ÉCOLE D'INGENIEURS EN INFORMATIQUE

Chiffrement et Codes Correcteurs : Évaluation Sommative 1

Nasko Karamanov, Ludovic Perret, Loïc Rouquette

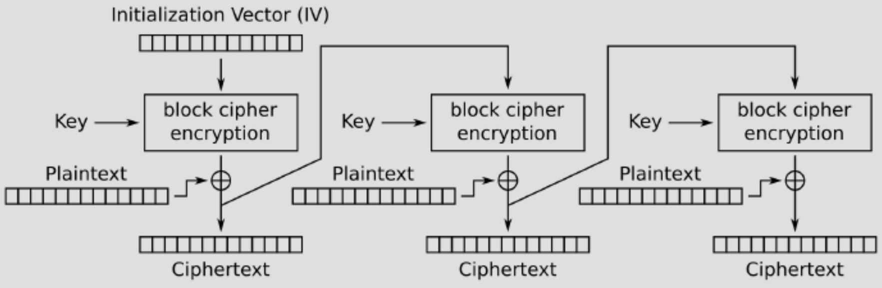
Exercices

Question 0-1 Cet exercice est à rédiger sur la feuille donnée, dans la zone Exercice 1.
Le mode opératoire CFB (cipher feedback) est décrit sur le schéma suivant :
cfb
Soit $c_0 = IV$ le vecteur d'initialisation et K la clé de chiffrement et $m_1, m_2, ...m_n$ les blocs de messages. Ainsi d'après le schéma
$c_i = m_i \oplus Enc_K(c_{i-1})$
Questions

a) Donner la formule que permet de récupérer les blocks m_i à partir des blocs chiffrés c_i et la clé K.

b) Une erreur s'est produit dans la transmission de c_2 et c_4 . Quels sont les blocs de messages impactés lors du déchiffrement ? Justifier.

c) Le chiffrement de Even-Mansour est défini ainsi : on choisit une permutation de bits $P : \{0,1\}^n \to \{0,1\}^n$ et deux clés k_1 et k_2 de longueur n. Alors un bloc de message de longueur n bits est chiffré par $Enc_{k_1,k_2}(x) = P(x \oplus k_1) \oplus k_2$.
On décide de combiner le mode opératoire CFB avec le chiffrement Even-Mansour en choisissant deux clés et en remplaçant $Enc_K(c_{i-1})$ par $Enc_{k_1,k_2}(c_{i-1})$
On choisit la permutation P qui décale les bits à gauche : $P(a_3a_2a_1a_0) = a_2a_1a_0a_3$. Par exemple $P(0110) = 1100$,
Déterminer c_1 si $k_1 = 1010$ $k_2 = 0110$, $IV = 1101$ et $m_1 = 0100$.



Cipher Feedback (CFB) mode encryption

==

This exercise is to be completed on the provided sheet, in the "Exercise 1" area.
The CFB (Cipher Feedback) mode of operation is described by the following diagram :
Let $c_0 = IV$ be the initialization vector, K the encryption key, and $m_1, m_2, ..., m_n$ the message blocks. According to the diagram (see above) :
$c_i = m_i \oplus Enc_K(c_{i-1})$

Questions :

a) Provide the formula to recover the message blocks m_i from the encrypted blocks c_i and the key K.

b) An error occurred during the transmission of c_2 and c_4. Which message blocks will be affected during decryption ? Justify your answer.

c) The Even-Mansour encryption is defined as follows : A bit permutation $P : \{0,1\}^n \to \{0,1\}^n$ and two keys k_1 and k_2 of length n are chosen. Then, a message block of length n bits is encrypted by $Enc_{k_1,k_2}(x) = P(x \oplus k_1) \oplus k_2$.
We decide to combine the CFB mode with the Even-Mansour encryption by choosing two keys and replacing $Enc_K(c_{i-1})$ with $Enc_{k_1,k_2}(c_{i-1})$.
We choose the permutation P that shifts the bits to the left : $P(a_3a_2a_1a_0) = a_2a_1a_0a_3$. For example, $P(0110) = 1100$.
Determine c_1 if $k_1 = 1010$, $k_2 = 0110$, $IV = 1101$, and $m_1 = 0100$.

Solution 0-1

a) **Formule de déchiffrement :**
On a la formule de chiffrement :
$$c_i = m_i \oplus Enc_K(c_{i-1})$$
En appliquant un `XOR` des deux côtés avec $Enc_K(c_{i-1})$, on obtient :
$$m_i = c_i \oplus Enc_K(c_{i-1})$$

b) **Propagation des erreurs :**
L'erreur dans c_2 va impacter :
— directement $m_2 = c_2 \oplus Enc_K(c_1)$, donc m_2 sera incorrect.
— et également $m_3 = c_3 \oplus Enc_K(c_2)$, car le chiffrement de c_2 est utilisé. Donc m_3 sera aussi affecté.
— mais m_4 dépend de c_3, et non plus de c_2, donc l'erreur ne se propage pas au-delà.
De même, une erreur dans c_4 affectera :
— $m_4 = c_4 \oplus Enc_K(c_3)$: donc m_4 est incorrect.
— $m_5 = c_5 \oplus Enc_K(c_4)$: donc m_5 est aussi incorrect.
— Les blocs suivants ne sont pas impactés.
Ainsi, chaque erreur dans un bloc c_i corrompt deux blocs de messages : m_i et m_{i+1}.

c) **Chiffrement Even-Mansour combiné avec le mode CFB :**
Données :

$$k_1 = 1010, \quad k_2 = 0110, \quad IV = 1101, \quad m_1 = 0100$$

Étapes du chiffrement :

1. $IV \oplus k_1 = 1101 \oplus 1010 = 0111$
2. $P(0111)$: On applique la permutation de bits à gauche $a_3a_2a_1a_0 \rightarrow a_2a_1a_0a_3$, donc :

$$P(0111) = 1110$$

3. On applique ensuite le `XOR` avec k_2 :

$$Enc_{k_1,k_2}(IV) = P(IV \oplus k_1) \oplus k_2 = 1110 \oplus 0110 = 1000$$

4. Enfin, on calcule $c_1 = m_1 \oplus Enc_{k_1,k_2}(IV) = 0100 \oplus 1000 = 1100$

Résultat : $c_1 = \boxed{1100}$

Question 0-2 Alice et Bob ont crée leur propre cryptosystem Shifted Power comme suit :

Génération de Clés :
Choix des Paramètres :

Choisir p premier, g générateur de $\mathbb{Z}/p\mathbb{Z}^{\times}$
Choisir un entier secret b (la clé privée), où $1 < b < p-1$
Choisir un entier de décalage $1 < s < p-1$

Calcul de la Clé Publique : $K_b = g^b \mod p$.

La clé publique est (p, g, K_b, s).
La clé privée est b.

Chiffrement :

Le message M doit être un entier tel que $1 \leq M \leq p-1$
Choisir un entier aléatoire a
$C_1 = g^a \mod p$
$C_2 = (M+s) \cdot K_b^a \mod p$
Le chiffré est $C = (C_1, C_2)$

Déchiffrement :

$M = (C_1^b)^{-1}C_2 - s \mod p$ La clé publique de Bob est $(17, 3, 15, 2)$.

a) Alice veut chiffrer le message $M = 10$ avec $a = 3$. Quel est le message chiffré C ?
b) Bob a perdu sa clé privé. Pour ceci il a appliqué l'algorithme de Shank et obtient les listes suivantes : $L_1 = 1, 3, 9, 10$ et $L_2 = 15, 9, 2, 8$. Quelle sa clé privée ? Justifier.

Goal: Solution of $g^x = b$

This is a *collision algorithm* : two lists of elements of are created, and we look for an element that appears in both lists (collision).

- **Step 1 :** choose $n > \sqrt{p}$, for example $n = 1 + \lfloor \sqrt{p} \rfloor$
- **Step 2 :** generate lists:
  - First list (baby-steps) : $1, g, g^2, \ldots, g^{n-1}$
  - Second list (giant-steps) : $b, bg^{-n}, bg^{-2n}, \ldots, bg^{(n-1)n}$
- **Step 3 :** find a collision (same element in both lists) $g^r = bg^{-qn}$
- **Step 4 :** then $g^{qn+r} = b$, thus $x = qn + r$

==

Alice and Bob created their own Shifted Power cryptosystem as follows :

Key Generation :

Parameter Selection :

Choose p prime, g generator of $\mathbb{Z}/p\mathbb{Z}^\times$
Choose a secret integer b (the private key), where $1 < b < p-1$
Choose a shift integer $1 < s < p-1$

Public Key Calculation :

$K_b = g^b \mod p$
The public key is $p, g, (K_b), s$.
The private key is b.

Encryption :

The message M must be an integer such that $1 \leq M \leq p-1$
Choose a random integer a
$C_1 = g^a \mod p$
$C_2 = (M+s) \cdot K_b^a \mod p$
The ciphertext is $C = (C_1, C_2)$

Decryption :

$M = (C_1^b)^{-1} C_2 - s \mod p$
Bob's public key is $(17, 3, 15, 2)$.

a) Alice wants to encrypt the message $M = 10$ with $a = 3$. What is the encrypted message C ?

b) Bob lost his private key. For this, he applied Shank's algorithm (see above) and obtained the following lists : $L_1 = 1, 3, 9, 10$ and $L_2 = 15, 9, 2, 8$. What is his private key ? Justify.

Solution 0-2

a) **Chiffrement du message** $M = 10$ **avec** $a = 3$

— Paramètres publics : $p = 17,\ g = 3,\ K_b = 15,\ s = 2$

— On calcule :

$$C_1 = g^a \mod p = 3^3 \mod 17 = 27 \mod 17 = 10$$

$$C_2 = (M+s) \cdot K_b^a \mod p = (10+2) \cdot 15^3 \mod 17$$

D'abord, $15^3 = 3375$. Calculons $3375 \mod 17$:

$$3375 \div 17 \approx 198.53 \Rightarrow 17 \cdot 198 = 3366, \quad 3375 - 3366 = 9 \Rightarrow 15^3 \mod 17 = 9$$

Donc :

$$C_2 = 12 \cdot 9 \mod 17 = 108 \mod 17 = 6 \quad (\text{car } 17 \cdot 6 = 102,\ 108 - 102 = 6)$$

Résultat : $C = \boxed{(10,\ 6)}$

b) **Retrouver la clé privée** b **via l'algorithme de Shank**

On cherche b tel que $g^b \equiv K_b \mod p$, c'est-à-dire :

$$3^b \equiv 15 \mod 17$$

D'après l'algorithme de Shank (Baby-Step Giant-Step), on a deux listes :

— $L_1 = \{1,3,9,10\} = \{g^j \mod p\}$ pour $j = 0,1,2,3$

— $L_2 = \{15,9,2,8\} = \{K_b \cdot g^{-im} \mod p\}$ pour $i = 0,1,2,3$

On cherche une collision entre L_1 et L_2. Ici :

$$9 \in L_1 \cap L_2$$

Dans L_1, $3^2 \equiv 9 \mod 17 \Rightarrow j = 2$

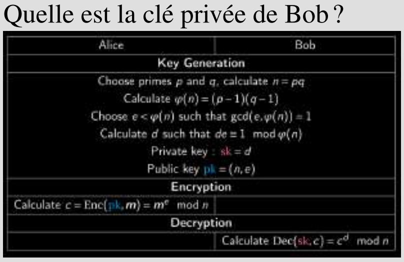
Dans L_2, $i = 1$ car $9 = 15 \cdot g^{-1 \cdot m} \mod 17$

Sachant que le dernier exposant de la premier liste est $n-1$ on a $n = 4$ donc

$$b = i \cdot n + j = 1 \cdot 4 + 2 = \boxed{6}$$

NB : ceux qui ont calculé n avec la formule du algorithme obtiennent $n = 5$ et $b = 7$, la réponse est aussi acceptée.

Question 0-3 Alice et Bob utilisent le cryptosysteme RSA avec la clé publique $(n,e) = (65,11)$.
Quelle est la clé privée de Bob ?



Alice	Bob
Key Generation	
Choose primes p and q, calculate $n = pq$	
Calculate $\varphi(n) = (p-1)(q-1)$	
Choose $e < \varphi(n)$ such that $\gcd(e, \varphi(n)) = 1$	
Calculate d such that $de \equiv 1 \mod \varphi(n)$	
Private key : $sk = d$	
Public key $pk = (n,e)$	
Encryption	
Calculate $c = \mathrm{Enc}(pk, m) = m^e \mod n$	
Decryption	
	Calculate $\mathrm{Dec}(sk, c) = c^d \mod n$

==

Alice and Bob use the RSA cryptosystem with the public key $(n,e) = (65,11)$.
What is Bob's private key ?"

Solution 0-3 Données :

$$(n,e) = (65,11)$$

Étape 1 : Factoriser $n = 65$

On remarque que :

$$65 = 5 \times 13$$

Donc :

$$p = 5, \quad q = 13$$

Étape 2 : Calcul de $\varphi(n)$

$$\varphi(n) = (p-1)(q-1) = (5-1)(13-1) = 4 \times 12 = 48$$

Étape 3 : Calcul de l'inverse de $e = 11 \mod \varphi(n) = 48$
On cherche d tel que :

$$e \cdot d \equiv 1 \mod 48$$

Autrement dit, $11d \equiv 1 \mod 48$
On utilise l'algorithme d'Euclide étendu pour cela :

$$\gcd(48, 11) = 148 = 4 \cdot 11 + 411 = 2 \cdot 4 + 34 = 1 \cdot 3 + 13 = 3 \cdot 1 + 0$$

Remontée :

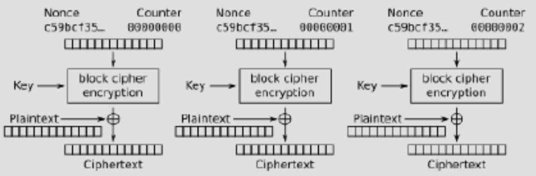
$$1 = 4 - 1 \cdot 3 = 4 - 1(11 - 2 \cdot 4) = 3 \cdot 4 - 1 \cdot 11 = 3(48 - 4 \cdot 11) - 1 \cdot 11 = 3 \cdot 48 - 13 \cdot 11$$

Donc :

$$1 = 3 \cdot 48 - 13 \cdot 11 \Rightarrow -13 \cdot 11 \equiv 1 \mod 48 \Rightarrow d = -13 \equiv 35 \mod 48$$

Résultat : La clé privée est $d = \boxed{35}$

Question 0-4 Dans le mode opératoire Counter, un compteur est ajouté (concaténé) au vecteur d'initialisation (appelé "nonce" dans ce mode). A chaque nouveau bloc le compteur augmente de 1, comme sur le schéma suivant.
Une erreur de transmission s'est produit sur le message chiffré c_2 . Combien de blocs de messages claires seront impactés lors du déchiffrement ?



Counter (CTR) mode encryption

==

In Counter mode, a counter is added (concatenated) to the initialization vector (called "nonce" in this mode). For each new block, the counter increases by 1, as shown in the diagram above. A transmission error occurred on the ciphertext c_2. How many plaintext blocks will be impacted during decryption ?"

Solution 0-4
Les blocs sont chiffrés de manières indépendantes l'un de l'autre. **Conclusion :**

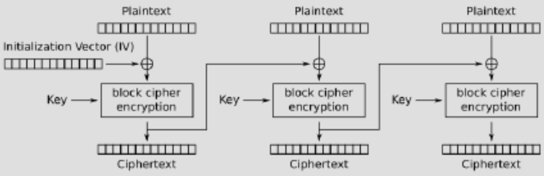
Un seul bloc de message est impacté : m_2

Question 0-5 Vous avez reçu le message "aWxlc3Rjb29sY2V0ZXhhbQo=" écrit en base 64.
Le message était chiffré avec le cryptosystem AES, le mode opératoire CBC en 128 bit, en utilisant les paramètres suivants :
clé en hexadécimale : K=cdee6ff703f5b4aac9cf61efd0397766

vecteur d'initialisation en hexadécimale : iv=654f344d1dd5c4abc514546e4c2cf590
Quel est le message d'origine ? (rajouter -base64 à la fin de votre instuction openssl)

==

The message you received, "aWxlc3Rjb29sY2V0ZXhhbQo=", is encoded in Base64. It was encrypted using the AES cryptosystem in CBC mode with 128-bit keys, and the following parameters :
Key in hexadecimal : K=cdee6ff703f5b4aac9cf61efd0397766
Initialization vector in hexadecimal : iv=654f344d1dd5c4abc514546e4c2cf590
What is the plaintext message (add -base64 at the end of your openssl instruciton)



Cipher Block Chaining (CBC) mode encryption

Solution 0-5 Sauvegarder le message base64 dans un fichier, par exemple : echo "aWxlc3Rjb29sY2V0ZXhhbQo=" > message.b64 Lancer la commande OpenSSL : openssl enc -d -aes-128-cbc -K cdee6ff703f5b4aac9cf61efd0397766 -iv 654f344d1dd5c4abc514546e4c2cf590 -base64 -in message.b64
Résultat du déchiffrement :

`ilestcoolcetexam`