Crypto1 – Examen Réparti 1
2023-2024

Énoncé

2 heures. Notes manuscrites et documents de cours autorisés. Vos copies doivent être lisibles et bien présentées. Un soin particulier doit être apporté à la rédaction et l'argumentation de vos réponses. La barème est donné à titre indicatif.

Dans la suite, $\mathcal{E}$ désigne un algorithme de chiffrement par bloc qui chiffre des blocs de n bits avec une clé secrète de n bits.

Exercice 1 : 3 points

1.a] Décrire le fonctionnement du mode `ECB` (chiffrement et déchiffrement).

1.b] Dani, qui gagne 105000€ par an, a retrouvé l'entrée chiffrée qui lui correspond dans la base de donnée des salaires de son entreprise : Q92DFPVXC9IO.

Sachant que la base de données est chiffrée avec le mode `ECB` et un chiffrement qui opère sur des blocs de deux caractères, retrouver le salaire de Dana – une autre employée – parmi le reste de la base de données : TOAV6RFPY5VXC9, YPFGFPDFDFIO, Q9AXFPC9IOIO, ACED4TFPVXIOIO, UTJSDGFPRTAVIO.

Exercice 2 : 3 points

Pour chiffrer des blocs clairs $m_1, \dots, m_s \in \{0,1\}^n$, le mode opératoire `CTROFB` procède de la manière suivante. L'émetteur génère une suite chiffrante $z_0, \dots, z_s \in \mathbb{F}_2^n$ comme :

$$z_0 = \mathrm{IV}, \text{ et } z_i = \mathcal{E}_k(z_{i-1} \oplus i), \forall i, 1 \leq i \leq s,$$

avec $k \in \mathbb{F}_2^n$ la clé secrète et $\mathrm{IV} \in \mathbb{F}_2^n$ un vecteur d'initialisation. On chiffre ensuite par $c_0 = \mathrm{IV}$ et $c_i = m_i \oplus z_i$, $\forall i, 1 \leq i \leq s$.

2.a] Expliquer comment déchiffrer dans un tel mode.

2.b] Supposons que l'émetteur utilise toujours le même vecteur d'initialisation IV. Sachant également que l'attaquant connait un couple $\big((m_1, \dots, m_s), (c_0, c_1, \dots, c_s)\big)$ de blocs clairs/chiffrés dans le mode `CTROFB`, expliquer comment retrouver les blocs clairs à partir d'autres blocs chiffrés $c'_1, \dots, c'_s$.

Exercice 3 : `AONT` et modes opératoires (7 points)

Un mode opératoire d'un chiffrement par bloc $\mathcal{E}$ transforme des blocs de messages clairs $m_1, \dots, m_s \in \mathbb{F}_2^n$ en des blocs chiffrés $c_1, \dots, c_t \in \mathbb{F}_2^n$. Nous dirons que le mode mode opératoire est *séparable* si le déchiffrement d'un bloc chiffré (i.e. $\mathcal{E}_k^{-1}(c_i)$, pour $i, 1 \leq i \leq t$) par un attaquant permet de retrouver un bloc du message clair.

3.a] Le mode `ECB` est-il séparable. Même question pour le mode `CBC`.

Un `AONT` (All-or-Nothing-Transform) est une fonction $F : (\mathbb{F}_2^n)^s \mapsto (\mathbb{F}_2^n)^{s'}$, avec $s' \geq s$, qui transforme des blocs clairs $m_1, \dots, m_s \in \mathbb{F}_2^n$ en de nouveaux blocs $m'_1, \dots, m'_{s'} \in \mathbb{F}_2^n$ tels que :

- F est inversible, i.e. la connaissance des blocs $m'_1, \dots, m'_{s'} \in \mathbb{F}_2^n$ permet de retrouver les blocs $m_1, \dots, m_s \in \mathbb{F}_2^n$, et
- la fonction F est calculatoirement impossible à inverser si l'un des blocs $m'_i \in \mathbb{F}_2^n$ n'est pas connu.

Soient $k_0 \in \mathbb{F}_2^n$ un paramètre public et $F_P : (\mathbb{F}_2^n)^s \mapsto (\mathbb{F}_2^n)^{s+1}$ la transformation suivante :

— Tirer aléatoirement $k_1 \in \mathbb{F}_2^n$ et calculer pour tout $i, 1 \leq i \leq s, m'_i = m_i \oplus \mathcal{E}_{k_1}(i)$,

— $m'_{s+1} = k_1 \oplus \mathcal{E}_{k_0}(m'_1 \oplus 1) \oplus \cdots \oplus \mathcal{E}_{k_0}(m'_s \oplus s)$.

3.b] Montrer que F_P est inversible, i.e. étant donnés $k_0, m'_1, \ldots, m'_{s+1}$, expliquer comment retrouver $m_1, \ldots, m_s$. Que se passe t'il lorsqu'un des blocs m'_i est manquant ? Dans la suite, nous supposerons que F_P est un `AONT`.

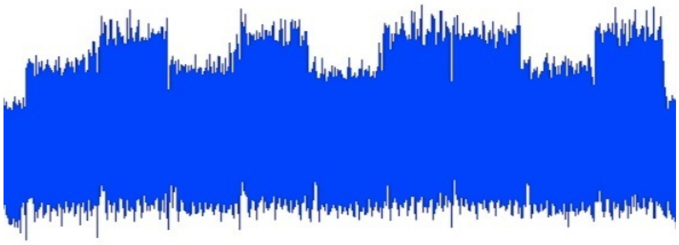
Le mode `CBC-AONT` consiste à 1) transformer des blocs clairs $m_1, \ldots, m_s \in \mathbb{F}_2^n$ en des nouveaux blocs $m'_1, \ldots, m'_{s'} \in \mathbb{F}_2^n$ avec un `AONT` et 2) chiffre ces blocs avec le mode `CBC`.

3.c] Expliquer comment fonctionne le déchiffrement du `CBC-AONT` avec un `AONT` général. Même question avec F_P.

3.d] Un mode opératoire est *fortement inséparable* lorsqu'il est calculatoirement impossible retrouver un bloc de message clair sans avoir déchiffré l'ensemble des blocs chiffrés. Montrer que le mode `CBC-AONT` est fortement inséparable.

Exercice 4 : Protection de RSA (6 points)

De nombreuses attaques se font par écoute des canaux cachés (consommation, rayonnements,...). Par exemple, on donne ci-dessous un fragment de la consommation d'une carte à puce non protégée effectuant une exponentiation :



L'algorithme d'exponentiation utilisé est le suivant. Soit $e = \sum_{i=0}^{n-1} e_i 2^i$, avec $e_{n-1} = 1$:

Algo1(X,e)

$T \leftarrow X$, $U \leftarrow X \cdot X$,

Pour $i = n-2$ à 0 faire

$T \leftarrow T \cdot T$ **(opération notée C)**

Si $e_i = 1$ alors $T \leftarrow T \cdot X$ **(opération notée M)**

Retourner T

4.a] Pour un fragment de clé valant 101101 donner la suite des opérations M et C effectuées.

4.b] On suppose qu'une opération C consomme plus qu'une qu'une opération M. Dans le fragment de consommation donné ci-dessus, comment repère-t-on les opérations M et C ?

4.c] Donner le fragment de clé que l'on peut déduire de ce fragment de consommation.

Pour éviter ceci, il est souhaitable d'avoir des algorithmes qui effectuent les mêmes opérations arithmétiques à chaque itération. Pour calculer X^e ($e = \sum_{i=0}^{n-1} e_i 2^i$, avec $e_{n-1} = 1$), nous faisons :

Algo2(X,e)

$T \leftarrow X$, $U \leftarrow X \cdot X$,

Pour $i = n-2$ à 0 faire

Si $e_i = 0$ alors $U \leftarrow T \cdot U$, $T \leftarrow T \cdot T$

Si $e_i = 1$ alors $T \leftarrow T \cdot U$, $U \leftarrow U \cdot U$

Retourner T

4.d] Donner le déroulement de cet algorithme pour le calcul de 10^{23} (le contenu des variables T et U)

4.e] Donner la trace d'exécution en terme de carrés C et de multiplication M.

4.f] Expliquer en quoi l'algorithme Algo2 est plus sûr que Algo1.