

Chapitre 1: Introduction.

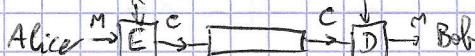
confidentialité: assurer que l'information ne soit accessible qu'à ceux dont l'accès est autorisé.

authenticité: assurer de la légitimité de l'information envoyée

intégrité: assurer l'absence d'alteration de l'information envoyée.

symétrique:

confidentialité: $C = \text{Enc}_K(M)$ $M = \text{Dec}_K(C)$

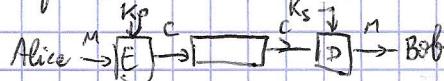


intégrité/authenticité: authenticité impossible en symétrique

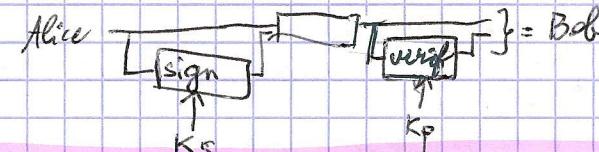


asymétrique:

confidentialité: $C = \text{Enc}_{K_p}(M)$ $D = \text{Dec}_{K_s}(C)$



intégrité/authenticité:



Chapitre 2: Chiffrement symétrique

- one time pad (chiffrement de Vernam): chiffrement parfait car $|K| = |M|$ et que si l'attaquant connaît C et que tous messages M ont la même probabilité alors il n'apprend rien sur K . inconditionnellement sûr et parfait. \rightarrow chiffrement à flot
- Théorème Shannon: chiffrement ne peut être parfait si $|K| > |M|$

Propriétés algorithmes de chiffrement:

$\hookrightarrow C = \text{Enc}_K(M)$ et $M = \text{Dec}_K(C)$ raisonnables à calculer

\hookrightarrow Pour tout K , Enc_K bijective:

- injective $\text{Enc}_K(M) = \text{Enc}_K(M') \Rightarrow M = M'$
- surjective $\forall C \quad C = \text{Enc}_K(M)$

\hookrightarrow exigence max sécurité: avec $\forall M$ et $\forall C$ \rightarrow calculatoirement difficile de déchiffrer un chiffré.

• 2018 $\rightarrow 2^{65}$ opérations faisibles avec 2^{80} infaisable (civil) et 2^{128} infaisable (militaire)
Loi de Moore: la puissance de calcul double tous les 18 mois.

Attaques:

\hookrightarrow attaques à clair connu: charlie connaît un ou plusieurs couples (M, C) où $C = \text{Enc}_K(M)$

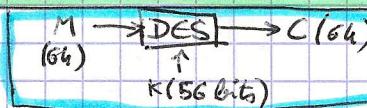
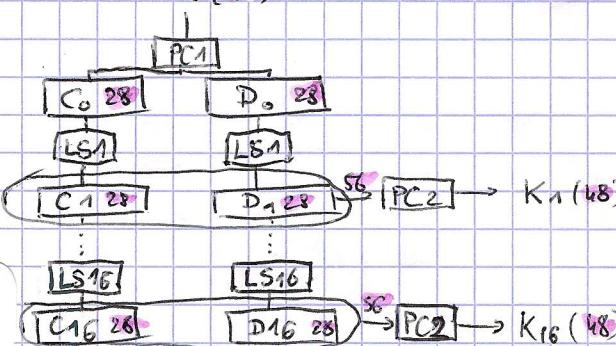
\hookrightarrow attaques à clair choisi: charlie peut choisir un ou plusieurs messages clairs M_1, M_2, \dots et obtenir le chiffré

\hookrightarrow attaques à chiffre choisi: charlie peut choisir un ou plusieurs chiffrés C_1, C_2, \dots et obtenir le clair -

DES: créé par IBM, modifié par NSA

\hookrightarrow dérivation des clés:

$K(56)$



\hookrightarrow Fonction F:

$$F(K_{i+1}, R_i) = P(S(E(R_i) \oplus K_{i+1}))$$

$R_i(32\text{ bits})$

$$E(R_i)(48\text{ bits}) \oplus K_{i+1}(48\text{ bits})$$

tour du DES
S1 S2 S3
6 bits 6 bits 6 bits

6 bits 6 bits 6 bits

6 bits 6 bits 6 bits

permutation (32 bits)

Chiffrement:

$$L_i = L_i$$

$$R_{i+1} = L_i \oplus F(K_{i+1}, R_i) \text{ pour } 0 \leq i \leq 15$$

$$L_{16} = L_{15} \oplus F(K_{16}, R_{15})$$

$$R_{16} = R_{15}$$

Déchiffrement:

$$R_{15} = R_{16}$$

$$L_{15} = L_{16} \oplus F(K_{16}, R_{15})$$

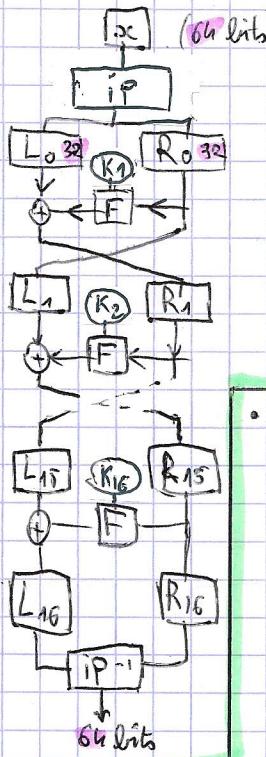
$$R_i = L_{i+1}$$

$$L_i = R_{i+1} \oplus F(K_{i+1}, L_{i+1}) \text{ pour } 0 \leq i \leq 14$$

$$\text{DES}_K^{-1}(x) = \text{DES}_K(x)$$

$K_{16}, K_{15}, K_{14}, \dots, K_1$

→ schéma général DES



DES:

→ attaque exhaustive: $O(2^{56})$

Double DES: $y = DES_K_1(DES_K_2(x)) \Leftrightarrow DES_{K_2}^{-1}(y) = DES_{K_1}(x)$
 → attaque exhaustive lente: $O(2^{56} \times 2^{56}) = O(2^{112})$
 → attaque exhaustive rapide: attaque milieu $O(2^{56} \times 2)$

Triple DES

→ attaque exhaustive lente: $O(2^{112})$

→ attaque exhaustive attaque milieu: $O(2^{112})$

AES (Advanced Encryption Standard)

→ appel candidature NIST (NBS), créé par Rijndael (2001)

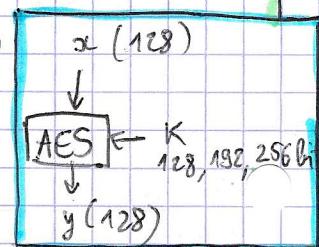
→ Addition $x \oplus y$

→ Multiplication $x \times y \bmod (X^8 + X^4 + X^3 + X + 1)$

→ $E = \{\text{octets}\}$

$(E, +, \times)$ corps commutatif $\rightarrow (E, +)$ groupe commutatif

$(E \setminus \{0\}, \times)$ groupe commutatif



$$x = (x_1, \dots, x_{16})$$

x_1	x_5	x_9	x_{13}
x_2	x_6	x_{10}	x_{14}
x_3	x_7	x_{11}	x_{15}
x_4	x_8	x_{12}	x_{16}

$S (4 \times 4)$

AES f

$S = \text{message plain } x$

$S = S \oplus K_0$

Pour (i de 1 à 10) {

$S = \text{ByteSub}(S)$

$S = \text{ShiftRows}(S)$

$S_i (i \neq 10) S = \text{MixColumn}(S)$

$S = S \oplus K_i$

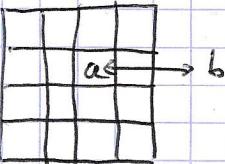
$K \rightarrow K_0 (\text{init})$

$K \rightarrow K_1$

\vdots

$K \rightarrow K_{10}$

1) ByteSub(S)



$$c = \text{inv}(a) = \begin{cases} 1 & \text{si } a \neq 0 \\ a & \text{dans le corps } \mathbb{F}_{2^{8}} \\ 0 & \text{si } a = 0 \end{cases}$$

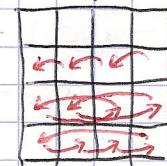
$$\begin{pmatrix} b \\ 1 \times 8 \end{pmatrix} = \begin{pmatrix} 8 \times 8 \\ \text{constante} \end{pmatrix} \begin{pmatrix} c \\ 1 \times 8 \end{pmatrix} + \begin{pmatrix} a \\ \text{constante} \\ 1 \times 8 \end{pmatrix}$$

$$(b) = (M)(c) + (u)$$

$$b(c) = M^{-1}((b) - (u))$$

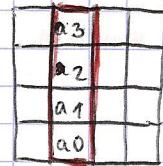
→ bijective

2) ShiftRows(S)



bijective

3) MixColumn(S)

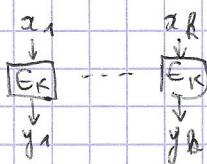


$$\begin{pmatrix} 4 \times 4 \\ \text{constante} \end{pmatrix} \begin{pmatrix} a_3 \\ a_2 \\ a_1 \\ a_0 \end{pmatrix} = \begin{pmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{pmatrix} \rightarrow \begin{pmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{pmatrix}$$

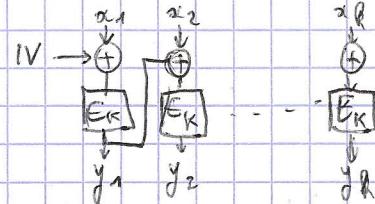
bijective avec pivot de gauß

• Modes opératoires

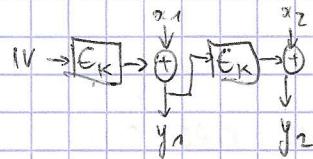
→ ECB



→ CBC



→ CFB

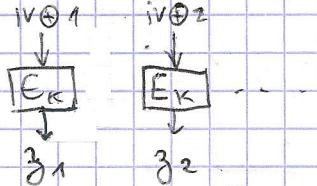


→ OFB



$$y_k = z_k \oplus x_k$$

→ CTR



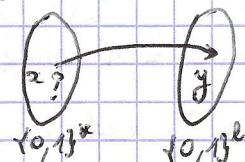
$$y_k = z_k \oplus x_k$$

Chapitre 3 : Intégrité des messages.

- $f : \{0,1\}^* \rightarrow \{0,1\}^l$ (avec l fixé) et une fonction de hachage si elle vérifie 3 propriétés :

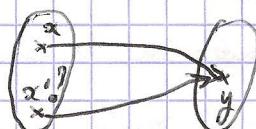
1) f est à sens unique : étant donné $y \in \{0,1\}^l$ il est calculatoirement difficile d'obtenir $x \in \{0,1\}^*$ tq $f(x) = y$

$$P = \frac{1}{2^l}$$
 d'avoir une collision



2) f est à collisions faibles difficiles : étant donné $x \in \{0,1\}^*$ on a $y \in \{0,1\}^l$ tq $f(x) = y$. Il est calculatoirement difficile d'obtenir $x' \in \{0,1\}^*$ à partir de y tq $x \neq x'$ et $f(x') = y$.

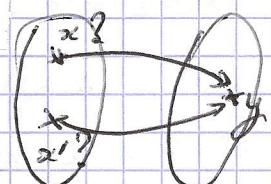
$$P = \frac{1}{2^l}$$
 d'avoir une collision



3) f est à collisions fortes difficiles : il est calculatoirement difficile de trouver x et x' tq $x \in \{0,1\}^*$, $x' \in \{0,1\}^*$, $x \neq x'$ et $f(x) = f(x')$

P probabilité d'avoir une collision

On va chercher proba de ne pas avoir de collisions $1 - P$



$$\begin{aligned} 1^{\text{er}} \text{ tirage: } p_1 &= \frac{1}{2^l} \\ 2^{\text{e}} \text{ ---: } p_2 &= \frac{(2^l - 1)/2^l}{2^l} = 1 - (1/2^l) \\ 3^{\text{e}} \text{ ---: } p_3 &= \frac{(2^l - 2)/2^l}{2^l} = 1 - (2/2^l) \\ \vdots & \\ n^{\text{e}} \text{ ---: } p_n &= \frac{(2^l - (n-1))/2^l}{2^l} = 1 - ((n-1)/2^l) \end{aligned} \quad \left. \right\} x$$

$$1 - P = 1 \times \left(1 - \frac{1}{2^l}\right) \times \left(1 - \frac{2}{2^l}\right) \times \dots \times \left(1 - \frac{n-1}{2^l}\right)$$

$$\ln(1 - P) = \ln\left(1 - \frac{1}{2^l}\right) + \ln\left(1 - \frac{2}{2^l}\right) + \dots + \ln\left(1 - \frac{n-1}{2^l}\right) \text{ or } \ln(1 - u) \approx -u$$

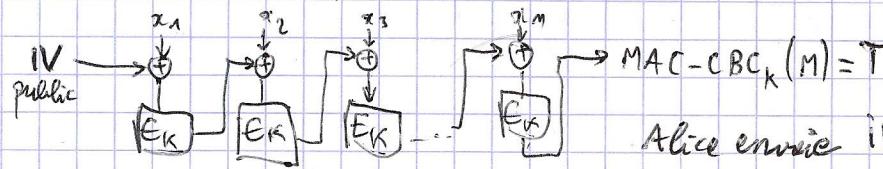
$$\ln(1 - P) = -\frac{1}{2^l} - \frac{2}{2^l} - \frac{n-1}{2^l} = -\frac{1}{2^l} (1 + 2 + \dots + (n-1)) = -\frac{1}{2^l} \times \frac{(n-1)n}{2}$$

$$1 - P = \exp\left(-\frac{n(n-1)}{2 \times 2^l}\right) \Leftrightarrow P = 1 - \exp\left(-\frac{n(n-1)}{2 \times 2^l}\right) \text{ d'avoir une collision}$$

- Le paradoxe des anniversaires résulte de l'estimation probabiliste du nombre de personnes que l'on doit réunir pour avoir au moins $\frac{1}{2}$ que il y ait une collision.

- MAC (Message Authentication Code)

Manuel MAC : MAC-CBC



Alice envoie $IV, T, x_1, x_2, x_3, \dots, x_m$
si Charlie envoie $IV', T, x'_1, x_2, \dots, x_m$ avec $IV \oplus x_1 = IV' \oplus x'_1$

Solution : rendre IV public ET CONSTANT.

Chapitre 4 : RSA → problème de factorisation : à partir de $p \times q$, retrouver p et q

$$K_{\text{pub}} = (n, e) \quad K_{\text{priv}} = (p, q, d, \phi(n))$$

1) choisir 2 nombres premiers p et q

2) calculer $n = p \times q$

3) calculer $\phi(n) = \phi(p) \times \phi(q) = (p-1)(q-1)$ ($\phi(n)$ pair car p et q impairs)

4) calculer $e \in \{2, \dots, \phi(n)-1\}$ et $\text{PGCD}(e, \phi(n)) = 1 \quad | e = 3, e = 17, e = 257$

5) calculer d tq $d \cdot e = 1 \pmod{\phi(n)}$

Ciffrement : $y = x^e \pmod{n}$

Déchiffrement : $x = y^d \pmod{n}$.

Théorème de Bézout : $\forall a, b \in \mathbb{N}, \text{tg} \text{PGCD}(a, b) = 1 \quad \exists u, v \in \mathbb{Z} \quad au + bv = 1$

Théorème de Fermat : Soit p premier et a entier $a \neq 0 \quad a^{p-1} \equiv 1 \pmod{p}$.

↳ Démonstration RSA : Montrons que $(x^e)^d \pmod{n} \equiv x \pmod{n}$ avec $n = p \times q$

• Montrons que $(x^e)^d \pmod{p} \equiv x \pmod{p}$
 $(x^e)^d = x^{ed} = x \wedge (1 + \lambda \phi(n)) = x \times x^{\lambda \phi(n)} = x \times x^{\lambda(p-1)(q-1)}$

$(x^e)^d = x \times (x^{p-1})^{\lambda(q-1)} \pmod{p}$ or $x^{p-1} \equiv 1 \pmod{p}$ si p premier

$(x^e)^d = x \times 1^{\lambda(q-1)} = x \pmod{p}$.

• Montrons que $(x^e)^d \pmod{q} \equiv x \pmod{q}$

$(x^e)^d = x^{ed} \stackrel{ed=1 \pmod{\phi(n)}}{=} x \wedge (1 + \lambda \phi(n)) = x \times x^{\lambda \phi(n)} = x \times x^{\lambda(p-1)(q-1)}$

$(x^e)^d = x \times (x^{q-1})^{\lambda(p-1)} \pmod{q}$ or $x^{q-1} \equiv 1 \pmod{q}$ si q premier

$(x^e)^d = x \times 1^{\lambda(p-1)} = x \pmod{q}$

• On en déduit $\begin{cases} (x^e)^d \equiv x \pmod{p} \\ (x^e)^d \equiv x \pmod{q} \end{cases}$ donc $(x^e)^d \equiv x \pmod{n}$

↳ sécurité RSA.

- méthode pour Charlie déchiffre $x = y^d \pmod{m}$
- factoriser n pour trouver p et q et $\phi(m) = (p-1)(q-1)$
- e est connu et vaut $e \in \{2, \dots, \phi(m)-1\}$ t.q. $\text{PGCD}(e, \phi(m)) = 1$.
- calculer d tq $d = e^{-1} \pmod{\phi(m)}$

(Factorisation meilleur algo : $O(\exp(x (\ln m)^{1/3} (\ln \ln m)^{2/3}))$)
 ↳ m doit faire au moins 1024 bits.

↳ Square and multiply : calculer $x = y^d \pmod{m}$ avec $d = d_{k-1} \cdot 2^{k-1} + \dots + d_1 \cdot 2^1 + d_0 \cdot 2^0$

$x = 1$
 Pour i de $(k-1)$ à 0
 $x = x \times x \pmod{m}$
 ↳ si $(d_i = 1)$ $x = x \times y \pmod{m}$

↳ Problèmes RSA confidentialité

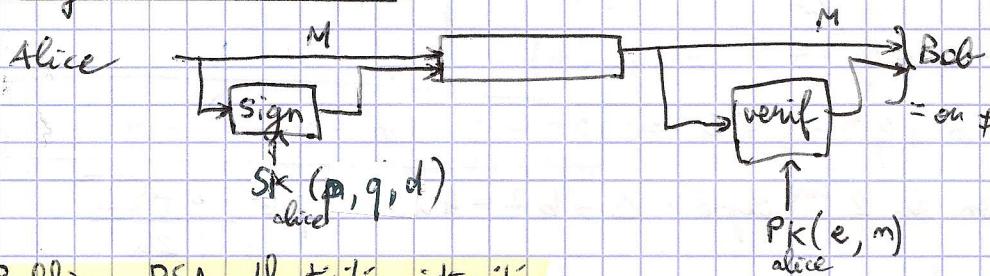
① si $|M| < \sqrt[2]{m}$ alors $C = M^e \pmod{m}$
 $C = M$

② ne pas envoyer le même message à plusieurs destinataires → utilisation du théorème des restes chinois.

↳ Solution RSA confidentialité

→ utiliser PKCS (Public Key cryptographic Standard)
 où $C = (\mu(M))^e \pmod{m}$ avec $\mu(M) = \phi\phi\phi_2 \parallel \dots \parallel \phi\phi\phi_1 M$

↳ Intégrité et authenticité.



$$\begin{aligned} S &= M^d \pmod{m} \\ M &= S^e \pmod{n} \end{aligned}$$

↳ Problèmes RSA authenticité, intégrité

① si $|M| > n$ alors M et $M+n$ auront la même signature

② Si Alice envoie 2 messages signés à Bob
 (M_1, s_1) avec $s_1 = M_1^d \pmod{m}$
 (M_2, s_1) avec $s_2 = M_2^d \pmod{m}$

Donc si Charlie construit $(M_1 \times M_2) \pmod{m} \rightarrow M_3$ alors $s_3 = s_1 \times s_2 \pmod{m}$

1024 bits

↳ Solution RSA authenticité, intégrité

→ utiliser PKCS où $S = (\mu(M))^d \pmod{m}$ avec $\mu(M) = \phi\phi\phi_1 FF\dots FF\phi\phi_2 \parallel c_H \parallel h(M)$

id de la fonction de hachage

Théorème des restes chinois:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases} \text{ avec } \text{PGCD}(m_i, m_j) = 1$$

Pour chaque i , m_i et $\hat{m}_i = \frac{M}{m_i}$ premiers entre eux $\Rightarrow \text{PGCD}(m_i, \hat{m}_i) = 1$

Donc d'après le théorème d'Euclide $\exists u_i$ et v_i tq $M; m_i + u_i; \hat{m}_i = 1$

$$\text{On pose } e_i = u_i; \hat{m}_i \text{ et on a donc } \begin{cases} e_i \equiv 1 \pmod{m_i} \\ e_i \equiv 0 \pmod{m_j} \end{cases}$$

On a donc $x = a_1 e_1 + \dots + a_n e_n \pmod{M}$

$$\text{car } x \equiv a_i e_i \equiv a_i (1 + u_i m_i) \equiv a_i \cdot 1 \equiv a_i \pmod{m_i}$$

Résumer p et q à partir de m et $\phi(m)$:

$$m = p \times q \Rightarrow p = m/q$$

$$\phi(m) = (p-1)(q-1) = pq - p - q + 1 = m - p - q + 1 = m - \frac{m}{q} - q + 1$$

$$\phi(m) = m - \frac{m}{q} - q + 1 \Leftrightarrow q \phi(m) = q \left(m - \frac{m}{q} - q + 1 \right)$$

$$\Leftrightarrow q \phi(m) = qm - m - q^2 + q$$

$$\Leftrightarrow q \phi(m) - qm + m + q^2 - q = 0 \Leftrightarrow \boxed{q^2 + q(\phi(m) - m - 1) + m = 0}$$

$$\text{Résolution d'équation du 2^{eme} degré: } \Delta = b^2 - 4ac \quad p = \frac{-b + \sqrt{\Delta}}{2a}$$

$$q = \frac{-b - \sqrt{\Delta}}{2a}$$

Théorème de Bézout: Si $\text{PGCD}(a, b) = 1$ alors $\exists u, v \in \mathbb{Z}$ tq $au + bv = 1$

Algorithme Euclide: $\text{PGCD}(a, b) = \text{PGCD}(a+bc, b)$

Théorème de Fermat: si p premier alors $a^{p-1} \equiv 1 \pmod{p}$.

Théorème d'Euler: si $\text{PGCD}(a, m) = 1$, $a^{\phi(m)} \equiv 1 \pmod{m}$

Calcul Euler $\phi(m)$: $\phi(156)$ si m non premier

$$\begin{array}{r|l} 156 & 2 \\ 78 & 2 \\ 39 & 3 \\ 13 & 13 \\ 1 & \end{array} \quad 156 = 2^2 \times 3^1 \times 13^1 \\ \phi(156) = (2^2 - 2^1) \times (3^1 - 3^0) \times (13^1 - 13^0) \\ \phi(156) = 48$$

$$\begin{aligned} \text{si } m \text{ premier et } m = p \times q \\ \phi(m) &= \phi(p) \times \phi(q) \\ &= (p-1)(q-1) \end{aligned}$$

Calcul inverse: utiliser Fermat ou Euler $a^{-1} \equiv [1] \pmod{b}$?
 ex: $4^{-1} \pmod{7} \rightarrow$ Fermat $\rightarrow 4^6 \equiv 1 \pmod{7} \rightarrow 4 \cdot 4^5 \equiv 1 \pmod{7}$
 $4^5 \equiv 2 [7]$ donc $4^{-1} \equiv 2 [7]$