Sécurité et Cryptographie

Matthieu Basseur

Introduction à la cryptographie

Sommaire

- Un premier exemple
- Sécurité et crytpographie?
- Définitions/Généralités
- La cryptographie classique

Exemple de message crypté

- Déchiffer le message suivant :
  - « CPOKPVS MF NPOEF »
- Indice n°1 : les espaces restent des espaces
- Indice n°2 : l'alphabet a été décalé
- Clé : chaque lettre a été décalée d'un rang
  - Message clair: « BONJOUR LE MONDE »

Deuxième exemple

- Déchiffer le message suivant :
  - « FH WHAWH HVW FKLIIUH SDU FHVDU »
- Indice n°1 : les espaces restent des espaces
- Indice n°2 : l'alphabet a été décalé
- Clé : chaque lettre a été décalée de 3 rangs
  - Message clair: « CE TEXTE EST CHIFFRE PAR CESAR »

Sommaire

- Un premier exemple
- Sécurité et crytpographie?
- Définitions/Généralités
- La cryptographie classique

Sécurité?

- Pourquoi de la sécurité informatique ?
  - l'informatique est omniprésente, dans des secteurs de plus en plus critiques
  - certaines dimensions changent dans le monde virtuel : l'espace, le temps… ainsi que les ordres de grandeurs ; par conséquent le danger des attaques aussi
  - les menaces pour les libertés professionnelles et individuelles sont réelles → la sécurité informatique devient primordiale

Vocabulaire

- sûreté : protection contre les actions non intentionnelles
- sécurité : protection contre les actions intentionnelles malveillantes
- menace : moyen potentiel par lequel un attaquant peut attaquer un système
- risque : prise en compte à la fois la probabilité d'une menace et de sa gravité si elle réussit

Les objectifs théoriques

- authentifier les utilisateurs, gérer leurs autorisations
- assurer la confidentialité et l'intégrité des données et des communications
- assurer la disponibilité des services

Difficultés

- historiques : Internet n'a pas été conçu en tenant compte de contraintes de sécurité
- législatives : retard du législatif sur la technologie, diversité des législations nationales
- économiques :
  - la sécurité informatique est coûteuse et sans bénéfices visibles directs
  - les attaques informatiques sont de plus en plus motivées par des gains financiers (« intelligence économique », spam…)
- humaines et organisationnelles : formation, responsabilisation (cf. l'ingénierie sociale)

Difficultés

- évolution permanente et soutenue (cf. attaques virales)
- systèmes très complexes, non séquentiels et couplés
- «le niveau de sécurité d'un système est caractérisé par le niveau de sécurité du maillon le plus faible »

→ Utilisation de systèmes de cryptages sûrs (peu sensibles aux attaques extérieures)

Sommaire

- Un premier exemple
- Sécurité et crytpographie?
- Définitions/Généralités
- La cryptographie classique

Introduction

- Un système cryptographique est un quintuplet S={P, C, K, E, D} avec:
  - P : ensemble fini de clairs (*plain texts*)
  - C : ensemble fini de chiffrés (*cipher texts*)
  - K : ensemble fini de clés (*key space*)
  - E : ensemble fini de règles de chiffrement (*encryption rules*)
  - D : ensemble fini de règles de déchiffrement (*decryption rules*)

$$\forall k \in K, \exists e_k \in E \text{ tel que } e_k : P \to C,$$
$$\exists d_k \in D \text{ tel que } d_k : C \to P \text{ et}$$
$$d_k \circ e_k = id_P \qquad (1)$$

Protocole

1. Alice et Bob conviennent de S.

2. Ils choisissent leur(s) clé(s).

3. Alice chiffre le clair $x = x_1x_2...x_n$, $x_i \in P$ en $y = y_1y_2...y_n$, $y_i \in C$ avec $y_i = E_K(x_i)$ et l'envoie à Bob.

4. Bob calcule $\forall i,\ x_i = D_K(y_i)$ c'est à dire x et retrouve ainsi le clair à partir du chiffré.

Remarque : x n'appartient pas à P, mais est un mot constitué d'éléments de l'alphabet P (les x_i ci-dessus).

Sommaire

- Un premier exemple
- Sécurité et crytpographie?
- Définitions/Généralités
- La cryptographie classique
  - Chiffrement par transposition
  - Chiffrement par substitution

Transposition par blocs

- Chaque bloc de n lettres est mélangé d'une certaine manière
  - Exemple: blocs de 3*3

```
DIEU EST LE POINT TANGENT ENTRE ZERO ET LINFINI
```

DIE U E ST	LE POI NT	TAN GEN T E	NTR E Z ERO	ET LI NFI	NI

- On lit ensuite par colonne:

```
DUSI TEE LPNEOT I TGTAE NNENEET RRZO  NELFTIIN  I
```

- Cheminement inverse pour reconstruire le message clair

Transposition avec clé simple

- Ex: k=FAUSTROLL (9 lettres→9 colonnes)

```
DIEU EST LE POINT TANGENT ENTRE ZERO ET L INFINI
```

```
DIEU EST
LE POINT
TANGENT E
NTRE ZERO
 ET LINFI
NI
```

- On lit par colonne, dans l'ordre défini par la clé :

```
FAUSTROLL
219786534
```

(Ordre alphabétique)

- On obtient :

```
IEATEIDLTN NTT RF   EOI SNTEN EINZI UPGE   OE L E NRT
```

Sommaire

- Un premier exemple
- Sécurité et crytpographie?
- Définitions/Généralités
- La cryptographie classique
  - Chiffrement par transposition
  - Chiffrement par substitution

Chiffrement par décalage

- $P=C=K=\mathbb{Z}/26\mathbb{Z}$
- $\forall k \in K,\ x \in P,\ e_k(x)=x+k=y,\ d_k(y)=y-k=x$
- Vérifions (1): $d_k \circ e_k(x) = d_k(x+k)=x+k-k=x$
- Cas du chiffrement de César
  - k=3
  - La transposition des caractères est la suivante:

$$\begin{pmatrix} A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z \\ D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z,A,B,C \end{pmatrix}$$

Substitution affine

- $P=C=\mathbb{Z}/26\mathbb{Z}$
- $K=\mathbb{Z}^*/26\mathbb{Z}.\mathbb{Z}/26\mathbb{Z}$
- $\forall\ k=(a,b)\in K,\ x\in P,$
  $e_K(x)=ax+b=y,\ d_K(y)= a^{-1}(x-b)= x$
- vérifions (1) : $d_K o e_K(x)= a^{-1}((ax+b)-b)= x$
  - Possible si $\mathrm{pgcd}(a,26)=1$!

- Exemple: K=(3,12)
  - La transposition des caractères est la suivante:

$$\begin{pmatrix} A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z \\ O,R,U,X,A,D,G,J,M,P,S,V,Y,B,E,H,K,N,Q,T,W,Z,C,F,I,L \end{pmatrix}$$

Substitution par permutation

- $P=C=\mathbb{Z}/26\mathbb{Z}$
- $K=(\mathbb{Z}/26\mathbb{Z})^{26}$, $|K|=26!$ (clé de 26 caractères)
- Soit Π une permutation:
  - Soit $x \in P$, $e_K(x)=\Pi(x)=y$, $d_K(y)=\Pi^{-1}(y)=x$
- vérifions (1) : $d_K o e_K(x)=\Pi^{-1}\Pi(x)=x$
- Exemple:
  - $\Pi(x)=$

$$\begin{pmatrix} A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z \\ D,X,Y,W,V,H,N,A,I,B,T,U,G,S,C,R,O,J,Q,P,E,Z,K,F,M,L \end{pmatrix}$$

  - **x= « CE TEXTE EST CHIFFRE PAR SUBSTITUTION »**
  - **Y= « YV PVFPV VQP YAIHHJV RDJ QEXQPIPEPICS »**

Chiffrement de Vigenère (XVI^{ème} siécle)

- $P=C=(\mathbb{Z}/26\mathbb{Z})^m$
  - m introduit la notion de chiffrement *poly-alphabétique* par bloc, le texte clair est découpé en blocs de taille m
- $|K|=26^m$ (clé=mot de taille m)
- $k=(k_1,k_2,\ldots,k_m)\in K$, $x=(x_1,x_2,\ldots,x_m)\in P$, $y=(y_1,y_2,\ldots,y_m)\in C$.
- $e_k(x)=(x_1+k_1,x_2+k_2,\ldots,x_m+k_m)=y$
- $d_k(y)=(y_1-k_1,y_2-k_2,\ldots,y_m-k_m)=x$
- (1) est vérifié aisément

Chiffrement de Vigenère

- Exemple:
  - K=« CHIFFRE »
  - Message: « CE TEXTE EST CHIFFRE PAR VIGENERE »
    (on simplifie par: « CETEXTEESTCHIFFREPARVIGENERE »)
- Codage:

```
  CHIFFRECHIFFRECHIFFRECHIFFRE
+ CETEXTEESTCHIFFREPARVIGENERE
= FMCKDLJHACINAKIZNVGJALONTKJJ
```

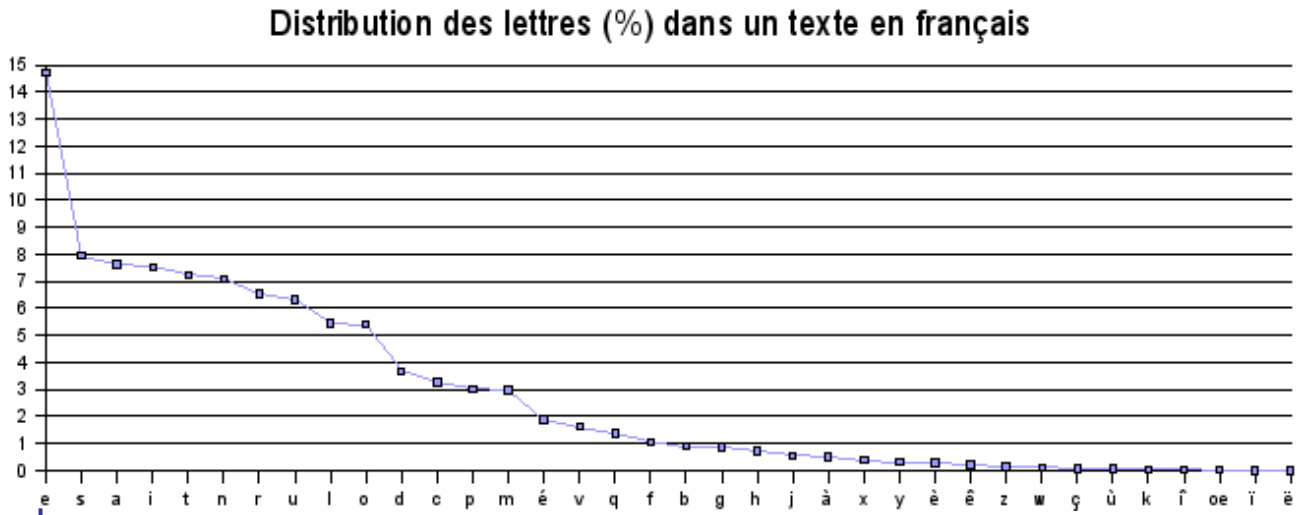
Cryptanalyse

- Cryptanalyse des substitutions mono-alphabetique
  - Rappel : substitution mono-alphabetique : on remplace chaque lettre par une lettre différente (césar, affine…).
  - Nombre de possibilités (alphabet de 26 lettres) ?
    - chiffrement de A : 26 possibilités
    - chiffrement de B : 25 possibilités
    - ... →26! $4*10^{26}$ possibilités
  - Ordre de grandeur de comparaison : plier 50 fois sur elle-même une feuille de papier (épaisseur : 1 dixième de mm)
    - épaisseur de la feuille : 250 dixièmes de millimétre 1,1 $*10^{8}$ kms (110 millions de km 300 fois distance Terre/Lune)

Cryptanalyse

- Cryptanalyse des substitutions mono-alphabétique
  - MAIS ne cache pas la fr équence d'apparition des symboles !
  - En francais, la lettre ‘e’ apparaît le plus souvent etc...
- Exemple : cryptanalyse du texte suivant :

  HQYRBHU GX UHQIRUW DYHF GHV DUPHV
  - Réponse : « envoyer du renfort avec des armes »
- Cryptanalyse proposée par Al Kindi au IXe siècle.



Cryptanalyse

- Cryptanalyse des substitutions poly-alphabétique
  - ne cache pas non plus la fréquence d'apparition des symboles !
- On connaît la longueur de la clé n
  - On réarrange le cryptogramme en n groupes de lettres
  - On applique l'analyse statistique classique sur chaque groupe
- On ne connaît pas la longueur de la clé
  - On cherche à la découvrir!
  - On applique l'analyse statistique classique sur chaque groupe

Cryptanalyse

- Cryptanalyse des substitutions poly-alphabétique (ex: vigenère)
  - Considérons par exemple le message codé suivant :

```
CS AZZMEQM, CO XRWF, CS DZRM GFMJECV. X'IMOQJ JC LB
NLFMK CC LBM WCCZBM KFIMSZJSZ CS URQIUOU.
CS ZLPIE ECZ RMWWTV, SB KCCJ QMJ FCSOVJ GCI ZI ICCKS...
```

  - Idée : une séquence se répète! La distance entre 2 séquences est probablement un multiple de la taille de la clef

Séquence	Position	Distance	Décomposition
COX	11-140	129	3.43
FCS	16-99	83	83
ZRM	20-83	63	$3^2 7$
FMJ	24-162	138	2.3.23
CLB	37-46	9	3^2
KCC	44-92	48	$2^3 3$
WTV	87-133	46	2.23
CCJ	93-126	33	3.11
ICC	110-155	45	$3^2.5$
MJI	136-163	27	3^3

pgcd pour les triplets 'pertinents' : 3

Cryptanalyse

- Cryptanalyse des transpositions
  - Méthode repérable grâce aux fréquences d'apparition des lettres
  - Problème : clé visible pour les messages courts
  - Difficulté de création de clés complexe (sinon facile à déchiffer en cherchant uniquement la taille des blocs)
  - Attaques par inversion de matrices…

Notion de sécurité inconditionnelle

- Cryptanalyses précédentes utilisent la répétition de la clé
- Définition (Sécurité inconditionnelle) :
  la connaissance du message chiffré n'apporte aucune information sur le message clair.
  - seule attaque possible : recherche exhaustive de clé secrète
  - la clé secrète doit être au moins aussi longue que le texte clair
- Existe-t-il un syteme cryptographique inconditionnellement sûr ?

Système cryptographique sûr

- Alice et Bob veulent s'échanger des données à l'aide de la méthode du masque jetable (Vernam) appelée aussi *One Time Pad*.
- One Time Pad : Xor entre une suite de bits aléatoires et le texte à chiffrer : $chiffre_t := clair_t \oplus alea_t$
- Pb : Alice et Bob doivent posséder la même suite de bits aléatoires pour pouvoir décoder : $clair_t := chiffre_t \oplus alea_t$

Opération « ou exclusif » : ⊕

⊕	0	1
0	0	1
1	1	0

Systèmes cryptographiques pratiquement sûr

- Vernam : seul système prouvé inconditionnellement sûr
  - MAIS problème du caractère aléatoire et du stockage de K
  - tous les autres systèmes sont théoriquement cassables
- Définition (chiffrement pratiquement sûr) :
  - un message chiffré ne permet de retrouver ni la clé secrète ni le message clair en un temps humainement raisonnable

  → permet d'utiliser des clés plus petites (56, 128 bits...)
- Cryptographie classique : système non sûr
  - Cryptanalyse statistiques etc…
  - Toujours possible lorsqu'on acumule des messages cryptés/clairs
    - Exemple : Enigma (3, puis 5 susbtitutions polyalphabétiques)

Systèmes cryptographiques pratiquement sûr

- 1977 : standard de chiffrement DES (56 bits)
  - basé sur des opérations facilement applicables (par blocs)
  - résultat du chiffrement statistiquement plat
  - utilisé dans les cartes à puces etc...
  - problème : clé devenu trop petite
    - cassable en 8h avec 100 PCs : ($2^{56} \approx 7.2 * 10^{16}$)

$$\frac{7.2 \bullet 10^{16}}{10^9 \bullet 3600 \bullet 24 \bullet 100} \approx 8 \text{ jours}$$

- depuis 2000 : nouveau standard A.E.S. (128, 192, 256 bits)
- Autres exemples de systèmes de chiffrement à clé secrète :
  - IDEA (1992) : blocs de 64 bits, clé de 128 bits ;
  - Triple DES à deux clés : blocs de 64 bits, clé de 112 bits :
    - C = EK1 (DK2 (EK1 (M)))
    - M = DK1 (EK2 (DK1 (C)))
- Chiffrement à clé publique: RSA (1976)

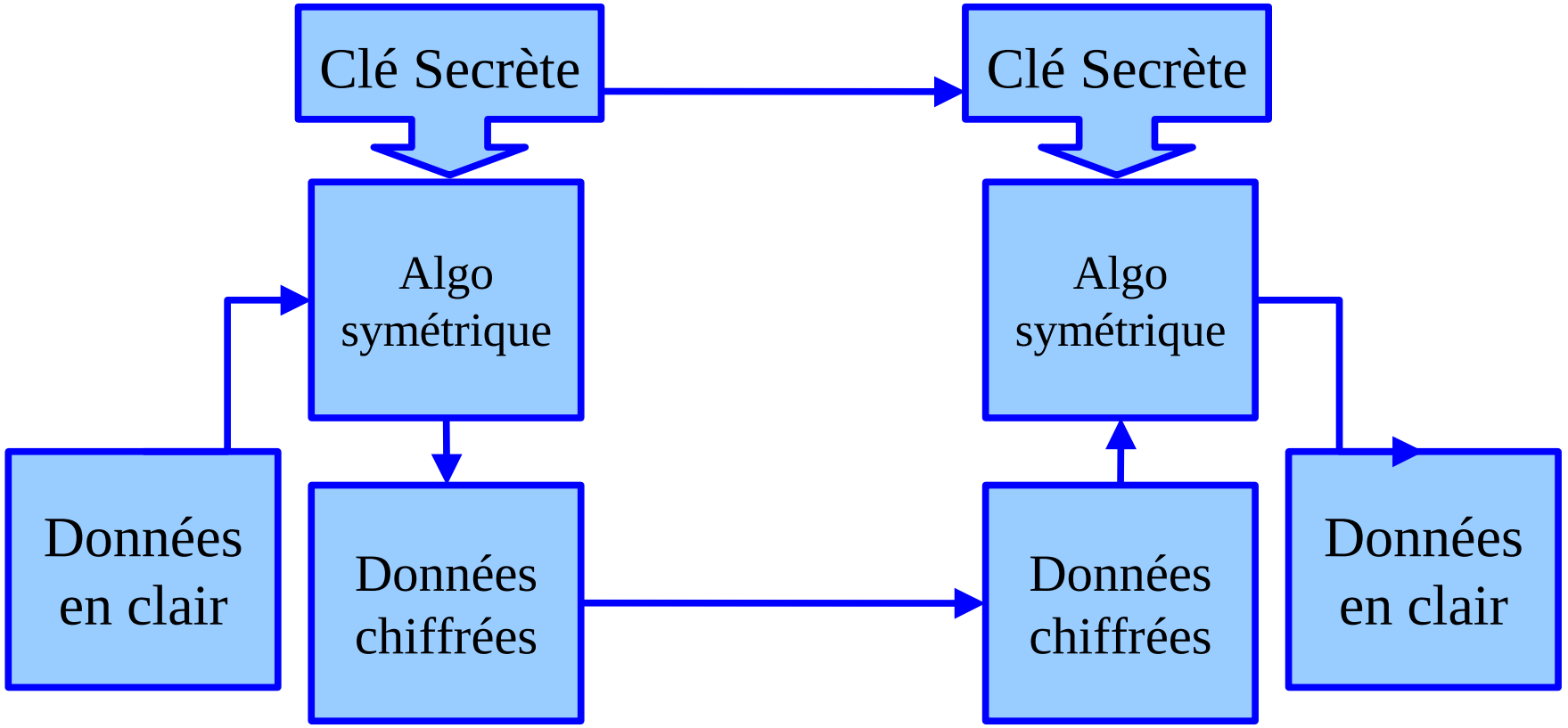
Mathématiques pour la cryptographie

- Euclide
  - PGCD
  - Algorithme d'Euclide étendu
- Arithmétique modulaire
  - Congruence et modulo
  - Classes d'équivalence
- Bezout
- Fermat
  - Restes chinois
- Exponentation rapide modulaire
- …

Cryptographie symétrique

Matthieu Basseur

Cryptographie symétrique



→ Tout les systèmes vus jusque maintenant!

Cryptographie symétrique

- Concept fondamental en cryptographie symétrique : la clé
- Principe de Kerckhoffs : l'algorithme doit pouvoir être divulgué.
- De plus, la clef prend suffisamment de valeurs contre une attaque exhaustive.

Masque jetable

- Le masque jetable combine le message en clair avec une clé.
  - La clé doit être une suite de caractères aussi longue que le message à chiffrer.
  - Les caractères composant la clé doivent être choisis de facon totalement aléatoire.
  - Chaque clé, ou "masque", ne doit être utilisée qu'une seule fois (d'ou le nom de masque jetable).
- Interêt : sécurité théorique absolue (C. Shannon 1949).

Masque jetable (rappel)

- Alice et Bob veulent s'échanger des données à l'aide de la méthode du masque jetable (Vernam) appelée aussi *One Time Pad*.
- One Time Pad : Xor entre une suite de bits aléatoires et le texte à chiffrer : $chiffre_t := clair_t \oplus alea_t$
- Pb : Alice et Bob doivent posséder la même suite de bits aléatoires pour pouvoir décoder : $clair_t := chiffre_t \oplus alea_t$

Opération « ou exclusif » : ⊕

⊕	0	1
0	0	1
1	1	0

Masque jetable

- Comment générer l'aléa?

  → Système de chiffrement à flot

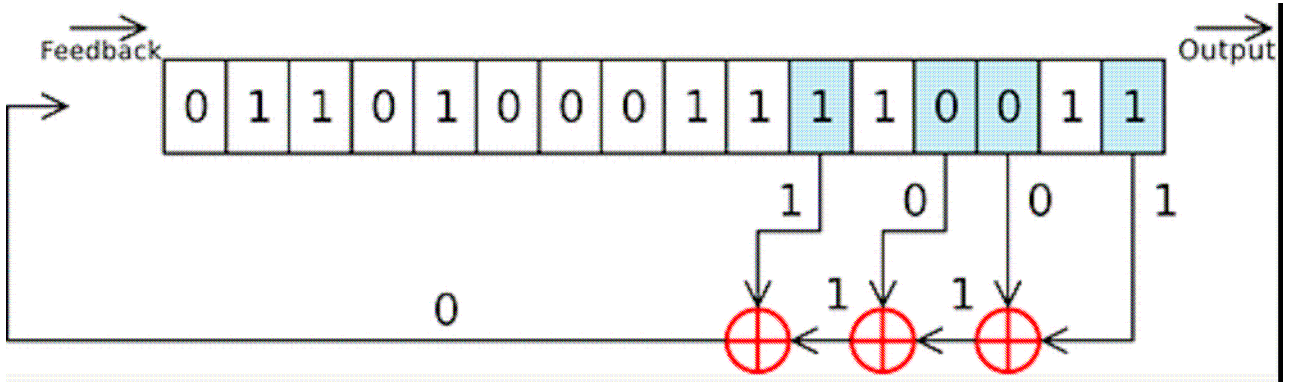
- Chiffrement à flot : générateurs aléatoires

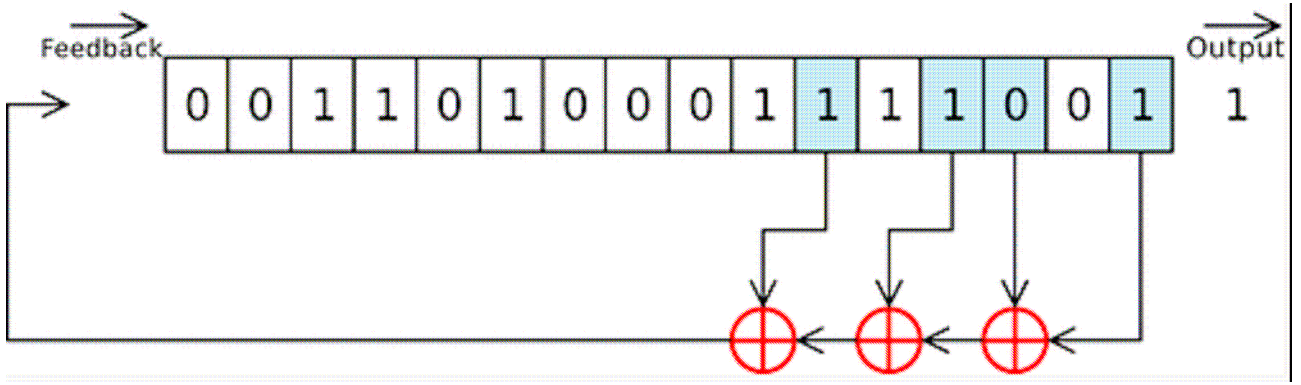
  → Un candidat naturel (rapide) : registre à décalage.
  (LFSR: *Linear Feedback Shift Register*)

Registre à décalage

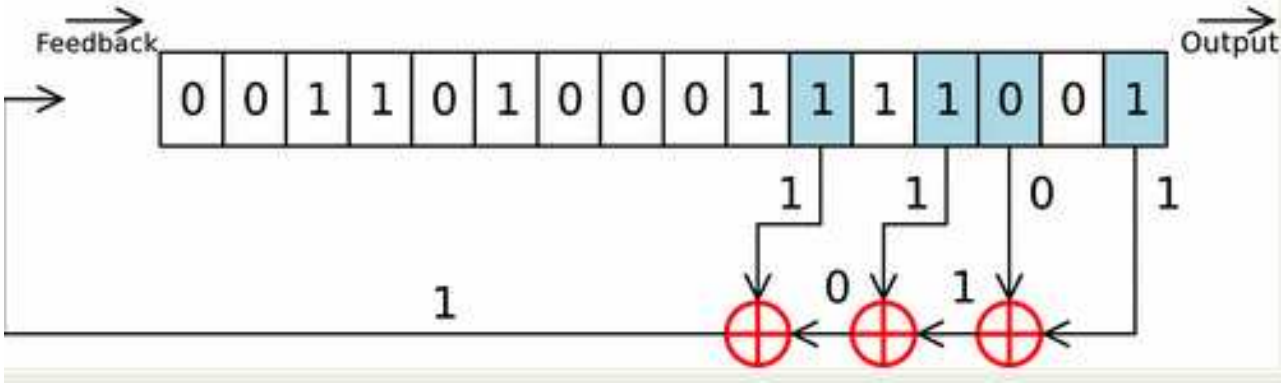
- LFSR de longueur L : L bits $s_{i+L-1}, \ldots, s_i$, et d'une fonction de rétroaction linéaire.
- A chaque top d'horloge, le bit de poids faible s_i constitue la sortie du registre et les autres bits sont décalés vers la droite.
- Le nouveau bit s_{i+L} placé dans la cellule de poids fort du registre est donné par une fonction linéaire des bits $s_i, \ldots, s_{i+L-1}$:
  - $s_{i+L} = c_1 s_{i+L-1} + c_2 s_{i+L-2} + \ldots + c_L s_i$
- où les coefficients de rétroaction $(c_i)_{1 \le i \le L}$ sont des éléments de F_2:

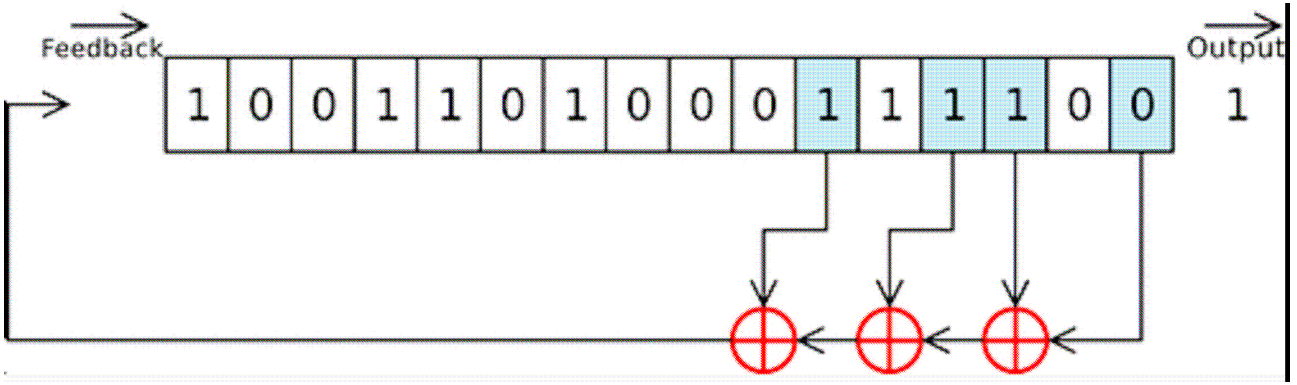
Registre à décalage : exemple





Registre à décalage : exemple





Registre à décalage

- En 1969, J. Massey a montré que l'algorithme proposé par Berlekamp pour le décodage des codes BCH *(Bose, Ray-Chaudhuri, Hocquenghem – algorithme pour Code correcteur)* pouvait être adapté pour retrouver le polynôme de rétroaction d'un LFSR à partir uniquement de 2L bits consécutifs de la suite produite s.
- Problème : facilement cassable via Berlekamp Massey
- Comment améliorer les registres à décalage ?
  - Idée : utiliser un système basé sur des LFSRs mais plus complexe
    → Registres combinés, registres filtrés, registres avec mémoire

Registre à décalage : exemples d'utilisation

- A5/1
  - Système de chiffrement à flot *synchrone* utilisé par le GSM dans la plupart des pays européens.
  - Suite chiffrante produite par 3 LFSRs de longueur 19, 22 et 23 bits et de polynômes de rétroaction :
  - LFSR initialisés à partir d'une clé secrète de 64 bits et d'une chaîne de 22 bits.
- RC4
  - Système de chiffrement à flot dû a Ron Rivest, couramment utilisé dans les protocole SSL et WiFi.
  - RC4 peut utiliser des clés de taille variables jusqu'a 2048 bits (!).
  - La description de RC4 n'est officiellement pas publique

Registre à décalage : exemples d'utilisation

- Chiffrement synchrone vs Chiffrement asynchrone

  - Synchrone : Le chiffrement est dit synchrone si les symboles produits par le GPA (Générateur Pseudo Aléatoire) ne dépendent que de son état interne et non du message à chiffrer.

  - Asynchrone : Le chiffrement est dit asynchrone ou auto-synchronisant si les symboles produits par le GPA ne dépendent que de son état interne et d'un nombre fixé t de symboles du message à chiffrer.