Arithmétique pour la cryptographie

Marine Minier

INSA Lyon

Plan du cours

- Les nombres premiers
- Le pgcd
- Congruence et modulo
- Fonction indicatrice d’Euler
- Exponentielle et logarithme modulaire
- Fonction à sens unique

- Exemples d’applications : la cryptographie
- Détermination de « grands » nombres premiers

Les nombres premiers

- Définition : Un entier naturel p est **dit premier** si il n'admet comme diviseur que 1 et lui-même. Les autres nombres sont dits composés. (0 et 1 sont exclus)

- Théorème : Tout nombre entier supérieur à 1 peut se décomposer comme un **produit unique** de nombres premiers

Les nombres premiers

- Comment trouver cette décomposition ?
- 2007 est-il premier ? Il faut tester 2007/n pour
  - Algo 1 : pour tout n entier entre 2 et 2007-1
  - Algo 2 : pour tout n entier entre 2 et $\lfloor 2007 \rfloor_{int}$
  - Algo 3 (Crible d'Eratosténe) pour tout n premier entre 2 et $\lfloor 2007 \rfloor_{int}$

- Algo 3 : le plus performant
  - Il y a 37 607 912 018 nb premiers inférieurs à 10^{12}.
  - Peuvent se « stocker » astucieusement sur 20 Go
  - Mais au-delà ?...

Les nombres premiers

- Algo 2 : utilisable pour des nombres de 12 chiffres ou un peu plus

  => impossible de décomposer des nombres de 100 chiffres.

- => la multiplication est donc une **fonction à sens unique** (sous certaines cdtions)
  - Si n=pq (p et q grand), connaissant p et q il est facile de calculer n
  - **MAIS** connaissant n il est difficile de trouver p et q

Les nombres premiers

- Théorème (Euclide) : Le sous-ensemble constitué par les nombres premiers est infini.

- Démonstration : Supposons que cet ensemble soit fini : $E=\{p_1,\ldots,p_n\}$. $N=p_1p_2\ldots p_n+1$. N n'est divisible par aucun des p_i et n'est pas premier => contradiction

- Il y a une infinité de nombres premiers.

Quelques résultats

- Théorème : pour tout entier m, on peut trouver une plage de m-1 nombres consécutifs non premiers.

- Théorème de raréfaction (Hadamard) : Le nombre $\pi(n)$ de nombres premiers inférieurs à n tend vers n/log(n) quand n tend vers l'infini.

La division dans $\mathbb{Z}$

- Définition : Soient a et b deux éléments de $\mathbb{Z}$.
  Nous dirons que a **est divisible** par b ou encore que a **est multiple** de b s'il existe un element q dans $\mathbb{Z}$ tel que a = bq. On note b|a.

- Propriétés :
  - a|a, 1|a, a|0, a|ab
  - Si a|b et b|c alors a|c
  - Si d|a et d|b alors d|ab, d|(a+b), d|(a b).

La division dans $\mathbb{Z}$

- Théorème : Soit a un entier et b un entier **non nul**. Il existe un unique entier q et un unique entier r tels que

  $$a = qb + r$$

  ou r est / $0 \leq r < |b|$.

- Faire la division euclidienne de a par b consiste à trouver q (quotient) et r (reste).

- Lorsque b | a, q est le quotient exact de a par b et r = 0.

La division dans $\mathbb{Z}$

- Démonstration : utilisation de l'algorithme d'Euclide :
  - B := b; R := a; Q := 0;
  - tant que R $\geq$ B faire
    - R := R-B;
    - Q := Q+1;
- Exemple : a = 46, b = 15.
  - On a successivement B = 15, R = 46;Q = 0;
    - R = 46-15=31, Q=1
    - R=31-15 = 16, Q=2
    - R=16-15=1, Q= 3
    - => 46=3*15 +1
- Se généralise aux entiers négatifs

Le pgcd

- Définition : Parmi l'ensemble des diviseurs communs à deux entiers a et b, le **PGCD,** est le plus grand commun diviseur.

- Théorème : a, b, c dans $\mathbb{N}$ et n dans $\mathbb{Z}$
  - pgcd(ac,bc)=|c|.pgcd(a,b)
  - pgcd(a,b) =pgcd(a, b+na)

Propriétés du pgcd

- Propriétés :
  - pgcd(a; b) =pgcd(b; a)
  - pgcd(a; 1) = 1
  - Soit a_0 = a/pgcd(a; b) et b_0 = b/pgcd(a; b). Alors pgcd(a_0; b_0) = 1.

Calcul de pgcd

- Utilisation de l'algorithme d'Euclide (version plus précise) pour déterminer pgcd(a,b)
  - R0 := |a|; R1 := |b|; (b ≠ 0)
  - tant que R1 > 0 faire
    - R := Reste Division(R0;R1) ; R0 := R1 ; R1 := R;
  - Le dernier reste non nul est le pgcd.
  - Exemple : a = 325, b = 145
    - On a successivement
    - R0 = a = 325; R1 = b =145
    - R0 = 2R1 + 35 => R=35; R0 = 145; R1 = R = 35;
    - R0 = 4R1 +5 => R=5; R0 = 35;R1 = 5;
    - R0 = 7R1 + 0; R0 = 5;R1 = 0.
  - Donc pgcd(325; 145) = 5.

Nombres premiers entre eux

- Définition : lorsque pgcs(a,b)=1, on dit que a et b sont premiers entre eux.
- Remarques :
  - cela signifie que leur seul diviseur commun est 1.
  - Un nombre premier est premier avec n'importe quel autre nombre

Théorèmes :

- Théorème (Gauss) : a,b $\in \mathbb{N}$ premiers entre eux si et seulement si $\forall$ x $\in \mathbb{Z}$, si a|x.b alors a|b.

- Théorème : Deux nombres a et b $\in \mathbb{N}$ sont premiers entre eux ssi $\exists$ u et v $\in \mathbb{Z}$ /

$$u.a + v.b = 1$$

- Théorème (Bezout) : Si pgcd(a,b)=c avec a et b $\in \mathbb{Z}$, alors $\exists$ u et v $\in \mathbb{Z}$ /

$$u.a+b.v = c$$

Démonstration du théorème de Bezout

- Démo : utilisation de Euclide étendu qui permet de trouver u et v.
- Algorithme :
  - R0 := a; R1 := b; U0 := 1; U1 := 0;
  - V0 := 0; V1 := 1;
  - tant que R1 > 0 faire
    - Q := Quotient Division(R0;R1) ;
    - R := Reste Division(R0;R1) ;
    - U := U0 – Q.U1; V := V0 –Q.V1;
    - R0 := R1; R1 := R;
    - U0 := U1; U1 := U ;
    - V0 := V1; V1 := V ;

Démonstration (suite)

- En sortie :
  - R0 = pgcd(a; b)
  - A l'initialisation : U0.a + V 0.b = R0 et U1.a + V1.b = R1
  - => U0 = u et V0 = v

- Exemple : a=325 et B=145, On a successivement :
  - R0 = a = 325; R1 = b =145; U0 := 1; U1 := 0; V0 := 0; V1 := 1;
  - Q = R0/R1=325/145=2; R=325-2.145=35;
  - U := 1; V=-2; R0 = 145; R1 :=35; U0 :=0; U1 := 1; V0 := 1; V1:=2;
  - Q = R0/R1=145/35=4; R=145-4.35=5;
  - U :=-4; V:=1-4.(-2)=9; R0=35;R1=5;U0:=1;U1 :=-4; V0=-2; V1:=9;
  - Q = R0/R1=35/5=7; R=0;
  - U :=29; V:=-65; R0=5;R1=0;U0:=-4;U1 :=29; V0=9; V1:=-65;

  - Arrêt : a.U0 + b.V0 = 5 => a.(-4)+b.9=5

Quelques propriétés :

- Lemme (Euclide – Gauss) : si c divise a.b et c est premier avec a alors c divise b

- Si a est premier avec b et c alors a est premier avec $b^p c^q$, $\forall$ p,q $\in \mathbb{N}$

- Si p est premier et $p|a^n$ alors p|a

Quelques propriétés (suite) :

- $\prod_{i=1..k} p_i^{a_i}$ divise $\prod_{i=1..k} p_i^{b_i} \Leftrightarrow a_i \leq b_i, \forall\, i$
- $Pgcd(\prod_{i=1..k} p_i^{a_i}, \prod_{i=1..k} p_i^{b_i}) = \prod_{i=1..k} p_i^{\min(a_i,b_i)}$
- $Ppcm(\prod_{i=1..k} p_i^{a_i}, \prod_{i=1..k} p_i^{b_i}) = \prod_{i=1..k} p_i^{\max(a_i,b_i)}$
- Si $\prod_{i=1..k} p_i^{a_i} = b^q$ alors $\forall\, i$, a_i multiple de q

Congruence et modulo : arithmétique modulaire (Gauss 1801)

- Définition : **a est congru à b modulo n** signifie :
  - $\exists k \in \mathbb{Z} / a=k.n + b$
  - $\Leftrightarrow$ a et b ont le même reste dans la division par n
  - Ne diffère que par un multiple de n.
  - a − b est un multiple de n.

- Écriture : a=b (mod n) ou a =b [n]

Classes d’équivalence

- Définition : On appelle classe modulo n d'un élément x de $\mathbb{N}$, l'ensemble des y qui sont congrus à x modulo n.

- Remarques :
  - x= y mod n ssi ils ont le même reste dans la division par n
  - les n restes possibles permettent de définir les n classes d’équivalence modulo n.
  - Ces **n classes** se notent $\mathbb{Z}/n\mathbb{Z}$
  - **$\mathbb{Z}/n\mathbb{Z}$ est l’ensemble quotient de $\mathbb{Z}$ par la congruence mod n**

Classes d'équivalence : addition

- L'addition sur $\mathbb{Z}/n\mathbb{Z}$ conserve ses propriétés classiques :
  - Commutativité : x+y = y+x mod n
  - Associativité : (x+y)+z = x+(y+z) mod n
  - Élément neutre : 0+x=x+0=x mod n
  - Existence d'un opposé : x-x=0 mod n

  => On dit que $\mathbb{Z}/n\mathbb{Z}$,est un groupe pour +

Classes d'équivalence : multiplication

- La multiplication conserve :
  - La commutativité
  - L'associativité
  - L'élément neutre 1
  - L'élément absorbant 0
  - La distributivité par rapport à l'addition
  - PAS L'EXISTENCE D'UN INVERSE

=> On dit que ($\mathbb{Z}$/n$\mathbb{Z}$,+,*) est un anneau commutatif

Théorèmes (1/2) :

- Théorème : si a=b mod n et u=v mod n alors a+u=b+v mod n et a*u = b*v mod n

- Théorème : Un entier a est inversible dans $\mathbb{Z}/n\mathbb{Z}$ ssi a et n sont premiers entre eux

Théorèmes (2/2) :

- Théorème : si p est premier alors tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible

- Théorème : un entier p est premier ssi $\mathbb{Z}/p\mathbb{Z}$ ne contient pas de diviseurs de 0

Théorème des restes chinois (280-480)

- Soient $m_1,m_2,\ldots,m_r$ r entiers positifs premiers entre eux deux à deux et $a_1,a_2,\ldots,a_r$ des entiers quelconques.
- Le système d'inconnue x suivant :

$$x=a_1 \bmod m_1$$
$$x=a_2 \bmod m_2$$
$$\ldots$$
$$x=a_r \bmod m_r$$

- Admet une solution unique modulo $M= m_1.m_2.\ldots m_r$ donnée par :

$$x=\sum_{i=1\ldots r} a_i \cdot M_i \cdot y_i \pmod M$$

Avec $M_i=M / m_i$ et $y_i = M_i^{-1} \pmod{m_i}$

Exemple

- Trouver x positif et minimal vérifiant : $\begin{cases} x \equiv 3 \pmod{17} \\ x \equiv 4 \pmod{11} \\ x \equiv 5 \pmod{6} \end{cases}$

- D'après le théorème des restes chinois (17, 11 et 6 sont premiers entre eux deux à deux), les solutions sont de la forme :

M=17x11x6 = 1122

x = y1×11×6×3 + y2×17×6×4 + y3×17×11×5 + k×17×11×6

soit **x = 198.y1 + 408.y2 + 935.y3 + 1122.k.**

- Trouver les yi par division euclidienne : **$y_i = M_i^{-1} \pmod{m_i}$**

M1 = 66 = 3×17 + 15, 17 = 1×15 + 2, 15 = 7×2 + 1 => 1=8x15+7x17

15 = 66 - 3×17 d'où 1 = 8(66 - 3×17) + 7×17

On obtient pour finir 1 = 8×66 - 17×17 et **y1 = 8**.

- De la même manière, on trouve **y2 = 4 et y3 = 1.**
- Donc x = **198×8 + 408×4 + 935 + 1122n = 4151 + 1122n.**
- 4151 est donc une solution possible mais pas la plus petite.
- division de 4151 par 1122 => reste **x=785**

Fonction indicatrice d'Euler

- Elle est notée ϕ ou φ
- <u>Définition :</u> $\varphi(n)$ est égale au nombre d'entiers entre 0 et n-1 premiers avec n.
- $\varphi(n)$ correspond aussi au nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$
- Par convention, $\varphi(0)=0$ et $\varphi(1)=1$

Théorèmes (1/3) :

- Théorème : un entier p est premier ssi $\varphi(p)=p-1$
- Théorème : Si n et m sont entiers strictement positifs et premiers entre eux alors $\varphi(n.m)= \varphi(n).\varphi(m)$
- Théorème : Si p est premier et $n = p^k$ alors $\varphi(n)= p^k(1-1/p) = p^k – p^{k-1}$

Théorèmes (2/3) :

- Théorème : Si n se décompose en produit de facteurs premiers $p_1.p_2 \ldots p_r$ alors $\varphi(n)=n.(1-1/p_1).(1-1/p_2)\ldots(1-1/p_r)$
- Théorème : tout n > 0 peut s'écrire $\varphi(n)=\sum_{d|n} \varphi(d)$
- Théorème : Si n et a sont deux entiers strictement positifs et premiers entre eux alors

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

Théorèmes (3/3) :

- Petit théorème de Fermat : Si p est premier et ne divise pas a (p et a premiers entre eux) alors

$$a^{p-1}=1 \bmod p$$

- Généralisation : Si n et a sont deux entiers strictement positifs et premiers entre eux, alors

$$\exists\, k > 0 \,/\, a^k=1 \bmod n$$

et le plus petit k vérifiant cette propriété divise $\varphi(n)$.

Exponentielle et logarithme modulaire

- Définition : La fonction exponentielle de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ est définie par x -> a^x mod n.

- Définition : Calculer le logarithme en base a, c'est, étant donné $A=a^x$ mod n, déterminer x dans $\mathbb{Z}/n\mathbb{Z}$

- Ce calcul n'est possible que si x->a^x mod n est une bijection

Racines primitives

- Définition : soit n un entier et φ(n) l'indicateur d'Euler. On appelle racine primitive de n un nombre a avec 1<a<n /
  - a est premier avec n
  - $a^d \neq 1, \forall\ d / 0 < d < \varphi(n)$
- En particulier, si n est un nombre premier et 1<a<n, a est une racine primitive de n si

$$a^d \neq 1, \forall\ d / 0 < d < n-1$$

Ordre et racines primitives :

- Définition : Soit p un nombre premier. On appelle ordre d'un nombre a de $\mathbb{Z}/p\mathbb{Z}$, la plus petite valeur k / $a^k = 1 \bmod p$.

- Une racine primitive est donc un élément a d'ordre maximal p-1, i.e. $a^{p-1} = 1 \bmod p$.

Logarithme discret (suite)

- Théorème : Si p est premier et a est une racine primitive de p, alors la fonction f, définie de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathbb{Z}/p\mathbb{Z}$ par x -> a^x mod p est une bijection.

- Nous ne nous intéresserons à présent qu'à ce cas la : p premier.

Fonctions à sens unique

- Définition : une fonction à sens unique est une fonction qui est :
  - Simple à calculer
  - Difficile à inverser

- Deux exemples vus précédemment :
  - La factorisation de grands entiers
  - La fonction logarithme discret : Soit p un grand nombre premier et g une racine primitive modulo p, il s'agit de retrouver a connaissant A et g /

$$g^a = A \bmod p \text{ avec } 0 \leq a \leq p - 2$$

Fonctions à sens unique (suite) :

- Avantage de l'exponentielle : sous certaines conditions, elle est facile à inverser si on garde secret certaines informations.

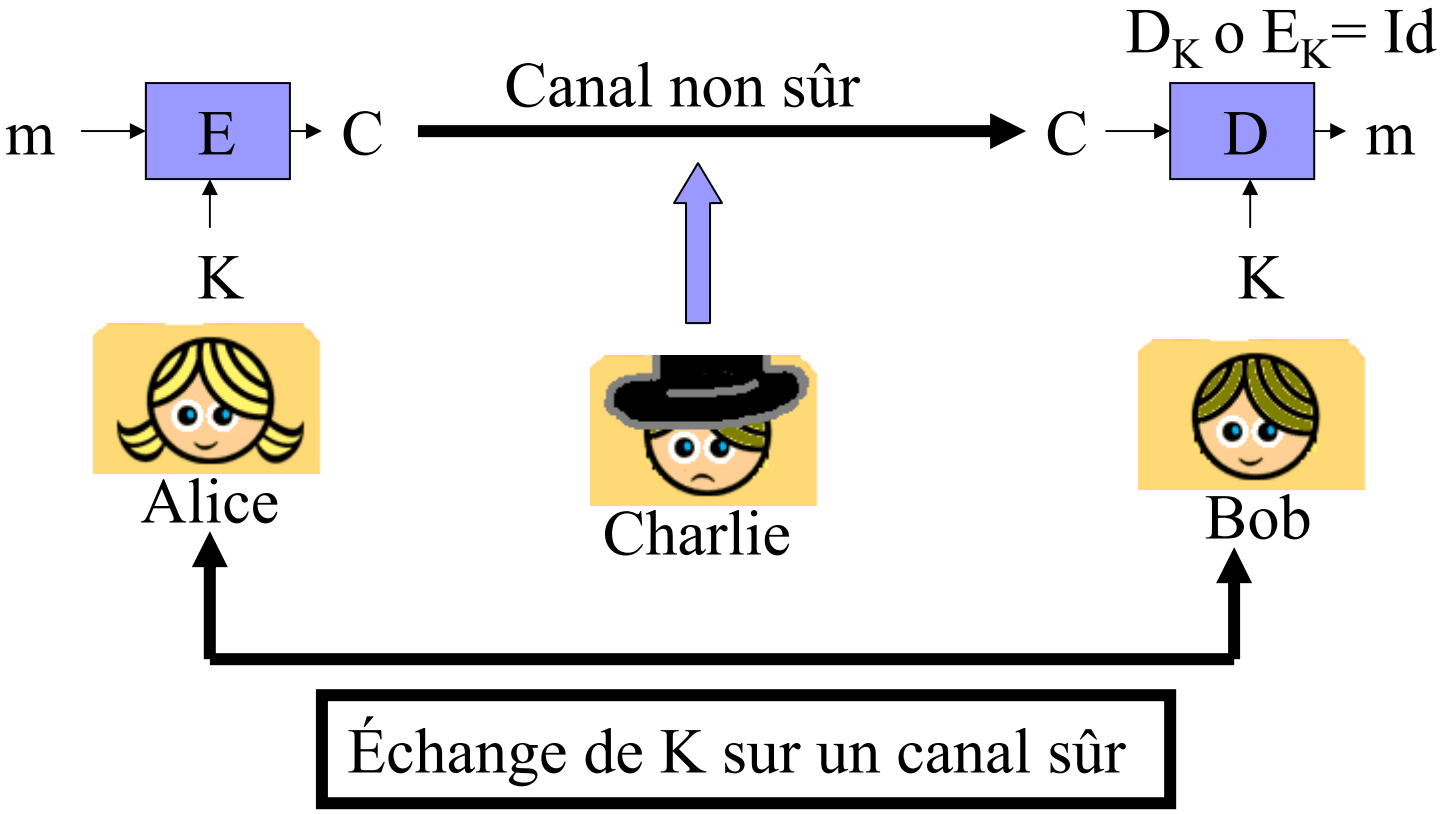
- Ces fonctions dites « à niche » servent en cryptographie.

Utilité de cette arithmétique :

- La cryptographie !

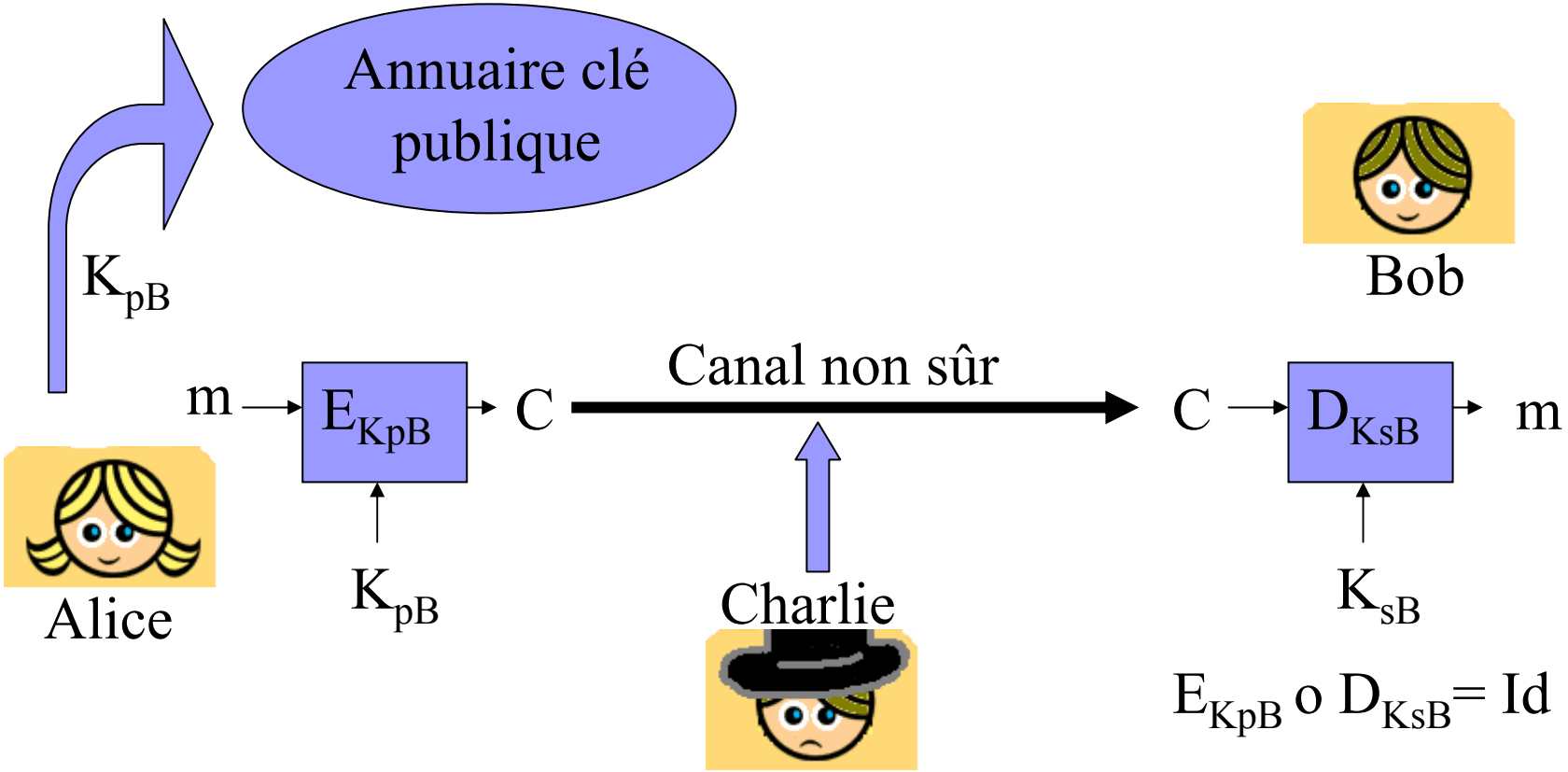
Deux méthodes pour chiffrer l'information (1/2)

- Cryptographie à clé secrète :



Deux méthodes pour chiffrer l'information (2/2)

- Cryptographie à clé publique :



Historique rapide (1/2)

- Algorithme à clé secrète plus rapide que clé publique (facteur 1000 entre les deux)

- Auparavant : la sécurité reposait sur le fait que l'algorithme utilisé était secret
  - Exemple : Alphabet de César : décalage de trois positions des lettres de l'alphabet

    => CESAR -> FHVDU

Historique rapide (2/2)

- Aujourd'hui : les algorithmes sont connus de tous : la sécurité repose uniquement sur le secret d'une clé (*principe de Kerckhoffs*).
  - Premier Exemple : Dernière guerre : Machine Enigma
  - Années 70 : développement des ordinateurs et des télécoms
  - 75-77 : Premier **standard de chiffrement** américain, le DES
  - 1976 : nouvelle forme de cryptographie : **la cryptographie à clé publique**, introduite par Diffie et Hellman (Exemple : RSA)

Cryptographie à clé publique

- Pour chiffrer un message, Alice utilise la clé publique de Bob et seul lui peut déchiffrer le message à l'aide de sa clé secrète

- Je ne donnerai pas ici les preuves permettant de garantir ces algorithmes

Problèmes mathématiques

- Besoin dans le cas de la cryptographie à clé publique de fonctions à sens unique afin de construire des problèmes asymétriques.

- Deux grands problèmes sont utilisés
  - La factorisation de grands nombres
  - Le problème du logarithme discret

Rappel

- Le problème difficile sur lequel repose RSA (Rivest Shamir Adleman) créé en 1977:
  - la factorisation : Il est très difficile de trouver p et q / n=p.q en ne connaissant que n

RSA (RFC 2437)

- Alice fabrique sa clé
  - n=pq avec p et q deux grands nombres premiers
  - e premier avec $\phi(n) = (p-1)(q-1)$ et d tel que $ed = 1 \bmod (p-1)(q-1)$
  - Rend publique (n,e)
- Bob veut envoyer un message m à Alice :
  - Bob calcule $c = m^e \bmod n$
  - Bob transmet c à Alice
- Alice déchiffre c en calculant :
  - $c^d = m^{ed} = m^1 \bmod n$

Taille des clés RSA :

- Aujourd'hui, factorisation de clés RSA (=n) de plus de 512 bits (154 chiffres décimaux)

- Taille minimum préconisé :
  - Au moins 768 bits
  - 1024 bits conseillé

Principes de construction du RSA

- Connaissant n retrouver p et q => problème difficile (pas d'algorithme en temps polynomiale)
- Factoriser n ⇔retrouver d ⇔Inverser x^e mod n
- Il existe une infinité de nombres premiers
  - On sait en construire (Fermat, Carmichael)
  - On sait tester si ils sont premiers (Miller – Rabin)
  - Voir plus loin…

Quelques solutions pour trouver des nombres premiers :

- Théorème de Wilson : un entier p est premier si et seulement si (p-1)!=-1 mod p

- => Inutilisable en pratique : trop lent

- Utilisation de tests de primalité.

Test de primalité

- Les nombres premiers ont beaucoup de propriétés que l'on peut tester
  - Si une propriété n'est pas vérifiée alors le nombre est composé
  - Si elle est vérifiée l'entier peut quand même être composé

Premier test :Fermat (petit thm)

- Certains nombres composés passent cependant le test de Fermat.

- Exemple : Nombres pseudo-premiers :
  - Un entier n est dit **probablement-premier de base b** si il vérifie (avec n et b premiers entre eux) :

$$b^{n-1} = 1 \pmod{n} \qquad (1)$$

  - Si n est composé et vérifie (1), il est dit **pseudo-premier** de base b

  - Exemple : 341=11.31 est pseudo premier de base 2

Ordre de grandeur :

- On a vu que le nombre de nombres premiers inférieur à n peut être approximer par n/ln(n)

- Le nombre de nombres premiers inférieurs à 10^{13} est d'environ 37 607 912 018
- Tandis que le nombre de pseudo-premiers de base 2 inférieur à 10^{13} est de 264 239

- => bonne probabilité de réussite du test de Fermat.

Nombres de Carmichael

- Définition : Les nombres de Carmichael sont des nombres composés et qui sont pseudo-premiers de base b, ∀ b premier avec eux.

- Exemple : le plus petit 561= 3x11x17

D’autres tests :

- Miller Rabin,…
- L’idée est surtout de combiné plusieurs tests afin d’avoir une probabilité très forte (99,999…%) d’avoir un nombre premier.

Principes de précaution pour RSA

- p et q doivent être grand ($\simeq$ 100 chiffres décimaux)
- p-q doit être grand (méthode de factorisation de Fermat)
- $p \pm 1$ et $q \pm 1$ doivent avoir un grand facteur premier chacun ($\simeq$ 100 bits)
- D'autres conditions,…

Car

- On a des algorithmes pour faciliter la factorisation des grands nombres
  - Méthode de Fermat
  - Crible quadratique, sur corps premiers,…
  - Méthode « rho » de Pollard,…

Méthode de Fermat :

- Se fonde sur la remarque suivante :

  Pour factoriser un entier N, on cherche à déterminer deux entiers x et y /

  $$x^2 = y^2 \bmod N \text{ mais } x \neq \pm y \bmod N$$

- En effet, cela implique que : $(x - y)(x+y) = k.N$

- Ce qui équivaut à pgcd(x - y,N) et pgcd(x+y,N) sont des facteurs non - triviaux de N.

- L'idée de base de Fermat est de calculer si $N=u.v$, $x^2 - N$ pour des valeurs successives de x en commencant par $x=N^{0.5}$ en incrémentant x à chaque étape

Exemple d'algorithme : Fermat amélioré

- Entrée : N entier composé impair
- $x := N^{0.5}$, $z := x^2 - N$;
- Tant que z n'est pas un carré parfait faire :
  - $z := z + 2x + 1$, $x := x + 1$
- Retourner $y := z^{0.5}$ et x-y et x+y

- Il existe des méthodes simples pour reconnaître des carrés parfaits (ils finissent par 00 ou 25,…)

Factorisation des nombres RSA

Record de Factorisation depuis 1970

années	70	83	86	89	90	93	96	99	03
Nombre de décimaux	39	50	80	100	116	120	130	155	160

- **Nouveau record en 2005 : RSA-200 digits (663 bits)**

RSA-200 =
27997833911221327870829467638722601621070446786955428537560009929326128400107609345671052955360856061822351910951365788637105954482006576775098580557613579098734950144178863178946295187237869221823983

=

35324619344027701212726049781984643686711974001976250236493034687761212536794232000585479565280883 49

X

79258699544783330333470858414800596877379758573642199607343303414557678728181521353814093047401854 67

Quelques chausse-trappe

- Même message avec l'exposant 3 vers trois destinataires :
  - $c_1 = m^3 \bmod n_1$
  - $c_2 = m^3 \bmod n_2$
  - $c_3 = m^3 \bmod n_3$

=>Calcul de m^3 par calcul de la racine cubique modulo $n_1 n_2 n_3$

Principe de El Gamal (1985)

- Repose sur le problème du log discret :
  - Soit p un grand nombre premier et g une racine primitive modulo p, il s'agit de retrouver a connaissant A et g /

$$g^a = A \bmod p \text{ avec } 0 \leq a \leq p-2$$

- Aussi difficile que la factorisation

Le cryptosystème El Gamal

- On choisit p premier (public) et g (public)
- La clé publique d'Alice est $y=g^x$ / clé secrète x
- Bob veut envoyer un message m à Alice :
  - Il tire un aléa r
  - Calcule y^r
  - Transmet ($A=my^r$, $B=g^r$)
- Alice déchiffre
  - $B^x = g^{xr} = (g^x)^r = y^r$
  - Calcule $A(y^r)^{-1} = m$

Recommandations

- Ne pas utiliser deux fois le même nombre aléatoire r
- p-1 doit avoir un grand facteur premier

- p doit être grand (pareil que pour RSA)
  - > 512 bits
  - On recommande 768 ou 1024 bits

Record de calcul de log discret

Thursday, September 22nd, 2005.

We are pleased to announce a new record for the discrete logarithm problem over GF(2^n). Using the function field sieve of Adleman [Ad94], we were able to compute discrete logarithms for **607 bits and 613 bits** prime. The first computation gives an interesting comparison between the function field sieve and Coppersmith's algorithm since the same field finite was already addressed by Thome using the later algorithm.

The two computations were done using different computers. For the first one, we used a **single 1.15GHz 16-processors HP AlphaServer** GS1280 computer **during one month**. For the second one, we used **four 16-processors nodes of the itanium 2 based Bull computer Teranova during 17 days (1.3GHz CPUs).**

Conclusion

- Une seule forme de cryptographie abordée : la cryptographie asymétrique
- Autre forme : cryptographie symétrique
  - 1000 fois plus rapide
  - MAIS suppose un pré échange de la clé commune sur un canal sûr
- => Fait grâce à la cryptographie asymétrique !