques notions d'arithmétique.
- 1.2. Le protocole Diffie & Hellman.
- 1.3. Le protocole RSA.
- 1.4. Autres protocoles.
- 1.5. Conclusion.



- Reprend le principe de Diffie & Hellman (logarithmes discrets) en le modifiant pour permettre l'authentification.
- Plus lent que le RSA.
- Il n'est plus couvert par un brevet depuis 1997.

- Mathématiquement beaucoup plus compliqué que RSA.
- Nécessite des clefs plus courtes que le RSA pour une sécurité réputée équivalente.
- Inventé par Neal Koblitz en s'inspirant du protocole de Diffie & Hellman.
- Plus lent que le RSA.



25/01/2010

63



- 1.1. Quelques notions d'arithmétique.
- 1.2. Le protocole Diffie & Hellman.
- 1.3. Le protocole RSA.
- 1.4. Autres protocoles.
- 1.5. Conclusion.



The image shows a large black padlock in the center, overlaid on a background of various mathematical equations and formulas. The equations include terms like  $(y+6x+2)^4$ ,  $(y+8x)^2$ ,  $(y+7x+4)^4$ , and  $(y+8x)^2(y+7x+4)^4$ . There are also expressions involving  $x$  and  $y$  in the denominator, such as  $\frac{x(x+6)^2}{(y+8x)^2}$  and  $\frac{x(x+6)^2}{(y+9x+1)}$ . The background is a dark, textured surface with light-colored mathematical text.



# Des questions ?



25/01/2010

- Photo de couverture: © Adi Shamir.
- Dessin du cadenas: © pkey.jpg.
- Circuit imprimé.
- Horloge.
- Photo Diffie, Hellman, Merkle.
- Point d'interrogation.
- Pots de peinture.
- Maléfique.
- Shamir, Rivest et Adleman
- Logo RSA Security.
- Cliparts libres de droit.
- Autres sources d'inspiration:
  - Cryptographie appliquée de Bruce Schneier, éditions Vuibert.
  - L'art du secret, in « dossier pour la science ».
  - Histoire des codes secrets, de Simon Singh, éditions livre de poche.