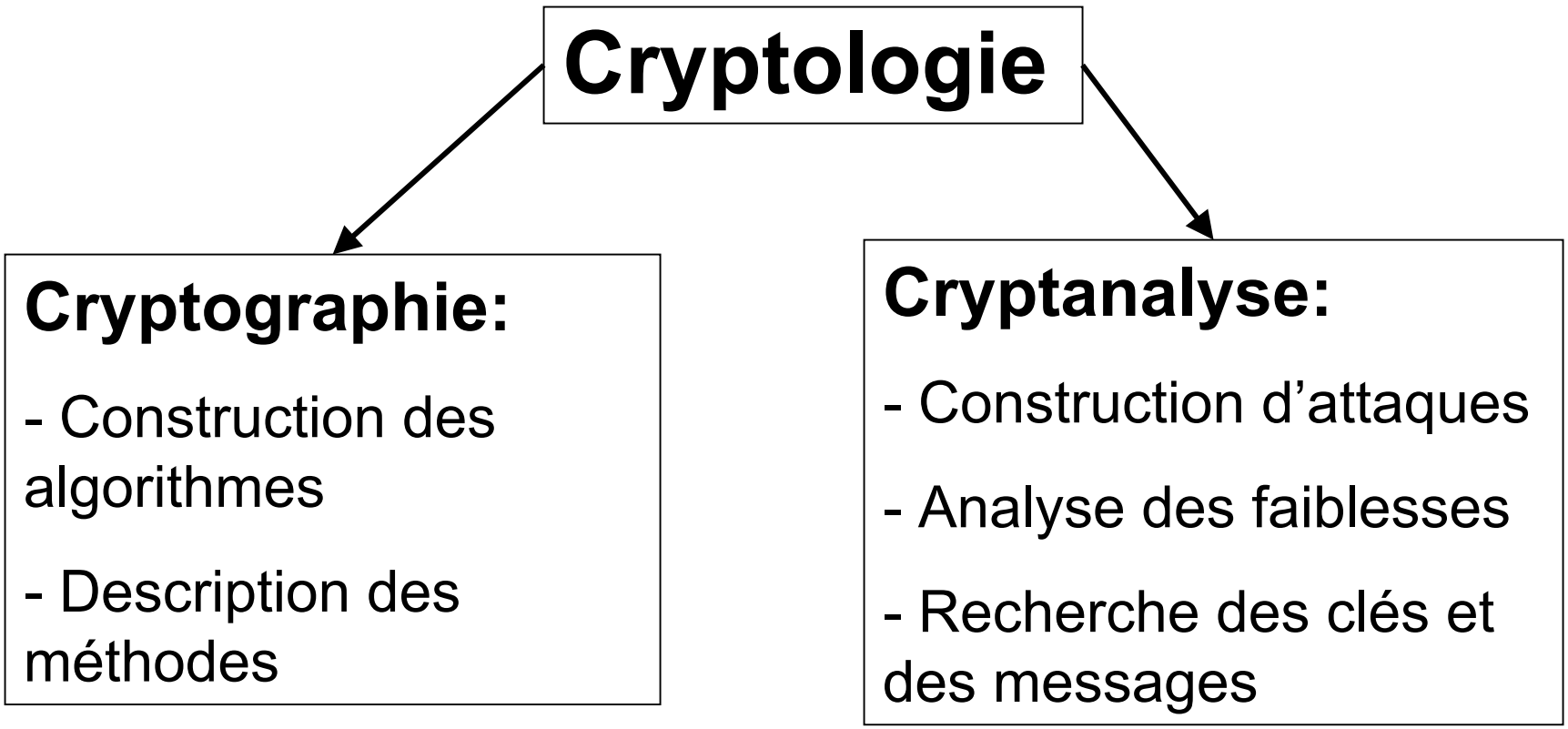
État-major général
Section cryptologie
3003 Berne

La cryptologie, l'armée suisse et … … les courbes elliptiques

Dr. François Weissbaum
État-major général
Section cryptologie

Préambule


Cryptologie
Cryptographie:
- Construction des algorithmes
- Description des méthodes
Cryptanalyse:
- Construction d'attaques
- Analyse des faiblesses
- Recherche des clés et des messages

Contenu

- Cryptologie au DDPS
- Le problème de base et sa solution
- Cryptographie moderne et classique
- Cryptographie à clé publique
- RSA et Diffie-Hellman
- Courbes elliptiques
- Cryptosystème et courbes elliptiques (ECC)
- Problème du logarithme discret (DLP)
- Conclusion

La cryptologie au DDPS

Administration

- Section cryptologie (S Krypt, GST)
- 10 professionnels

(adjoints scientifiques)

1. Mathématiciens
2. Informaticien
3. Physicien

Défense

- Troupe de transmission (Br 41, Krypt Kp II/47)
- Unité de miliciens

1. Mathématiciens
2. Informaticiens
3. Ingénieurs
4. …

La cryptologie au DDPS

Administration

S Krypt

- Tâches
  - Analyse des appareils
  - Connaissance des algorithmes standards
  - Construction de nouveaux algorithmes
  - Analyse des faiblesses de certains procédés

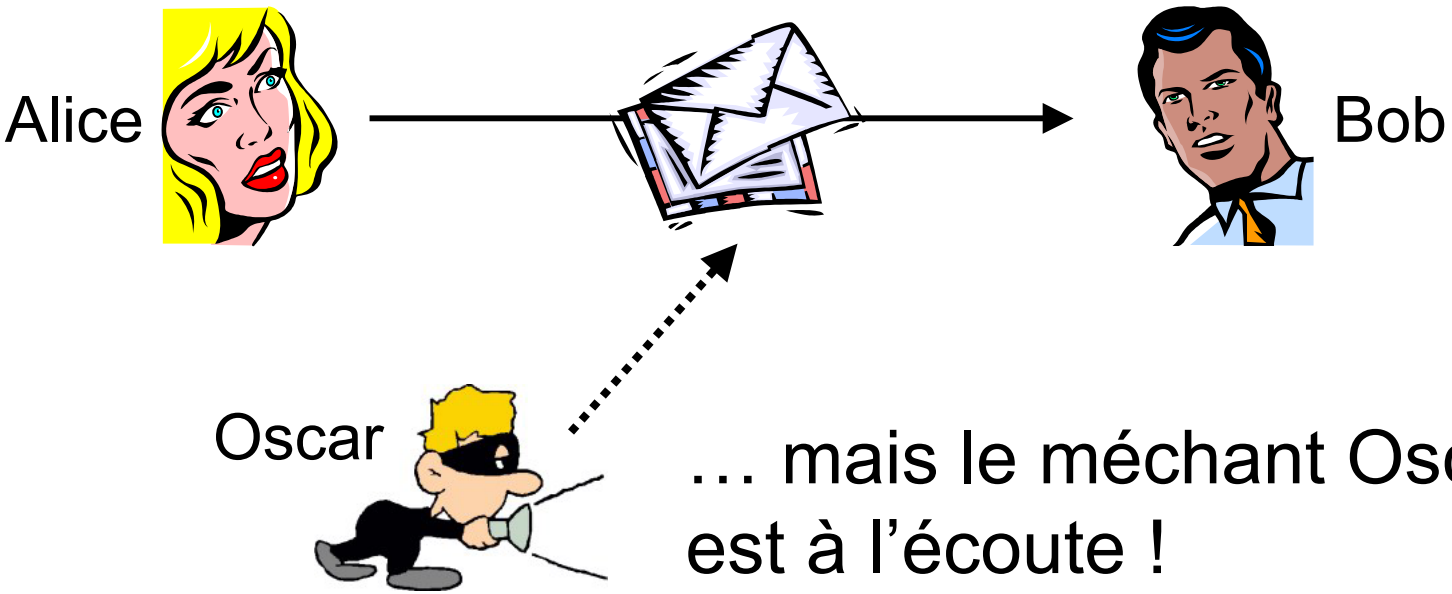
Défense

Krypt Kp

- Tâche
  - Comprendre les méthodes
  - Effectuer les travaux définis par S Krypt
  - Cryptanalyse
  - Formation militaire “allégée”

Le problème de base

Alice désire envoyer
un message secret à Bob, …



… mais le méchant Oscar
est à l'écoute !

État-major général
Section cryptologie
3003 Berne

LA SOLUTION

One-time pad (“+” = XOR):

```
M = 0 0 0 1 1 0 1 0 1 1 …
K = 0 1 0 0 1 0 1 1 1 0 …
---------------------------
C = 0 1 0 1 0 0 0 1 0 1 …
```

Alice: C = M + K
Bob: M = C + K

One-time pad garantit une sécurité absolue

Les 2 inconvénients du One-time pad

1. **Génération aléatoire de la clé K**
2. **Distribution de la clé K (à Alice et à Bob uniquement)**

Le but essentiel du cryptographe:
construire un système très proche du One-time pad … sans les inconvénients !

Bref historique (1)

- 1900 av JC Égypte: dérivé des hiéroglyphes
- 100-44 av JC Jules César: décalage de l'alphabet
- 1570 Vigenère: chiffrement «indéchiffrable»
- 1623 Francis Bacon: codage par bloc de 2 lettres
  - Première notion de compression
- 1917 Vernam: One-time pad
- 1920 FBI crée un office spécialisé
- 1939-1945 utilisation de la machine « Enigma » par l'armée allemande

Bref historique (2)

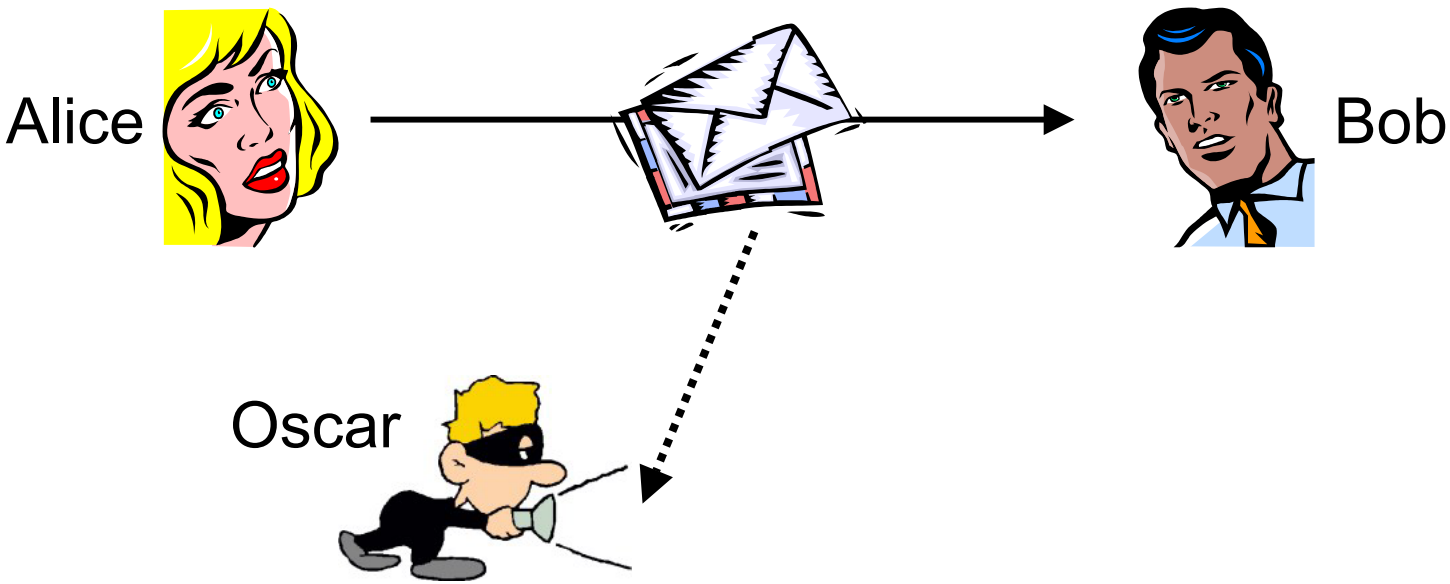
- 1948 Shannon: théorie de l'information
- 1970 Feistel: chiffrement par « round »: Data Encryption Standard (DES)
- 1976 Diffie et Hellman: cryptographie à clé publique
- 1978 Rivest, Shamir et Adleman: RSA
- 1985 Koblitz et Miller: courbes elliptique
- 1990 Lai et Massey: IDEA (International Data Encryption Algorithm)
- 1991 Phil Zimmerman: PGP (RSA + IDEA)
- 2000 Advanced Encryption Standard (AES)

Cryptographie moderne

- Confidentialité
- Authentification
- Intégrité
- Non-répudiation

Confidentialité

- Certitude qu'Oscar ne sait rien sur le contenu du message envoyé à Bob

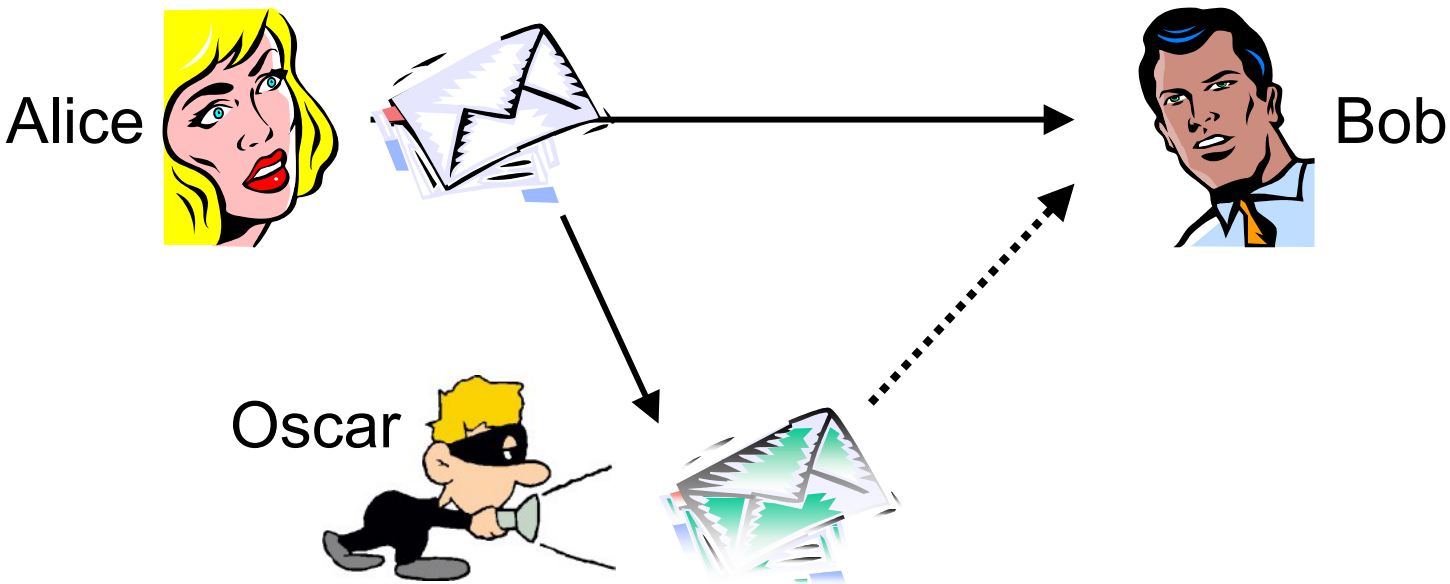


Authentification

- Bob est sûr qu'il communique avec Alice et seulement avec elle

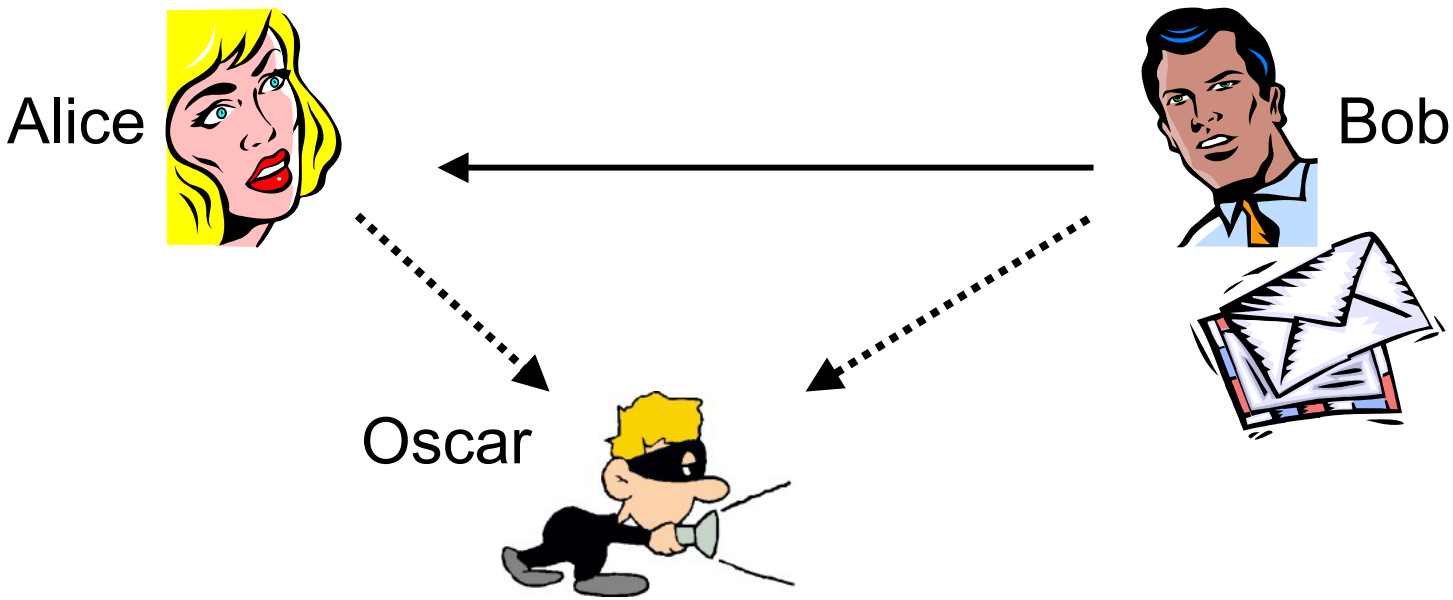
Intégrité

- Oscar n'a pas la possibilité de modifier le message entre Alice et Bob



Non-répudiation

- Bob peut démontrer qu'Alice est l'unique auteur du message



Cryptographie classique

- Un méthode cryptographique se résume par les 2 transformations:

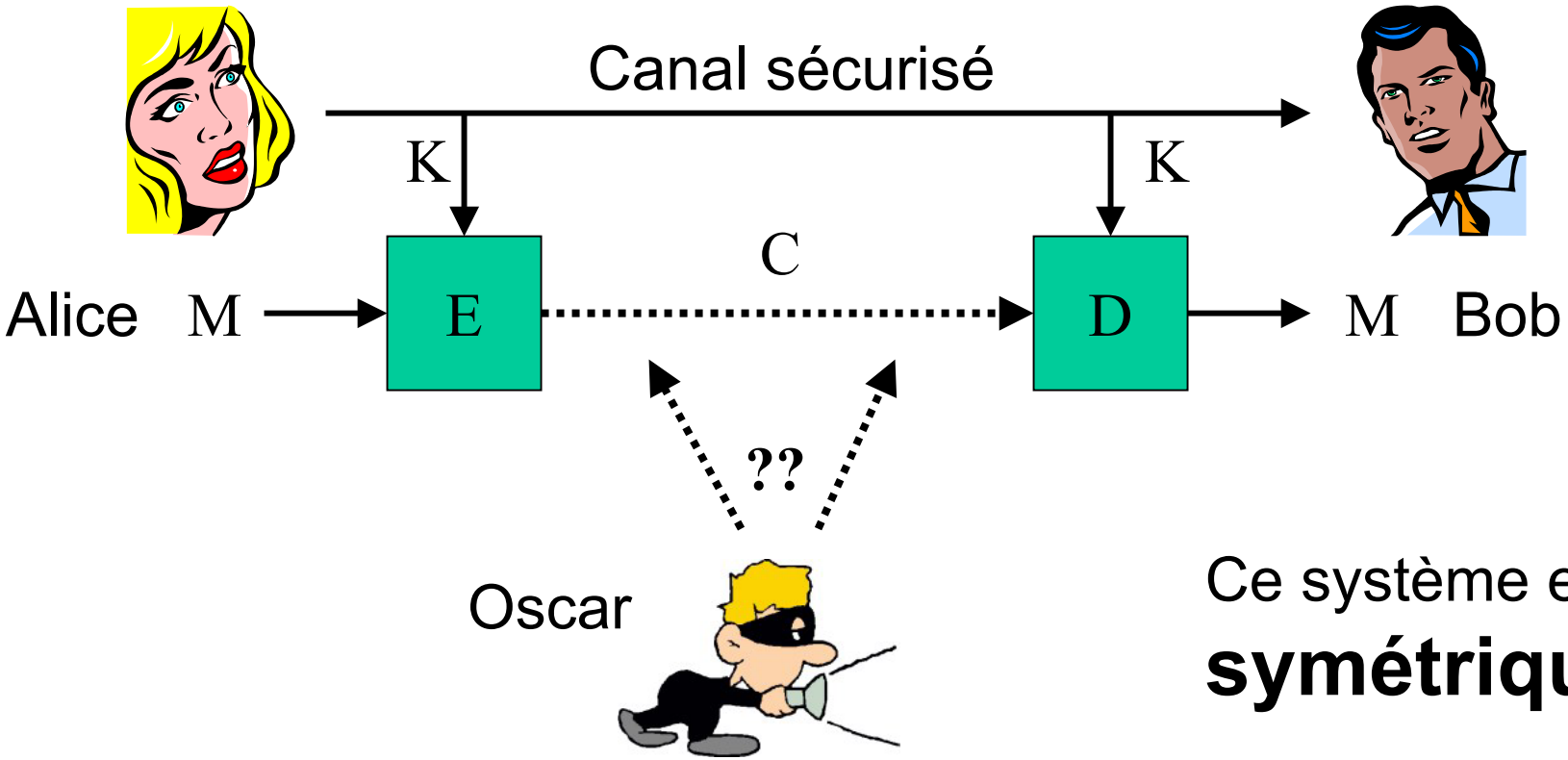
$$E : M \times K \rightarrow C \qquad D : C \times K \rightarrow M$$

- Ou 2 familles de transformations inversibles:

$$E_k : M \rightarrow C \qquad D_k : C \rightarrow M$$

Le paramètre *k* représente la clé secrète

Cryptographie classique

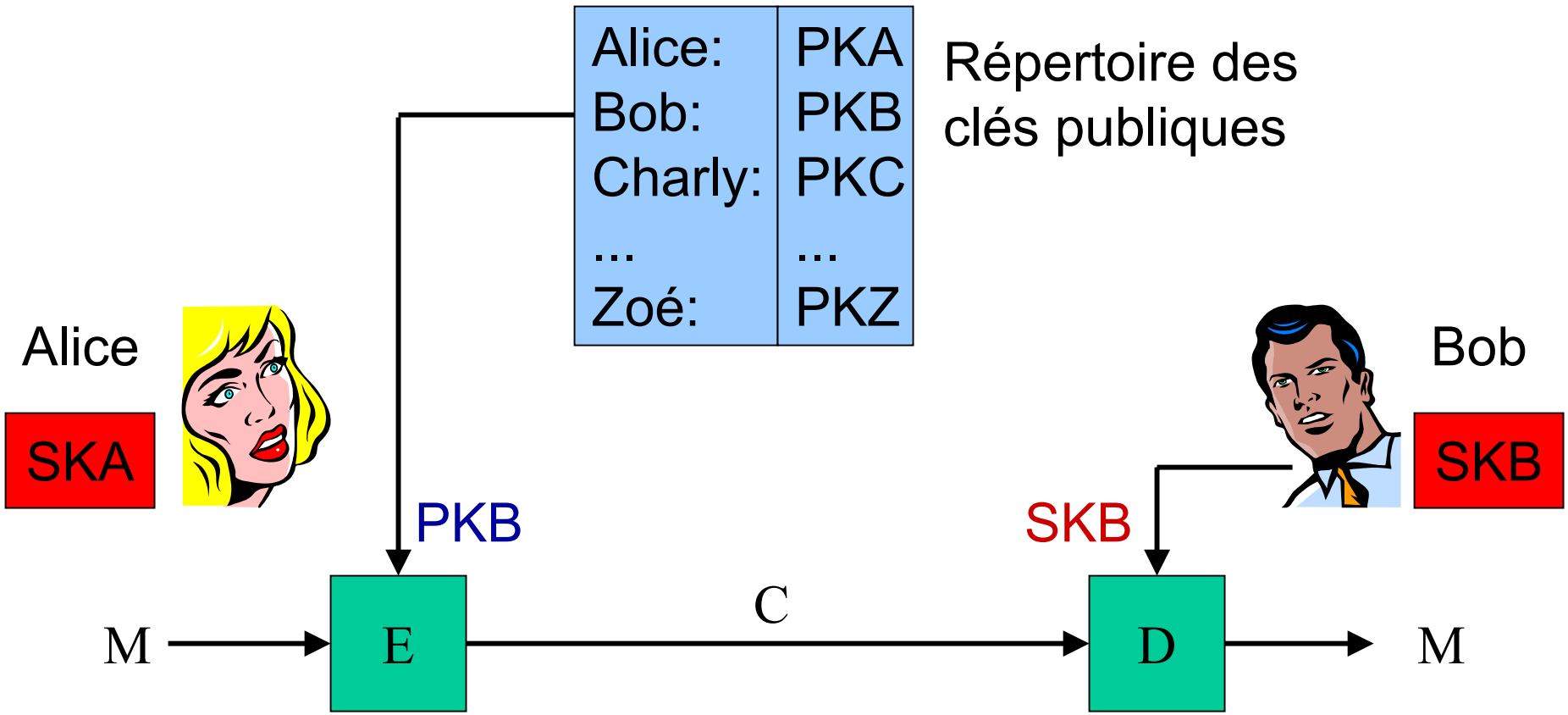


Ce système est
symétrique

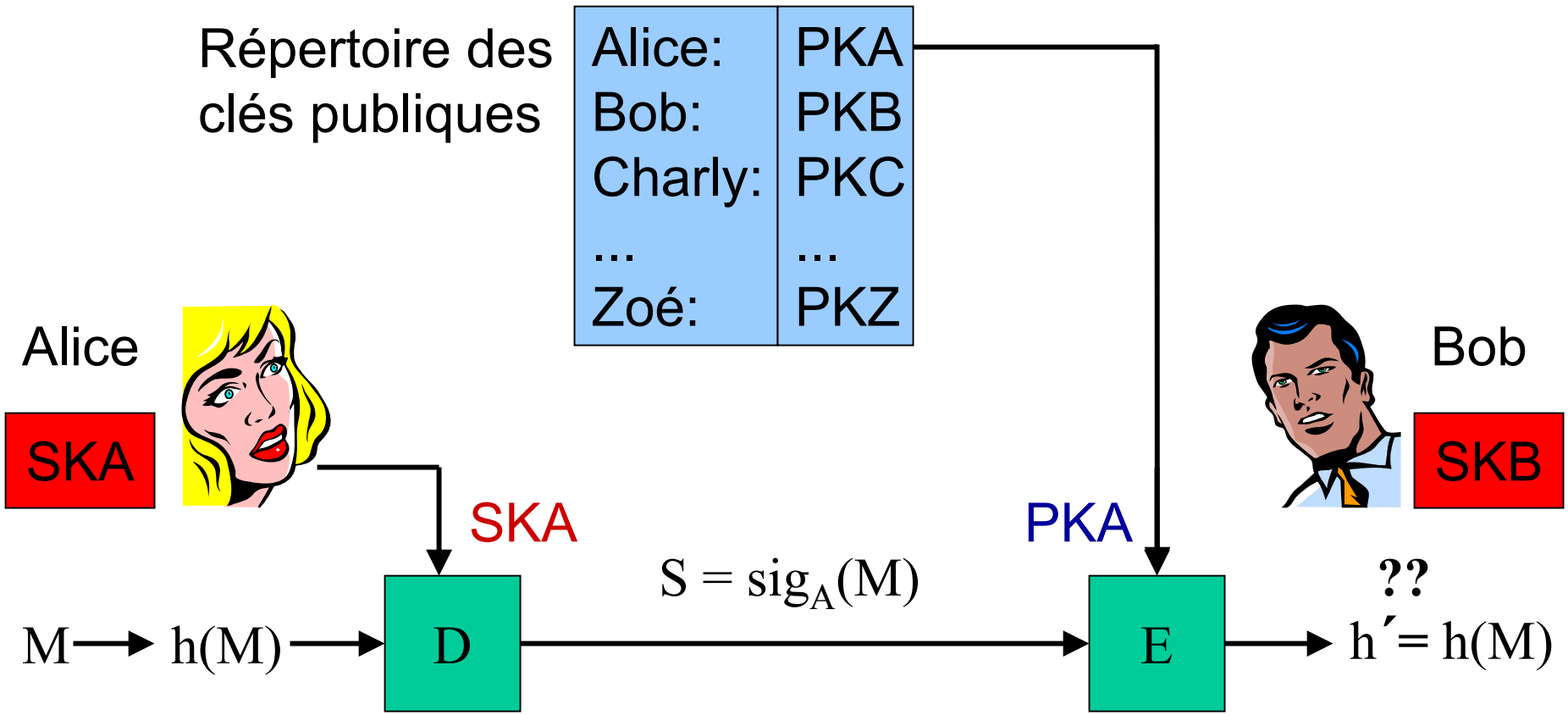
Cryptographie à clé publique

- Asymétrique (Diffie et Hellman, 1976):
  - Chiffrement et déchiffrement sont réalisés par deux clés différentes l'une de l'autre
  - Alice et Bob ont **chacun** deux clés:
    - clé publique (chiffrement)
    - clé privée (déchiffrement)
- Signature électronique ou digitale

Cryptographie à clé publique



Signature électronique



Fonction à sens unique

- Fonction à sens unique (one-way function):
  - La valeur $y = f(x)$ peut être vite calculée
  - Pour presque toutes les valeurs y, le calcul de $x = f^{-1}(y)$ est pratiquement impossible
- Exemple: $\boxed{y = \alpha^x \pmod p}$

  où p est un très grand nombre premier

  Le problème du logarithme discret (DLP):

  Données: y, α, p

  A trouver: x

Trapdoor one-way functions

- Famille de fonctions: $f_z : M \rightarrow C$
  - Pour chaque z, il existe une définition de $E = f_z$ et $D = f_z^{-1}$
  - Si z est inconnu, E est une fonction à sens unique
  - Si z est connu, E est facilement inversible

  Le paramètre z est la „Trapdoor“ (brèche secrète)
- Application:
  - Clé publique est définie par E
  - Clé privée est définie par z (ou D)

RSA

(Rivest, Shamir, Adleman, 1978)

- Théorie des nombres (Fermat-Euler):
  - Soit $n = pq$, p, q sont des premiers. Alors:

$$x^{(p-1)(q-1)} \equiv 1 \pmod{n} \qquad (x, n) = 1$$

  - Choisir $ed \equiv 1 \pmod{(p-1)(q-1)}$

$$E : y = x^e \pmod{n} \qquad D : x = y^d \pmod{n}$$

  - Preuve:

$$y^d = (x^e)^d = x^{ed} = x^{1+k(p-1)(q-1)} = x(x^{(p-1)(q-1)})^k = x$$

RSA

- Choisir 2 grands nombres premiers p et q, $n = pq$; Choisir $ed \equiv 1 \pmod{(p-1)(q-1)}$
  - Public Key: (n, e)
  - Private Key: (n, d)
- Trapdoor: la factorisation de n
- La sécurité est basée sur le problème de la factorisation des grands nombres
- Équivalence avec le calcul de $\varphi(n) = (p-1)(q-1)$

État-major général
Section cryptologie
3003 Berne

Exemple RSA

$p = 7, q = 11, n = 77 \qquad \varphi(77) = 60 \qquad e = 7, d = 43 \ (7 \cdot 43 = 301 \equiv 1)$

$x = 30 \qquad e = 1 + 2 + 4$

$x^7 = x^1 x^2 x^4$

$x^1 = 30$

$x^2 = 30^2 = 900 = 11 \cdot 77 + 53$

$x^4 = 53^2 = (-24)^2 = 576$

$= 7 \cdot 77 + 37 = 37$

$x^7 = (30 \cdot 53) \cdot 37 = 1590 \cdot 37$

$= (20 \cdot 77 + 50) \cdot 37 = 1850$

$= 24 \cdot 77 + 2 = 2$

$y = 2 \qquad d = 1 + 2 + 8 + 32$

$y^{43} = y^1 y^2 y^8 y^{32}$

$y^1 = 2 \qquad y^2 = 2^2 = 4$

$y^4 = 4^2 = 16 \qquad y^8 = 256 = 3 \cdot 77 + 25$

$y^{16} = 25^2 = 625$

$= 8 \cdot 77 + 9 \qquad y^{32} = 9^2 = 81 = 4$

$y^{43} = 2 \cdot (4 \cdot 25) \cdot 4$

$= 2 \cdot (23 \cdot 4)$

$= 2 \cdot 15 = 30$

Factorisation des grands nombres

- Algorithmes dédiés: Pollard, Rho
- Méthode basée sur les courbes elliptiques

$$O(e^{(1/2)\cdot(\log p)^{1/2}(\log\log p)^{1/2}})$$

- Multiple Polynomial Quadratic Sieve

$$O(e^{(\log n)^{1/2}(\log\log n)^{1/2}})$$

- Number Field Sieve

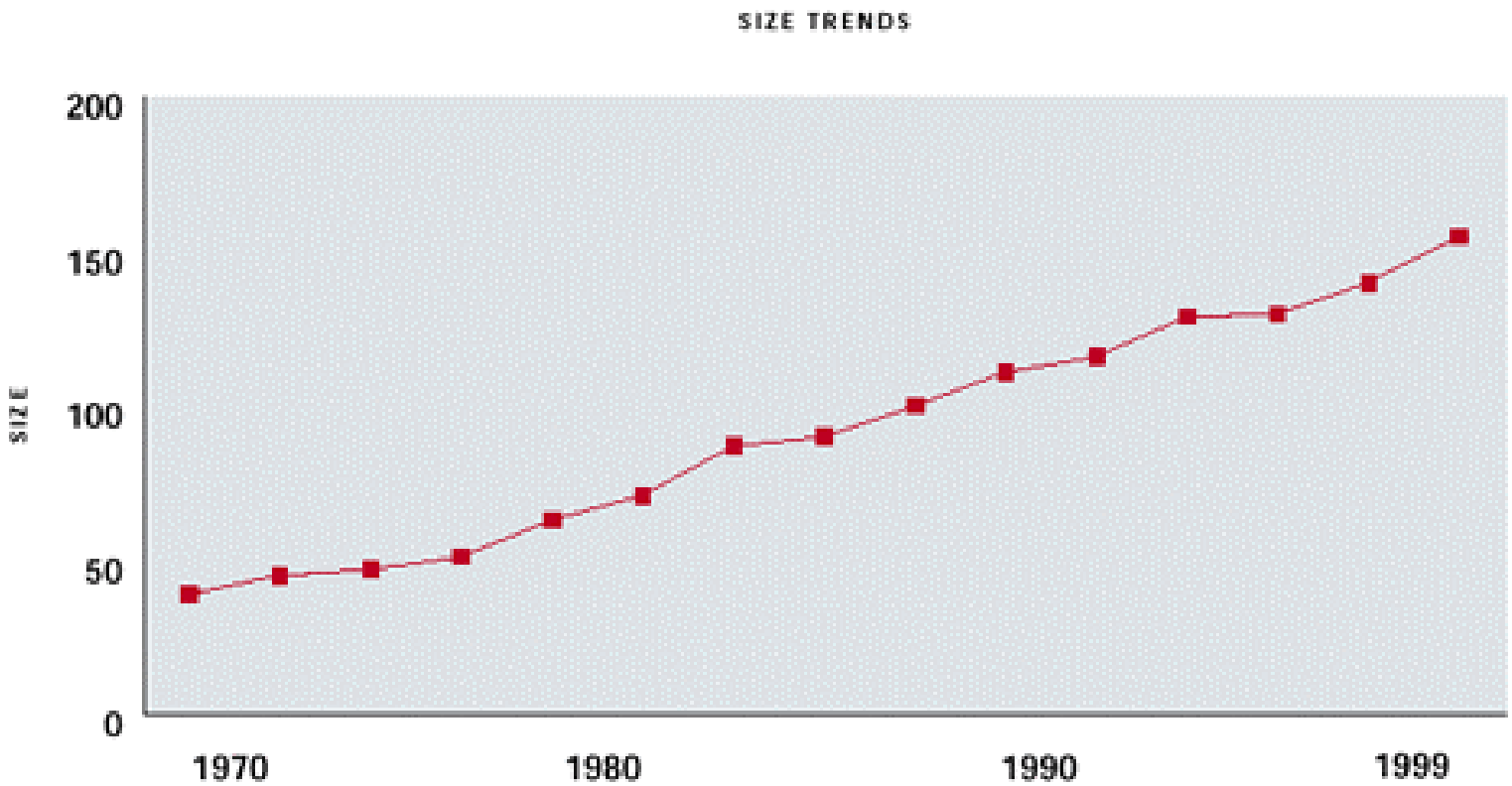
$$O(e^{1.923\cdot(\log n)^{1/3}(\log\log n)^{2/3}})$$

Factorisation: les records

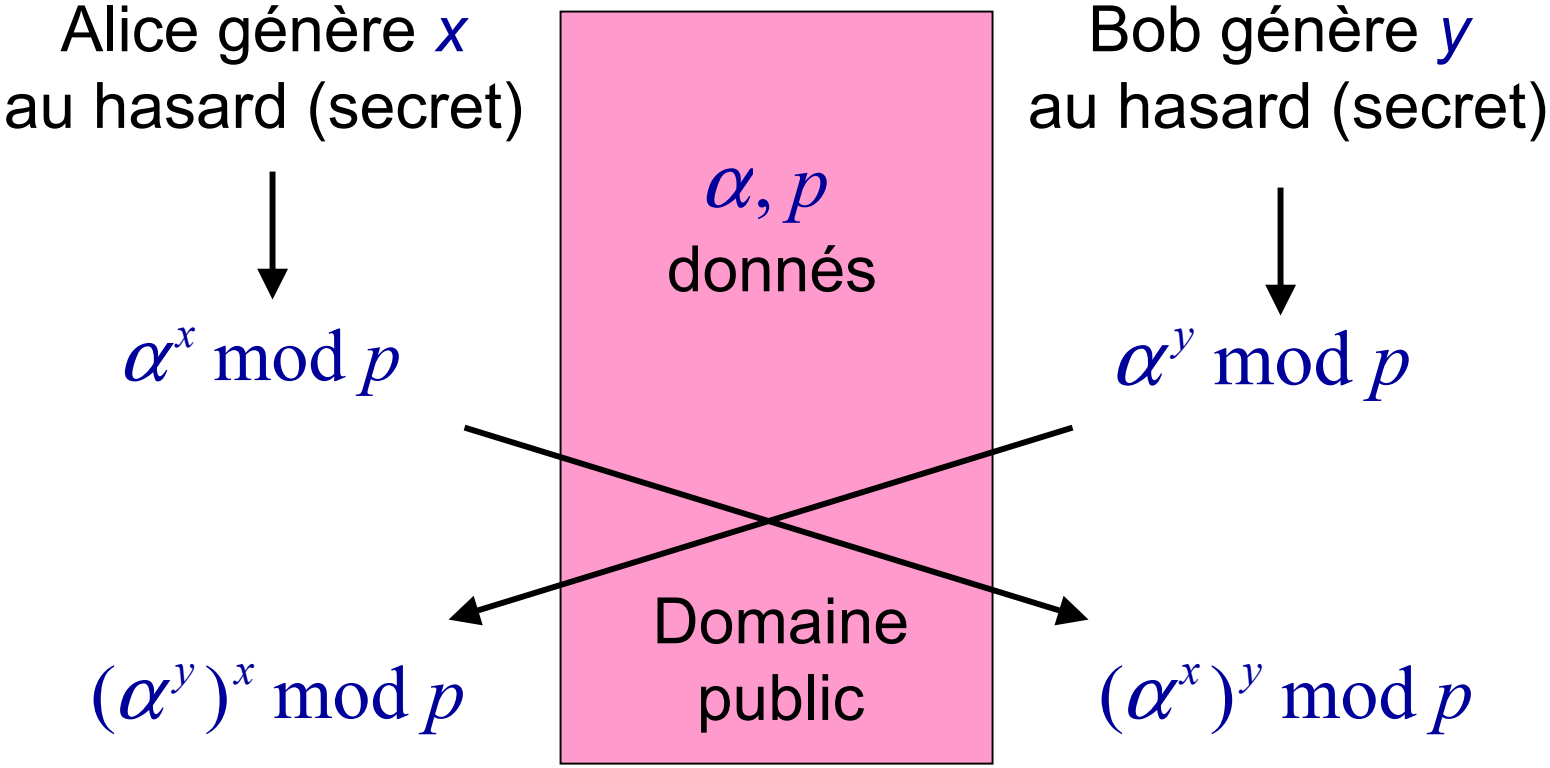
Nombre de décimales (Bits)	Date	MIPS-Années	Algorithme
RSA-100 (330)	Avr 1991	7	MPQS
RSA-110 (364)	Avr 1992	75	MPQS
RSA-120 (397)	Juin 1993	830	MPQS
RSA-129 (427)	Avr 1994	5000	MPQS
RSA-130 (430)	Avr 1996	1000	NFS
RSA-140 (463)	Fév 1999	2000	NFS
RSA-155 (512)	Août 1999	8000	NFS

Factorisation: les records

(graphique de RSA Laboratories)



Diffie-Hellman



Clé commune : $K = \alpha^{xy} \bmod p$

Sécurité de Diffie-Hellman

- Sécurité basée sur la difficulté du problème du logarithme discret (DLP):
  - Trouver *x* dans l'équation: $y = \alpha^x \bmod p$
  - Difficulté du DLP modulo un premier *p* est comparable à la factorisation d'un nombre *n* qui a le même ordre de grandeur que *p*
- 512 Bit : cassable avec beaucoup d'effort
- 768 Bit : sûr ... pour l'instant !
- 1024 Bit : une taille adaptée aujourd'hui

Diffie-Hellman dans un groupe

- Diffie-Hellman (DH) dans un corps fini F_q
- Exemple: $q = 2^n$
  - Multiplication rapide pour la construction de la clé
  - Mais aussi ... algorithme rapide pour résoudre le DLP (Coppersmith 1984)
- DH est défini essentiellement par une structure de groupe abélien
- N. Koblitz et V. Miller (1985): utilisation des courbes elliptique (groupe abélien) pour DH

Courbe elliptique - Historique

- A l'origine: analyse complexe, intégrales elliptiques, fonctions elliptiques
- Géométrie algébrique
- Théorie des nombres:
  - Exemple célèbre: démonstration du dernier théorème de Fermat (Andrew Wiles, 1995):

    $$x^n + y^n = z^n$$

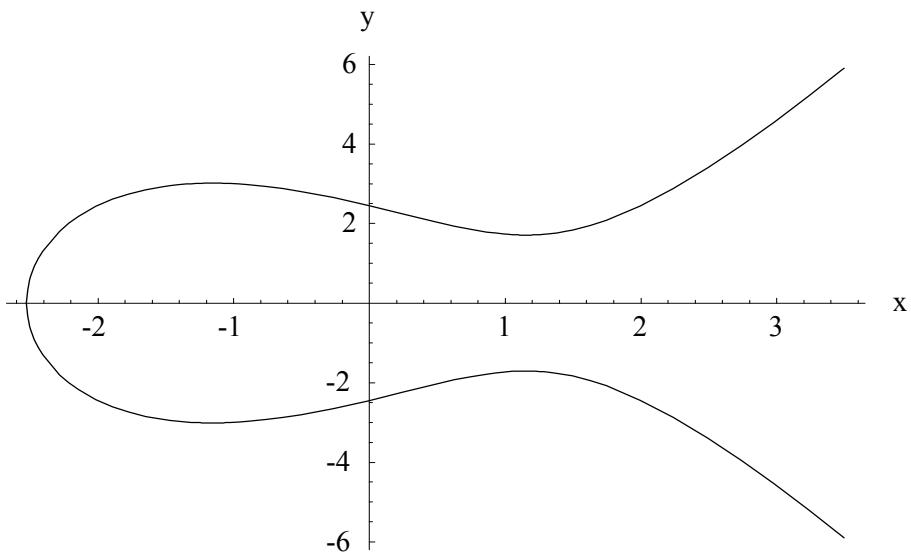
    n'a pas de solution entière pour $n > 2$
- Cryptographie, Factorisation

Courbe elliptique sur un corps

- Soit K un corps et a, b dans K. Une courbe elliptique $E(a,b)$ est définie par

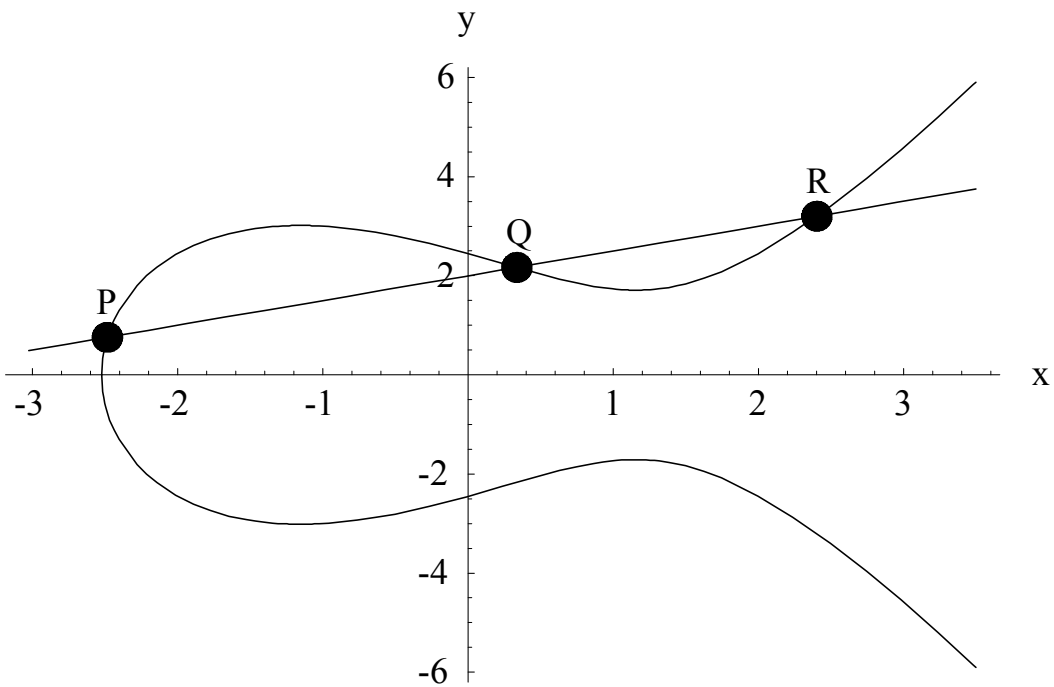
$$\{(x,y) \in K^2 \mid y^2 = x^3 + a\,x + b\} \cup \{O\}$$

- Exemple $a = -4, b = 6$ dans $R \times R$:



Courbe elliptique sur *K*

La droite qui coupe la courbe en 2 points *P* et *Q* a un 3ème point d'intersection *R*.



Equation de la droite:

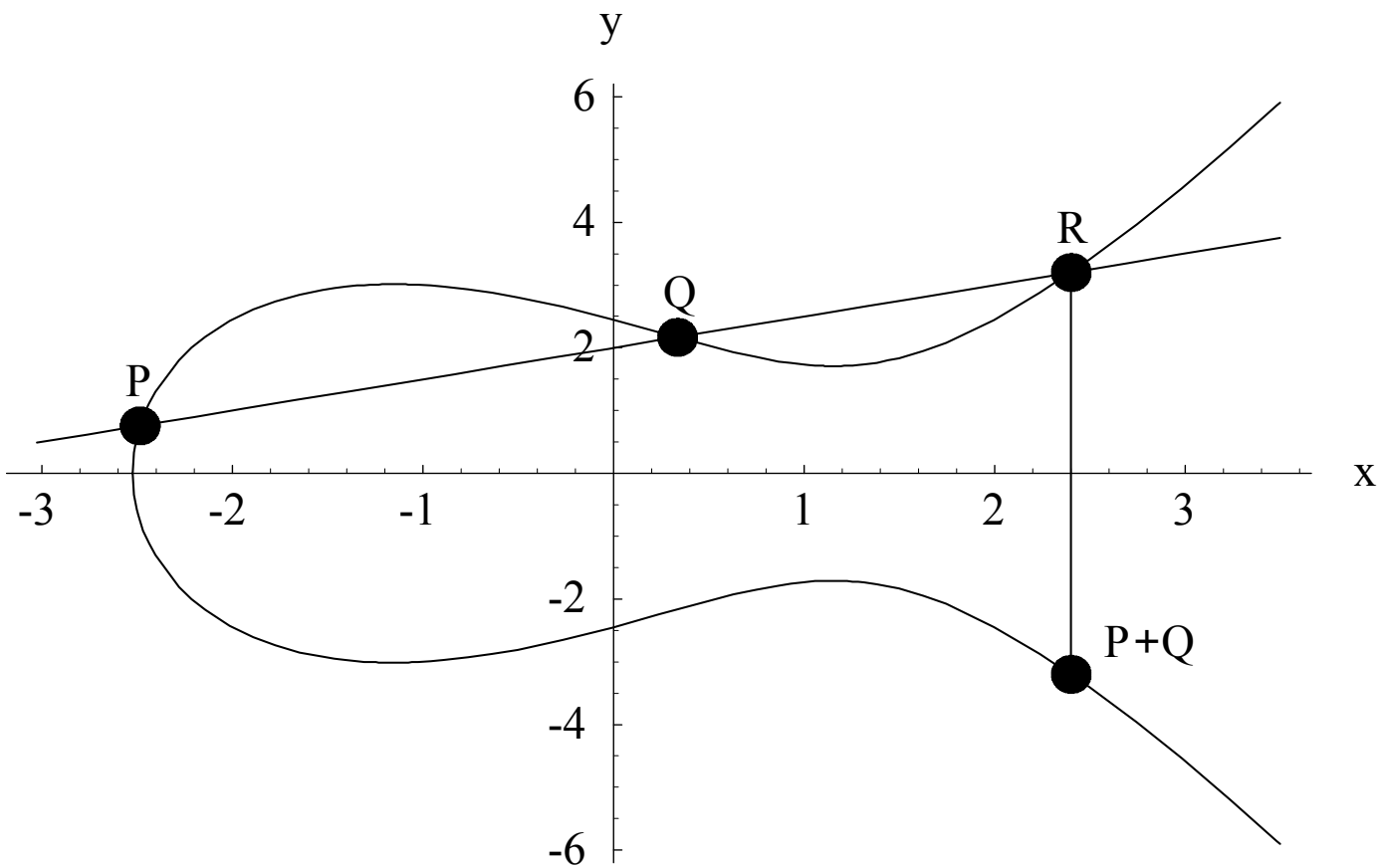
$$y = \alpha x + \beta$$

Intersection:

$$(\alpha x + \beta)^2 = x^3 + a x + b$$

Si cette équation a 2 solutions dans *K*, alors il en existe une 3ème.

Addition de points



Le groupe „courbe elliptique“

- Élément neutre: $O = \infty$
- L’inverse: symétrique par rapport à l’axe x.
- Associativité (non trivial): Preuve:
  - Calcul minutieux (Mathematica: 20 sec. avec un Dual-Pentium 800 MHz)
  - Théorique: géométrie algébrique
  - Sur le corps C : analyse complexe
- Abélien: $P + Q = Q + P$

État-major général
Section cryptologie
3003 Berne

Associativité avec Mathematica

```
In[1]:= y1 = Sqrt@x1^3 + a x1 + bD;   y2 = Sqrt@x2^3 + a x2 + bD;   y3 = Sqrt@x3^3 + a x3 + bD;

        u1 = -x1 - x2 + HHy2 - y1L ê Hx2 - x1LL^2;
        v1 = -y1 - HHy2 - y1L ê Hx2 - x1LL Hu1 - x1L;      H   Hx1, y1L + Hx2, y2L = Hu1, v1L   L
        u2 = -u1 - x3 + H Hv1 - y3L ê Hu1 - x3LL^2;
        v2 = -v1 - HHy3 - v1L ê Hx3 - u1LL Hu2 - u1L;      H   Hu1, v1L + Hx3, y3L = Hu2, v2L   L

        p1 = -x2 - x3 + HHy3 - y2L ê Hx3 - x2LL^2;
        q1 = -y2 - HHy3 - y2L ê Hx3 - x2LL Hp1 - x2L;      H   Hx2, y2L + Hx3, y3L = Hp1, q1L   L
        p2 = -p1 - x1 + H Hq1 - y1L ê Hp1 - x1LL^2;
        q2 = -y1 - HHq1 - y1L ê Hp1 - x1LL Hp2 - x1L;      H   Hx1, y1L + Hp1, q1L = Hp2, q2L   L

        Simplify@p2 - u2D                                          u2

Out[10]= 0      (* 1 sec. Dual Pentium 800 MHz *)

In[11]:= Simplify@q2 - v2D

Out[11]= 0      (* 20 sec. Dual Pentium 800 MHz / 4.5 min. sans p2 ← u2 *)
```

Courbe elliptique modulo *p*

- Courbe elliptique sur un corps fini F_p :

$$E : y^2 = x^3 + a\,x + b \pmod{p} \qquad p \neq 2,3$$

p est un nombre premier

- Exemple:

$$p = 23, a = 19, b = 6$$

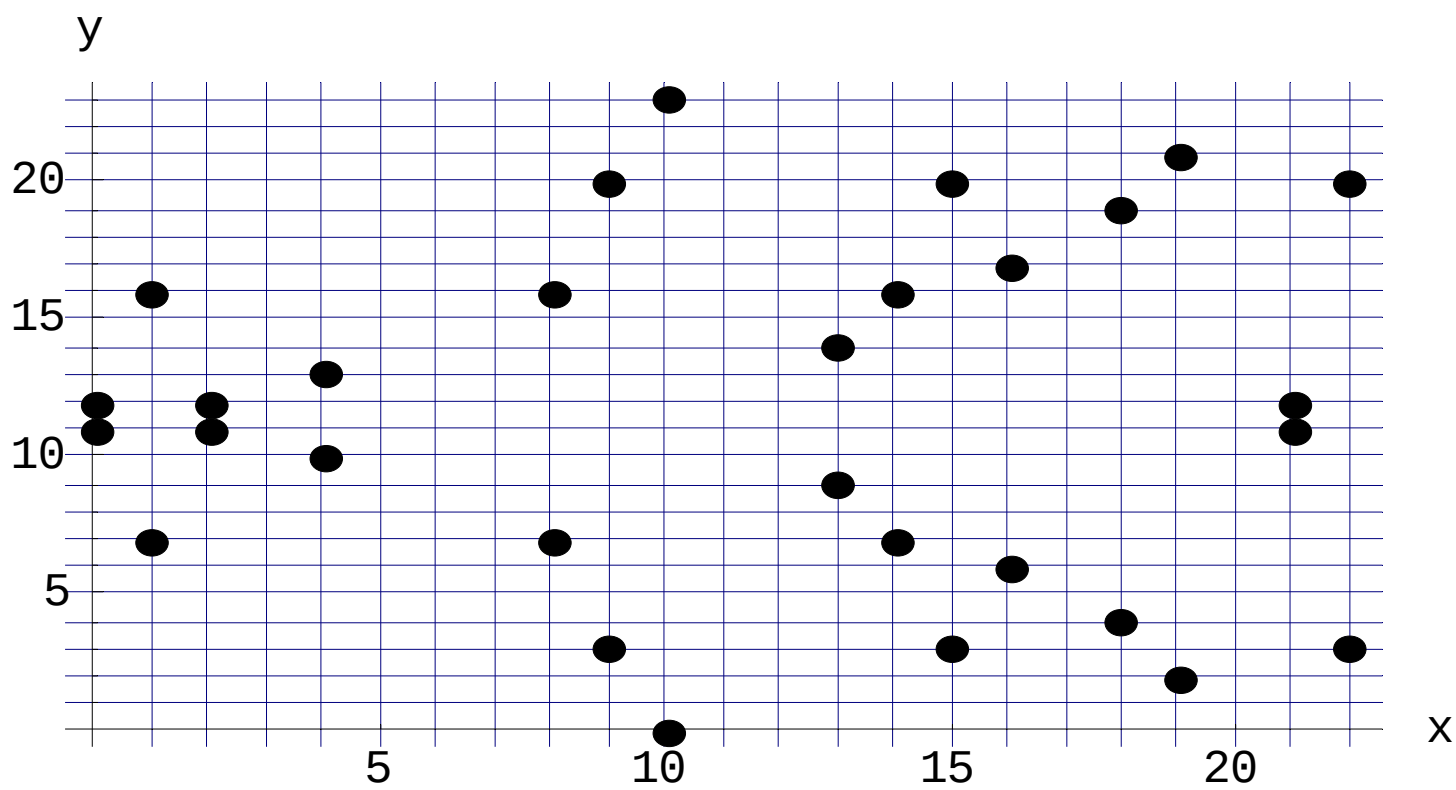
$$x = 2: \qquad x^3 + a\,x + b = 8 - 4 \cdot 2 + 6 = 6$$

$$y = 11: \qquad y^2 = 121 = 5 \cdot 23 + 6$$

Les points (2,11) et (2,12) appartiennent à *E*

Courbe elliptique modulo *p*

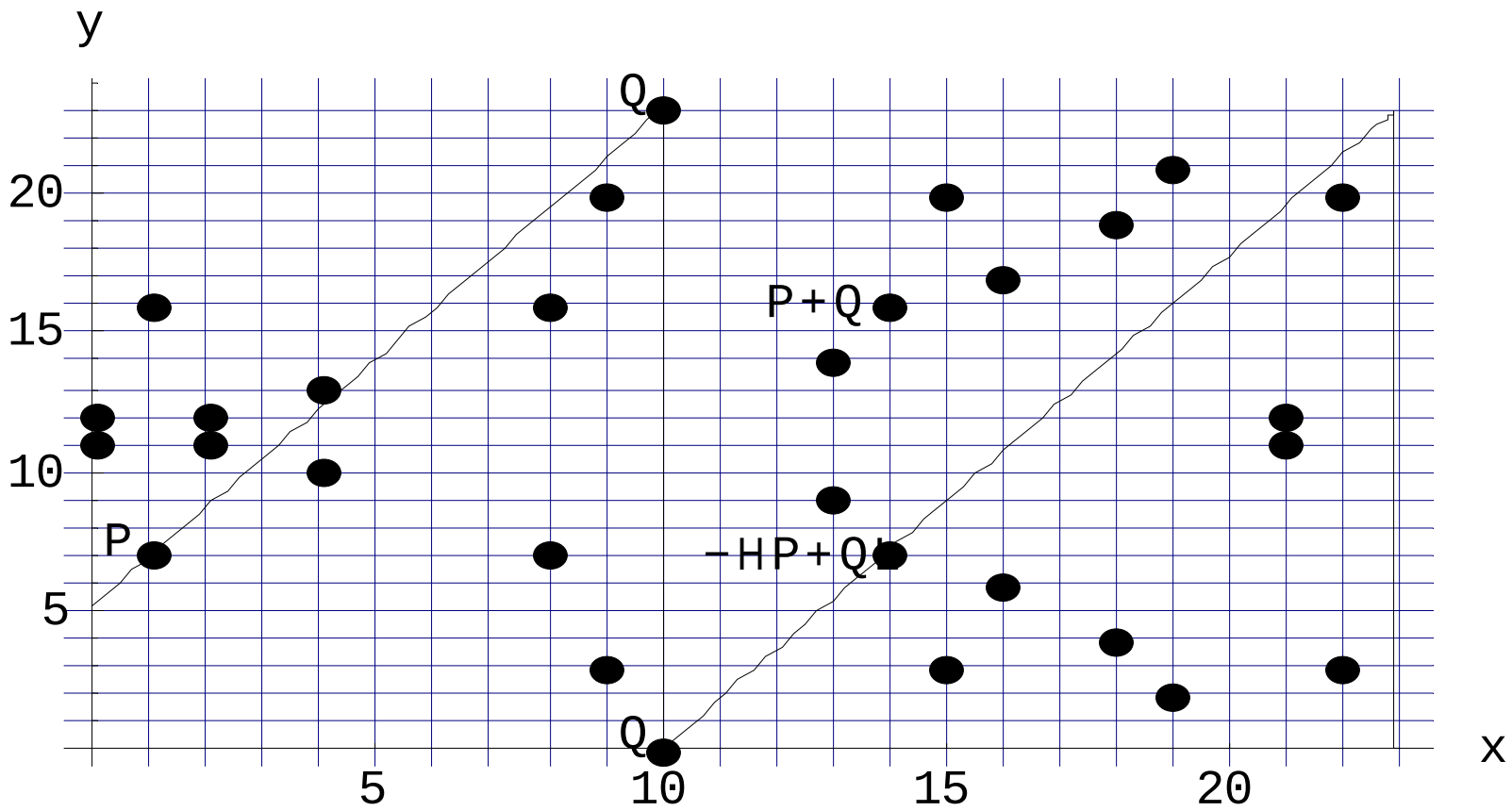
Les points de la courbe $E : y^2 = x^3 + 19x + 6 \pmod{23}$



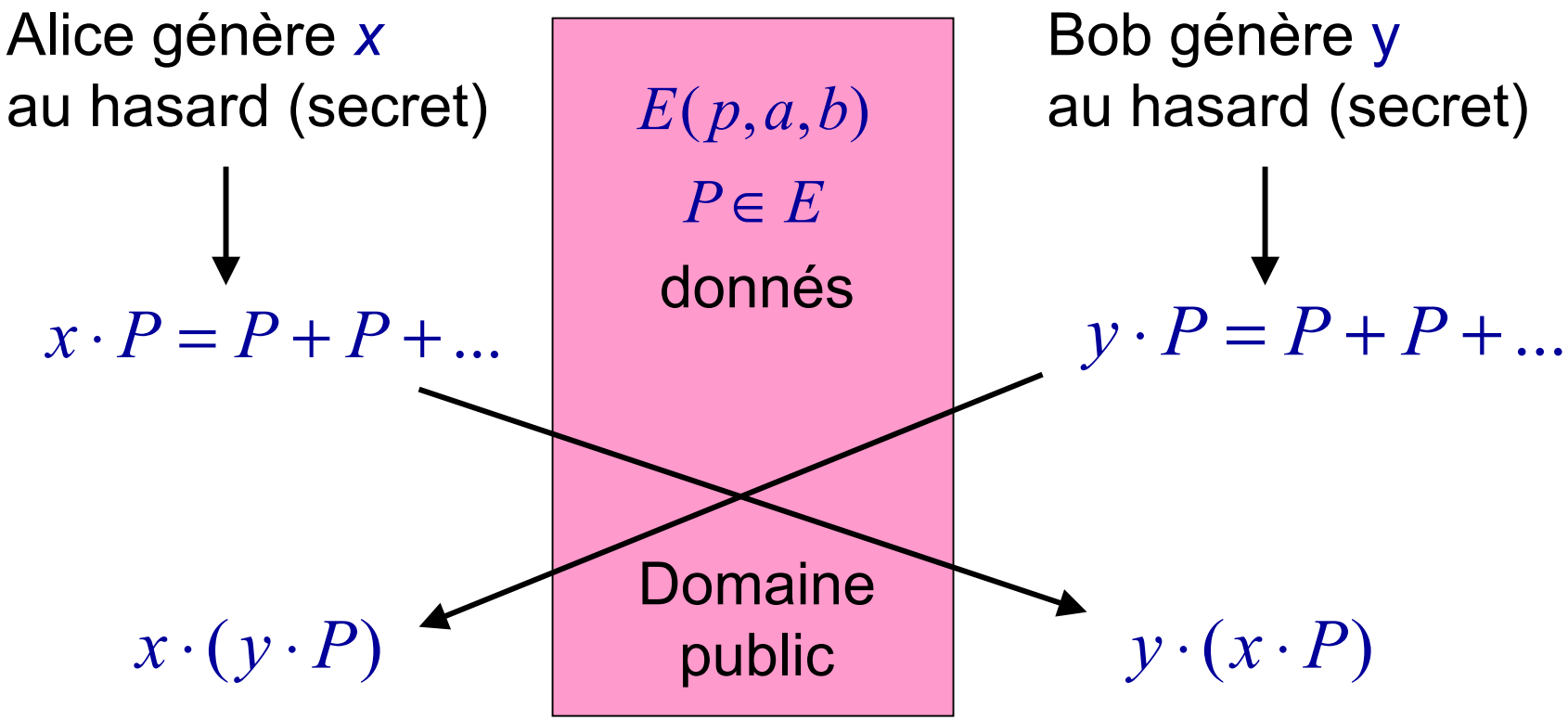
État-major général
Section cryptologie
3003 Berne

Addition sur $E: y^2 = x^3 + a \cdot x + b \bmod p$

$$p = 23, a = 19, b = 6$$



DH avec les courbes elliptiques



Clé commune: $K = xy \cdot P$

Nombre de points

- Sécurité de DH dans un groupe *G*:
  - L'ordre de *G* doit contenir un **grand nombre premier**
  - En particulier, l'ordre de *G* doit être calculé
- Pour une courbe elliptique (Th. de Hasse):

$$p+1-2\sqrt{p} \leq \#E(p,a,b) \leq p+1+2\sqrt{p}$$

- L'ordre de *G*, $\#E(p,a,b)$ peut être calculé en un temps raisonnable

Sécurité de ECC

- Menezes, Okamoto, Vanstone (MOV) 1991:
  - Réduction: DLP($E(F_p)$) → DLP(F_{p^k}).
  - Courbes supersingulières ($\#E(F_p) = p+1$) ne sont pas sûres
  - Choisir $P \in E(F_p)$ d'ordre *r*, un premier, tel que pour de petites valeurs de *k* : $p^k \neq 1 \pmod{r}$
- Smart, Satoh-Araki, 1997: $\#E(F_p) \neq p$ (non anomal)
- But: définir des courbes telles que seuls les algorithmes généraux pour résoudre le DLP peuvent être appliqués
- Complexité: $O(\sqrt{r})$ (Shanks, Pollardρ)

Baby-Step Giant-Step
(Shanks)

- Soit p un premier, α un générateur du groupe multiplicatif Z_p^* : $y = \alpha^x$, on veut trouver x
- Q le plus petit entier tel que $Q(Q+1) > p \quad \left(Q \approx \sqrt{p}\right)$
- Écrire x sous la forme $x = Qk + m, \quad 0 \le k, m < Q$

$$\alpha^{kQ} = y\alpha^{-m}$$

- Calculer et mémoriser (dans une table triée):

$$\alpha^{kQ},\ 0 \le k < Q$$

- Calculer

$$y\alpha^{-i},\ 0 \le i < Q$$

et chercher une valeur qui se trouve dans la table

Complexité des algorithmes pour résoudre le DLP

- Shanks: $O(\sqrt{p})+O(\sqrt{p})=O(\sqrt{p})$
- Pollard-ρ: $O(\sqrt{p})$, mais la mémoire nécessaire est négligeable par rapport à Shanks
- Pohlig-Hellman: $O(\sqrt{q})$, où q est le plus grand facteur premier de $n=|G|$
  - Idée:

$$n = q_1^{e_1} q_2^{e_2} \ .... \ q_r^{e_r}$$

$$G \cong G_1 \times G_2 \ldots . \times G_r \qquad |G_i| = q_i^{e_i}$$

  - Résoudre le DLP dans G_i (application du th. reste chinois)

ECDLP

Algorithme symétrique	ECC	Complexité	MIPS-years MY
80 Bit	160 Bit	2^{80}	8.5×10^{11}
96 Bit	192 Bit	2^{96}	5.6×10^{16}
112 Bit	224 Bit	2^{112}	3.7×10^{21}
128 Bit	256 Bit	2^{128}	2.4×10^{26}

CPU-Power de la planète entière en 2004 = 10^{11} MIPS (Odlyzko):
Équiv. à 10^{8} ordinateurs de 1000 MIPS chacun (IBM PC/XT = ¼ MIPS)

8.5×10^{11} MY = $8.5 \cdot 10^{11} \cdot 10^{6} \cdot 3600 \cdot 24 \cdot 365 = 2.7 \cdot 10^{25}$ instructions

10^{6} ordinateurs de 1000 MIPS chacun ont besoin de 850 ans dans le premier cas et plus de 10^{15} ans dans le dernier cas

Courbe elliptiques sur F_{q^m}

- Courbes elliptiques sur F_{q^m}, en part. sur F_{2^m}
- Arithmétique dans F_{2^m} plus simple
- Hasse: $\#E(F_q) = q + 1 - t,\ |t| \leq \sqrt{2q}$
- Calcul du nombre points est facile:

$$\#E(F_{q^m}) = q^m + 1 - \alpha^m - \beta^m$$

α, β sont les zéros du polynôme $T^2 - tT + q$

- Par un choix approprié, sécurité identique à

$$F_p,\ p \approx q^m$$

État-major général
Section cryptologie
3003 Berne

Exemple dans F_{2^m}

- Courbe de Koblitz (NIST-Standard K-163, Juil.1999):

$$E : y^2 + xy = x^3 + x^2 + 1 \qquad \#E(F_2) = 2$$

zéros du polynôme char.: $\alpha, \beta = (1 \pm \sqrt{-7})/2$

$$\#E(F_{2^{163}}) = 2 \cdot p_{49}$$

- Koblitz: calcul $\ell \cdot P$ rapide: $m \approx \log_2 \ell$
  - Methode standard: $3m/2$ EC-Additions
  - Koblitz, 1991: $3m/4$ EC-Additions
  - Meier, Staffelbach, 1992: $m/2$ EC-Additions
  - Solinas, 1997: $m/3$ EC-Additions

Résumé

- ECC: une essence nouvelle pour la cryptographie à clé publique
- ECC: clé plus courte que RSA pour la même sécurité
- EC-Arithmétique plus complexe
- RSA et ECC seront plus utilisés dans le futur
- La recherche sur les courbes elliptiques a des implications directes sur la cryptographie
- Mots-clés: Elliptic Curve Factoring Methods, Elliptic Curve Primality Tests

Littérature et informations

- A.J. Menezes, P.C. van Oorschot & S.A. Vanstone, „Handbook of Applied Cryptography“.
- A.J. Menezes, „Elliptic Curve Public Key Cryptosystems“.
- J.H. Silverman, „The Arithmetic of Elliptic Curves“.
- N. Koblitz, „Algebraic Aspects of Cryptography“.
- www.certicom.com
- www.rsa.com