

# Rapide Introduction à la Cryptographie

Jean-Claude Bajard

LIRMM - Université Montpellier 2

## Buts de la cryptographie

- Confidentialité : les informations ne sont lisibles que par les personnes autorisées
- Intégrité des données : les données transmises ne doivent pas être corrompues
- Authentification : identifier son correspondant ou l'origine des données
- Non-répudiation : fiabilité d'un document signé, ne peut pas être réfuté par son auteur.

## Terminologie

**Chiffrer - Crypter** transformation d'un message clair  $M$  en un message  $C$  appelé cryptogramme ou message chiffré, illisible par un intru.

**Déchiffrer** transformation du message chiffré  $C$  en message clair  $M$  via un secret

**Décrypter** reconstruction de  $M$  à partir de  $C$  sans connaissance préalable du secret

**Cryptanalyse** Etude de la sécurité, casser un cryptosystème

## Les premiers pas

**César** principe de substitution de caractère

**Substitutions** fréquences des occurrences de chaque caractère propres à chaque langage

**Enigma** (Scherbius - 1920) Cassée par Turing

**Stéganographie** Dissimulation d'un message (par ex dans une image)

# Les grands Principes de la cryptographie moderne

**Kerckhoffs** sécurité basée sur des clés, l'algorithme est supposé connu de tous

**Securité** déchiffrer sans la clé est impossible

**secret** la connaissance d'un message clair et de son cryptogramme ne permet pas de reconstruire la clé

## Fonction trappe

- "one-way function" : fonction facile à calculer mais dont l'inverse est très difficile (voire impossible) à trouver
  - \* Logarithme discret : Soit la fonction  $f(x) = 3^x \bmod p$  où  $x \in \{0, 1, \dots, p-1\}$  et  $p$  premier. Inverser revient pour un  $y$  donné à trouver  $z$  tel que  $3^z = y$ .
  - \* Factorisation : soit la fonction  $f(x) = x^3 \bmod n$  où  $n = pq$ , deux premiers. Inverser revient pour un  $y$  donné à trouver  $z$  tel que  $z^3 \bmod n = y$  ce qui est difficile si on ne connaît pas  $p$  et  $q$ .
- "Trapdoor one-way function" : one-way function où la connaissance d'une information rend l'inversion faisable.
  - \* Pour  $f(x) = x^3 \bmod n$  où  $n = pq$ , deux premiers. la connaissance de  $p$  et  $q$  est une trappe (plus précisément l'inverse de 3 modulo  $(p-1)(q-1)$ ).

# Cryptographie et informatique

- 1970-1977 adoption du protocole DES (Data Encryption Standard) du à Feitel
- 1976 Diffie-Hellman : échange de clés secretes et notion de clef publique
- 1978 RSA premier protocole à clefs publiques
- 1985 El-Gamal nouveau concept.
- 1985 Koblitz cryptographie sur les courbes elliptiques

# Fonction de Hachage

# Fonction de Hachage

## principes

- Transformation d'une chaîne binaire d'une longueur arbitraire en un mot d'une longueur fixée
- En cryptographie il ne faut pas de collisions facilement détectables (deux chaînes donnant le même mot)
- De plus il ne faut pas qu'il soit facile de construire une chaîne donnant un mot pré-défini.
- Utilisations: signature (ex: signature du hachage d'un fichier), intégrité (si erreur de transmission hachage différent) et identification (mot de passe)

# Algorithme MD5

## RFC 1321

### R. Rivest 1992

- 128-bit "fingerprint" or "message digest"
- message  $M = m_0m_1\dots m_{b-1}$  en mots de 32-bits
- On pré-définit
  - $z(j)$  quatre permutations de  $0\dots15$  pour  $j = 0\dots15, 16\dots31, 32\dots47, 48\dots63$
  - $s(j)$  quatre ensembles de décalages pour  $j = 0\dots15, 16\dots31, 32\dots47, 48\dots63$
  - quatre registres  $A, B, C, D$  initialisés
  - quatre fonctions  $FGHK$  à trois variables

## Algorithme MD5

1. Extension du message  $M$  pour avoir une longueur congrue à 448, modulo 512
2. Ajout de la longueur de  $M$  sur 64 bits
3. procédure : pour  $i = 0$  à  $(\text{longueur de } M)/(16 * 32)$ 

$(HA, HB, HC, HD) < -(A, B, C, D)$  Dans chaque round pour  $j$ , on effectue

$(A, B, C, D) < -(D, B + ((A + f(B, C, D) + m[16i + z(j)] + t(j)) << s(j)), B, C)$

round 1:  $j = 0...15, f = F$

round 2:  $j = 16...31, f = G$

round 3:  $j = 32...47, f = H$

round 4:  $j = 48...63, f = K$

$(A, B, C, D) < -(HA + A, HB + B, HC + C, HD + D)$

# Algorithme MD5

## Propriétés

- Collision possible (crypto 2004)
- Bonne confusion ( non conservation de motifs)
- Bonne diffusion (un caractère différent tout diffère)
- Un peu court pour résister à certaines attaques (anniversaires)
- A l'avenir SHA-256 ou SHA-384

# Cryptographie à clé privée

# Types de protocoles

## Clés symétriques- clés secrètes

$$A : E(K_s, M) = C \longrightarrow C \longrightarrow B : D(K_s, C) = M$$

- $K_s$  secret commun à A et B
- modes d'utilisation:
  - \* chiffrement par bloc
  - \* chiffrement par flot
  - \* signature
- Problèmes de l'échange des clés, du partage par plusieurs personnes du secret.

## Chiffrement par flot

Le message est découpé en blocs réguliers (généralement de petite taille: bit , octet), puis chaque bloc est chiffré différemment.

- Notion de clé de la longueur du message  $k = e_1e_2\dots$  (générateur aléatoire)
- Chiffrement des blocs avec les éléments de la clé:  $c_i = E_{e_i}(m_i)$
- Exemple : simple xor avec une clé générée par une fonction pseudo-aléatoire

## Chiffrement par bloc (DES, AES)

Le message est découpé en blocs réguliers, puis chaque bloc est chiffré de la même façon.

- Permutation des éléments

- "ou exclusif" avec une clé  $k$

- Exemple :

$M$ (messages) =  $C$  (mots chiffrés) =  $K$ (clés) ensemble des mots de six chiffres binaires. soit le bloc de six lettres:  $m = (m_1 m_2 \dots m_6)$

on définit

$$E_k^1(m) = m \oplus k \text{ avec } k \in K$$

$$E^2(m) = (m_4 m_5 m_6 m_1 m_2 m_3)$$

La composée  $E_k^1 \circ E^2$  forme un tour élémentaire.

## Rijndael - AES - NIST 2000

- Longueur de bloc et de clé indépendamment de 128, 192 or 256 bits.
- Etat : matrice d'octets de quatre lignes et (longueur du bloc)/32 colonnes
- Clé de chiffrage : matrice d'octets de quatre lignes et (longueur clé)/32 colonnes

$$\begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} & a_{04} & a_{05} \\ a_{10} & a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{20} & a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{30} & a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \end{pmatrix} \begin{pmatrix} k_{00} & k_{01} & k_{02} & k_{03} \\ k_{10} & k_{11} & k_{12} & k_{13} \\ k_{20} & k_{21} & k_{22} & k_{23} \\ k_{30} & k_{31} & k_{32} & k_{33} \end{pmatrix}$$

## Rijndael - AES algorithme

Il est basé sur un principe de "round"

```
Round(State, RoundKey)
{
ByteSub(State); (  $GF(2^8)$  )
ShiftRow(State);
MixColumn(State); (sauf final) (polynôme de  $GF(2^8)$ )
AddRoundKey(State, RoundKey);
}
```

où RoundKey est une matrice de même taille que l'état, qui est générée par la clé de chiffrement.

## Rijndael - AES algorithme

Le nombre de tours est défini par rapport aux attaques possibles

Nr	Nb = 4	Nb = 6	Nb = 8
Nk = 4	10	12	14
Nk = 6	12	12	14
Nk = 8	14	14	14

## Rijndael - AES propriétés

- L'inverse est obtenu en inversant simplement le processus des rounds avec les procédures inverses
- l'extension de la clé élimine les symétries, les attaques avec connaissance partielle de la clé,...
- nombre de tours : diffusion (deux tours), attaques linéaires (corrélation entrée-sortie), attaques différentielles, propagation de motifs, attaques quadratiques, interpolation

# Cryptographie à clé publique

## Types de protocoles

### Clés asymétriques- clés publiques

$$A : E(K_{pB}, M) = C \longrightarrow C \longrightarrow B : D(K_{sB}, C) = M$$

- clé publique de B  $K_{pB}$   
clé secrète de B  $K_{sB}$

- modes d'utilisation:

- \* chiffrement
- \* signature - authentification

$$B : D(K_{sB}, M) = C \longrightarrow C \longrightarrow A : E(K_{pB}, C) = M$$

# Cryptographie à clés publiques

Diffie-Hellman	partage d'un secret	problème du logarithme discret
RSA	chiffrement, authentification	problème de la factorisation d'entier
ElGamal		discrete logarithm problem
McEliece	chiffrement	linear code decoding problem

- échange de clés publiques sans contrainte
- partage des clés publiques
- Problème de l'authentification

## Rappels sur le calcul modulaire 1

**Calcul modulaire:** choix d'un entier  $n$ , toutes les opérations sont faites modulo  $n$  c'est à dire sur les restes de la division euclidienne par  $n$ . Ceci revient à définir des opérations d'addition et de multiplication dans l'ensemble  $\mathbb{Z}_n = \{0, 1, 2, \dots, n - 1\}$ .

$$12345 + 98765 \bmod 1111111 = 111110$$

$$12345 * 98765 \bmod 1111111 = 365158$$

**L'inverse d'un nombre  $x$  modulo  $n$ :** Si  $x$  est premier avec  $n$  alors il existe  $y$  tel que  $x * y \bmod n = 1$ ,  $y$  est l'inverse de  $x$  modulo  $n$  (algorithme D'Euclide étendu)

$$12345^{-1} \pmod{1111111} = 145718$$

$$(12345 * 145718 - 1) = 1111111 * 1619$$

## Rappels sur le calcul modulaire 2

$\phi(n)$  **fonction d'Euler** donnant le nombre de nombres premiers avec  $n$ , plus petits que  $n$

**Théorème de Fermat**, pour tout entier  $x$  premier avec  $n$  nous avons,  
 $x^{\phi(n)} = 1 \pmod n$

### Exemples

$$\phi(1111111) = 1106224$$

$$12345^{1106224} \pmod{1111111} = 1 \text{ et } 98765^{1106224} \pmod{1111111} = 1$$

## Rappels sur le calcul modulaire 3

**Générateur** lorsque  $p$  est premier il existe  $g$  tel que tout élément de  $\mathbb{Z}_p^* \{1, 2, \dots, p-1\}$  s'écrit sous la forme d'une puissance de  $g$  modulo  $p$ : les puissances de  $g$  génèrent  $\mathbb{Z}_p^*$

### Exemples

$$p = 13 \text{ et } g = 2$$

$x$	1	2	3	4	5	6	7	8	9	10	11	12
$g^x$	2	4	8	3	6	12	11	9	5	10	7	1

## Rappels sur le calcul modulaire 4

### Euclide étendu

- initialisation

$$(u_1, u_2, u_3) \leftarrow (1, 0, n)$$

$$(v_1, v_2, v_3) \leftarrow (0, 1, a)$$

- itération tant que  $v_3 \neq 0$  :  $q = \lfloor u_3 \div v_3 \rfloor$

$$(t_1, t_2, t_3) \leftarrow (u_1, u_2, u_3) - q \times (v_1, v_2, v_3)$$

$$(u_1, u_2, u_3) \leftarrow (v_1, v_2, v_3)$$

$$(v_1, v_2, v_3) \leftarrow (t_1, t_2, t_3)$$

## Diffie-Hellman : établissement d'une clé secrète

1. Choix d'un nombre premier  $\mathbf{p}$  et d'un générateur  $\mathbf{g}$  de  $\mathbb{Z}_p^*$
2.  $\mathbf{p}$  et  $\mathbf{g}$  sont publiques
3. Correspondant A choisit un entier  $\mathbf{x}$   
envoie  $\mathbf{a} = \mathbf{g}^{\mathbf{x}} \bmod \mathbf{p}$  à B
4. De même, B choisit  $\mathbf{y}$  et envoie  $\mathbf{b} = \mathbf{g}^{\mathbf{y}} \bmod \mathbf{p}$  à A
5. A construit  $\mathbf{k} = \mathbf{b}^{\mathbf{x}} \bmod \mathbf{p}$
6. B construit  $\mathbf{k}' = \mathbf{a}^{\mathbf{y}} \bmod \mathbf{p}$
7.  $\mathbf{k} = \mathbf{k}'$  clé secrète commune

## Diffie-Hellman : établissement d'une clé secrète (exemple)

1.  $p = 11111117$  et  $g = 111112$
2. A calcule  $a = 111112^{1234} \bmod 11111117 = 7218868$
3. et B  $b = 111112^{876} \bmod 11111117 = 8671412$
4. A calcule  $k = 8671412^{1234} \bmod 11111117 = 6146319$
5. et B  $k' = 7218868^{876} \bmod 11111117 = 6146319$

# RSA (Rivest Shamir Adleman) Fabrication de deux clés

## Le destinataire :

1. choisit deux grands nombres premiers  $p$  et  $q$
2. construit  $n = p * q$  et  $\phi(n) = (p - 1)(q - 1)$
3. choisit  $e$  premier avec  $\phi(n)$
4. calcule  $d$  l'inverse de  $e$  modulo  $\phi(n)$

la **clé publique** que les correspondants utiliseront pour chiffrer le message est  $(n, e)$

la **clé privée** que le destinataire utilisera pour déchiffrer est  $d$

# RSA (Rivest Shamir Adleman) Protocole

## L'expéditeur:

1. a un message  $m$ ,  $m < n$  (sinon découpe)
2. calcule  $c = m^e \bmod n$
3. envoie  $c$

## Le destinataire

1. reçoit  $c$
2. calcule  $m = c^d \bmod n$

## RSA (Rivest Shamir Adleman) Exemple

$$1111111 = 239 * 4649 \text{ et } \phi(1111111) = 238 * 4648 = 1106224$$

$$e = 5 \text{ d'où } d = 5^{-1} \text{ mod } 1106224 = 221245$$

### L'expéditeur:

1.  $m = 999999$ ,
2.  $c = 999999^5 \text{ mod } 1111111 = 761766$

### Le destinataire

1. cal  $m = 761766^{221245} \text{ mod } 1111111 = 999999$

## El-Gamal fabrication de la clé

Inspiré de Diffie-Hellman

### Destinataire

1. Choisit un nombre premier  $p$  et un générateur  $g$  de  $\mathbb{Z}_p$
2. sélectionne aléatoirement un nombre  $a \in \mathbb{Z}_p$
3. publie  $(p, g, g^a \bmod p)$

## El-Gamal protocole

### Expéditeur:

1. soit  $m$  le message avec  $m < p$  choisit **aléatoirement** un entier  $b \in \mathbb{Z}_p^*$
2. calcule  $c_1 = g^b \bmod p$  et  $c_2 = m \cdot (g^a)^b \bmod p$
3. envoie  $c = (c_1, c_2)$

### Destinataire :

1. calcule  $d_1 = (c_1)^{p-1-a} \bmod p = (c_1)^{-a} \bmod p = g^{-ab} \bmod p$
2. puis calcule  $d_2 = d_1 \cdot c_2 \bmod p = g^{-ab} \cdot m \cdot (g^a)^b \bmod p = m$

## El-Gamal exemple

1.  $p = 11111117$  ,  $g = 111112$  et  $a = 1234$
2. A calcule  $k_a = 111112^{1234} \bmod 11111117 = 7218868$
3. A publie  $p = 11111117, g = 111112, k_a = 7218868$

## El-Gamal exemple

1. B choisit  $b = 876$  et  $a$  pour message 99999
  2. B calcule  $c_1 = 111112^{876} \bmod 1111117 = 8671412$
  3. et  $c_2 = 99999 \cdot 7218868^{876} \bmod 1111117 = 3205709$
  4. B envoie  $(8671412, 3205709)$
- 
1. A calcule  $d_1 = 8671412^{-1234} \bmod 1111117 = 5300581$
  2. et  $d_2 = 5300581 * 3205709 \bmod 1111117 = 99999$

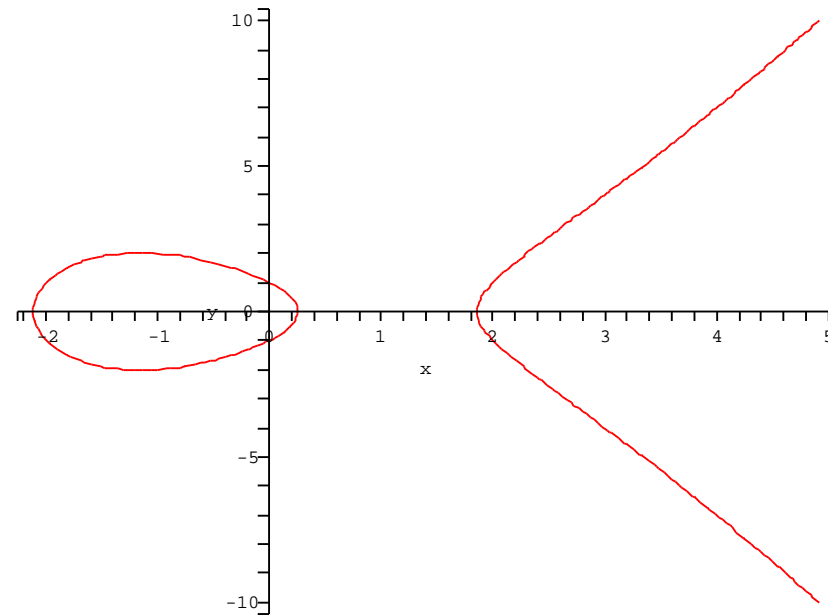
# Courbes elliptiques

- L'équation générale d'une courbe elliptique :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

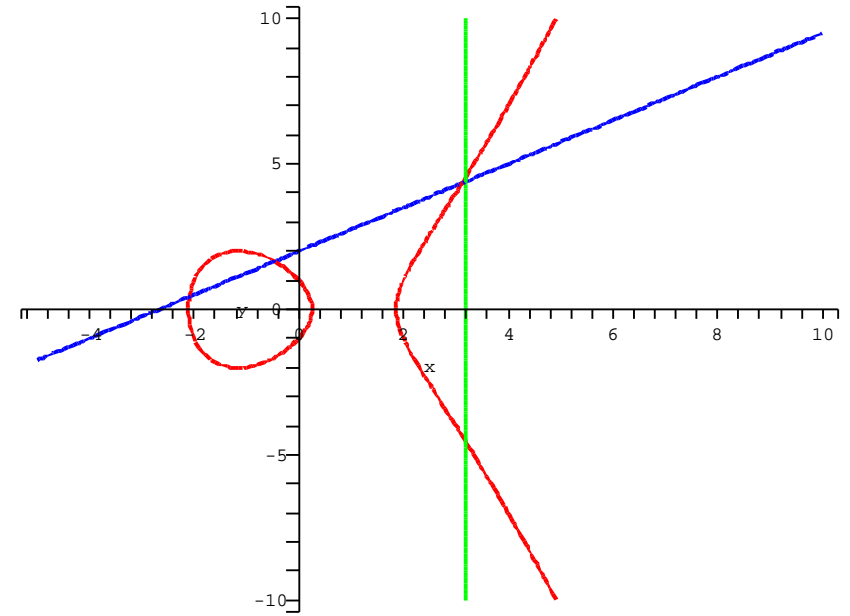
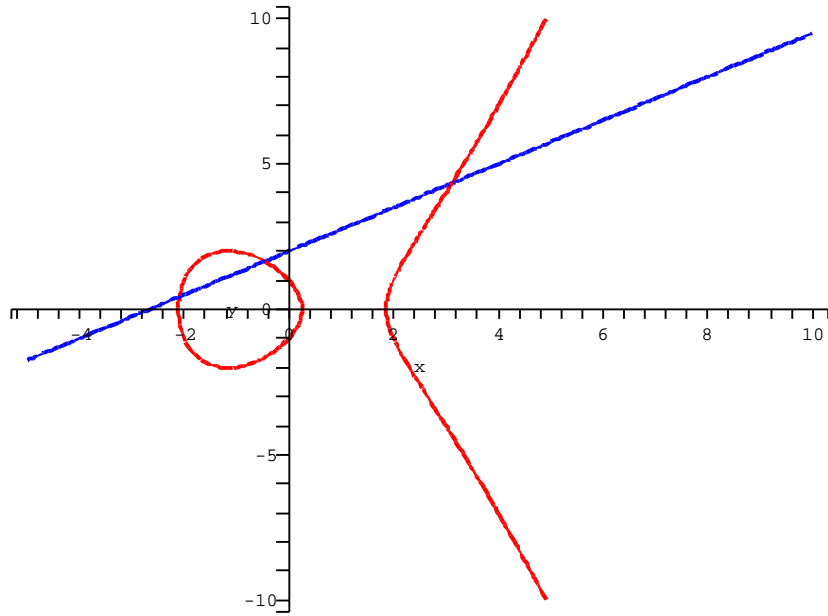
- Loi de groupe sur les points
- Application à la crypto: 1985 Neal Koblitz (University of Washington), et Victor Miller (IBM, Yorktown Heights).

## Exemple de courbe dans $\mathcal{R}$



$$y^2 = x^3 - 4x + 1$$

# Exemple d'addition



## Loi de groupe

- $P_1 + P_2 = P_3$  trois points de la courbe tels que:  $P_1$ ,  $P_2$  et  $-P_3$  sont alignés
- $P_1 (x_1, y_1)$ ,  $P_2 (x_2, y_2)$  et  $P_3 (x_3, y_3)$ 
  - \* Si  $P_1 \neq P_2$  alors  $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$
  - \* Si  $P_1 = P_2$  alors  $\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_2x_1 + a_3}$

et

- \*  $x_3 = -x_1 - x_2 - a_2 + \lambda(\lambda + a_1)$
- \*  $y_3 = -y_1 - a_3 - a_1x_3 + \lambda(x_1 - x_3)$

## Diffie Hellman sur les courbes elliptiques

1. Choix d'une courbe elliptique  $E$  sur un corps fini et d'un point générateur  $\mathbf{P}$  de  $E$
2.  $E$  et  $P$  sont publiques
3. Correspondant A choisit un entier  $x$   
envoie  $\mathbf{P}_a = x\mathbf{P}$  à B
4. De même, B choisit  $y$  et envoie  $\mathbf{P}_b = y\mathbf{P}$  à A
5. A construit  $\mathbf{K} = x\mathbf{P}_b$
6. B construit  $\mathbf{K}' = y\mathbf{P}_a$
7.  $\mathbf{K} = \mathbf{K}'$  clé secrète commune

## El Gamal sur les courbes elliptiques

**Destinataire** : publie  $(\mathbf{E}, \mathbf{P}, \mathbf{P}_a)$

**Expéditeur**:

1. soit  $m$  le message traduit en point  $P_m$  choisit **aléatoirement** un entier  $y$
2. calcule  $\mathbf{P}_1 = y\mathbf{P}$  et  $\mathbf{P}_2 = \mathbf{P}_m + y\mathbf{P}_a$
3. envoie  $P_c = (P_1, P_2)$

**Destinataire** :

1. calcule  $\mathbf{P}_3 = \mathbf{a}(-\mathbf{P}_1) = -xy\mathbf{P}$
2. puis calcule  $\mathbf{P}_4 = \mathbf{P}_3 + \mathbf{P}_2 = \mathbf{P}_m$

## Dans $GF(p^k)$ pour $p \neq 2, 3$

- Forme simplifiée de l'équation de la courbe

$$y^2 = x^3 + a_4x + a_6$$

- Addition

- \* Si  $P_1 \neq P_2$  alors  $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$
- \* Si  $P_1 = P_2$  alors  $\lambda = \frac{3x_1^2 + a_4}{2y_1}$

et

- \*  $x_3 = -x_1 - x_2 + \lambda^2$
- \*  $y_3 = -y_1 + \lambda(x_1 - x_3)$

## Dans $GF(2^k)$

- Forme simplifiée de l'équation

$$y^2 + xy = x^3 + a_2x^2 + a_6$$

- Addition

- \* Si  $P_1 \neq P_2$  alors  $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$
- \* Si  $P_1 = P_2$  alors  $\lambda = x_1 + \frac{y_1}{x_1}$

et

- \*  $x_3 = x_1 + x_2 + a_2 + \lambda^2 + \lambda$
- \*  $y_3 = y_1 + x_3 + \lambda(x_1 + x_3)$

## Valeurs dans $GF(p^k)$ : forme polynomiale

- Les éléments de  $GF(p^k)$  sont des polynômes de degré inférieur à  $k$  à coefficients dans  $GF(p)$ .
- Les opérations d'additions et soustractions se font sur les coefficients de même degré modulo  $p$ .
- La multiplication et l'inversion sont faites modulo un polynôme irréductible de degré  $k$

## Opérations dans $GF(p^k)$ : forme polynomiale

- Soit  $F(x) = x^k + f_{k-1}x^{k-1} + \dots + f_2x^2 + f_1x^1 + f_0$  un polynôme irréductible
- Soient  $A(x) = a_{k-1}x^{k-1} + \dots + a_2x^2 + a_1x^1 + a_0$   
et  $B(x) = b_{k-1}x^{k-1} + \dots + b_2x^2 + b_1x^1 + b_0$ 
  - \*  $A(x) + B(x) = |a_{k-1} + b_{k-1}|_p x^{k-1} + \dots + |a_1 + b_1|_p x + |a_0 + b_0|_p$
  - \*  $A(x) \times B(x) = (|a_{k-1} * b_{k-1}|_p x^{2k-2} + \dots + |a_0 * b_0|_p) \bmod F(x)$

## Dans $GF(2^4)$

Les éléments sont:

(0000) (0001) (0010) (0011) (0100) (0101) (0110) (0111)

(1000) (1001) (1010) (1011) (1100) (1101) (1110) (1111)

$F(x) = x^4 + x + 1$  est irréductible.

Addition  $(0110) + (0101) = (0011)$ .

## Dans $GF(2^4)$

### Multiplication

$$\begin{aligned} & (1101)(1001) \\ = & (x^3 + x^2 + 1)(x^3 + 1) \bmod F(x) \\ = & x^6 + x^5 + 2x^3 + x^2 + 1 \bmod F(x) \\ = & x^6 + x^5 + x^2 + 1 \bmod F(x) \\ = & (x^4 + x + 1)(x^2 + x) + (x^3 + x^2 + x + 1) \bmod F(x) \\ = & x^3 + x^2 + x + 1 \\ = & (1111) \end{aligned}$$

## Dans $GF(2^4)$

Inversion  $g = (0010)$  generateur du corps.

$$g^0 = (0001); g^1 = (0010); g^2 = (0100); g^3 = (1000)$$

$$g^4 = (0011); g^5 = (0110); g^6 = (1100); g^7 = (1011)$$

$$g^8 = (0101); g^9 = (1010); g^{10} = (0111); g^{11} = (1110)$$

$$g^{12} = (1111); g^{13} = (1101); g^{14} = (1001); g^{15} = (0001)$$

Élément neutre :  $g^0 = (0001)$ .

L'inverse de  $g^7 = (1011)$  is  $g^{-7} \bmod 15 = g^8 \bmod 15 = (0101)$ .

## Conclusion

- produit de grands nombres, réduction modulaire
- produit modulaire sur de grands nombres
- exponentiation modulaire
- idem sur les corps finis