Chiffrement et codes correcteurs

Commencé le	Monday 7 April 2025, 10:19
État	Terminé
Terminé le	Monday 7 April 2025, 11:19
Temps mis	59 min 52 s

Description

Marquer la question

Le téléphone portable est strictement interdit ainsi que l'utilisation d'internet.

Vous pouvez utiliser Python comme calculatrice .
Pour rappel x^y s'écrit $x**y$ sur Python

Pour les puissances modulaires il est conseillé d'utiliser la fonction pow(a,i,n) qui calcule $a^i \mod n$ (si vous écrivez un script vérifier s'il ne faut pas rajouter import math en début). L'inverse modulo n de a peut être calculer par pow(a,-1,n).

Pour l'exercice sur la feuille je vous invite à écrire votre prénom et nom en majuscules ainsi que l'UID de façon lisible .

Bon travail !
===

Internet and phones are forbiden.

You can use Python as a calculator.

Recall that x^y is written as $x**y$ in Python. It is advisable to use pow(a,i,n) to calculate $a^i \mod n$ (if you write a script check whether you need to add import math at the begging). The modular inverse of a modulo n can be calculated by pow(a,-1,n).

Please try to write your name and UID on the paper as readable as you can.

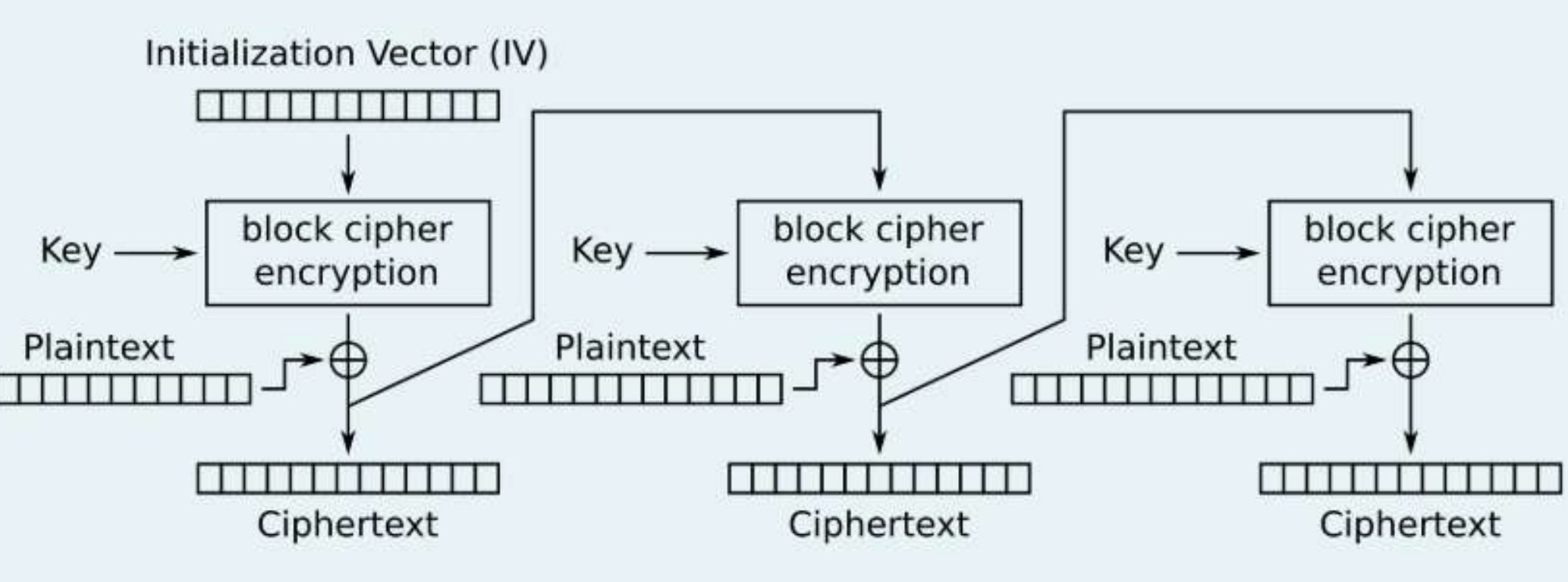
Have a nice work!

Description

Marquer la question

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 :



Cipher Feedback (CFB) mode encryption

Soit $c_0 = IV$ le vecteur d'initialisation et K la clé de chiffrement et $m_1, m_2, \ldots m_n$ les blocs de messages. Ainsi d'après le schéma

$c_i = m_i \oplus \mathrm{Enc}_K(c_{i-1})$

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 $\mathrm{Enc}_{k_1,k_2}(x) = P(x \oplus k_1) \oplus k_2$.

On décide de combiner le mode opératoire CFB avec le chiffrement Even-Mansour en choisissant deux clés et en remplaçant $\mathrm{Enc}_K(c_{i-1})$ par $\mathrm{Enc}_{k_1,k_2}(c_{i-1})$

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 $m_1 = 0100$.

===

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 $m_1, m_2, \ldots, m_n$ the message blocks. According to the diagram (see above):

$c_i = m_i \oplus \mathrm{Enc}_K(c_{i-1})$

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 $\mathrm{Enc}_{k_1,k_2}(x) = P(x \oplus k_1) \oplus k_2$.

We decide to combine the CFB mode with the Even-Mansour encryption by choosing two keys and replacing $\mathrm{Enc}_K(c_{i-1})$ with $\mathrm{Enc}_{k_1,k_2}(c_{i-1})$.

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 $m_1 = 0100$.

Description

Marquer la question

Alice et Bob ont crée leur propre cryptosystem "Shifted Power" comme suit:

Génération de Clés :

- **Choix des Paramètres :**
  - Choisir p premier, g générateur de $Z/pZ^\times$
  - 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.

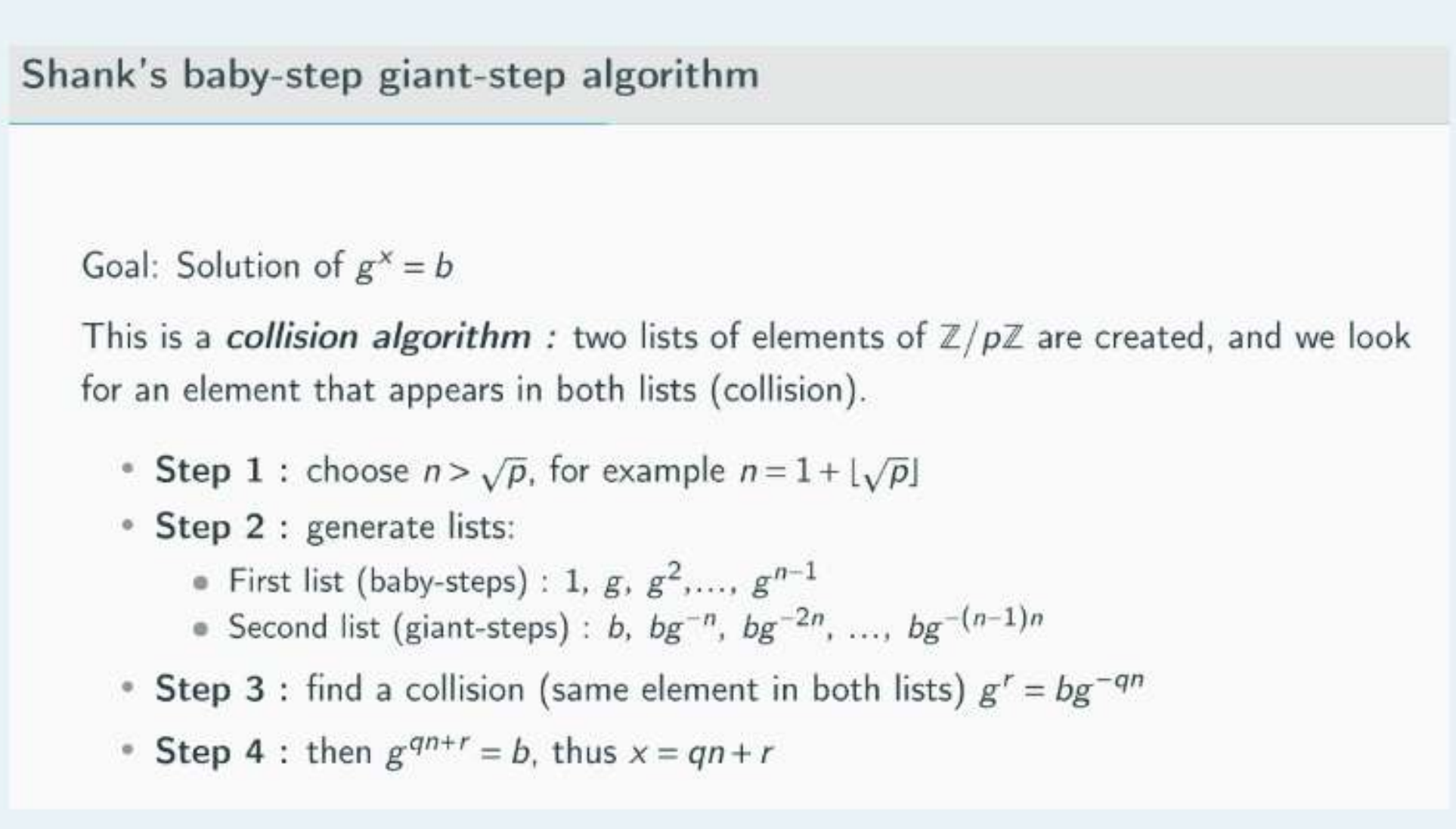
Chiffrement :

- **Codage du Message :**
  - Le message M doit être un entier tel que $1 \le M \le p-1$
  - 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.



Shank's baby-step giant-step algorithm

Goal: Solution of $g^x = b$

This is a ***collision algorithm*** : two lists of elements of $\mathbb{Z}/p\mathbb{Z}$ 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 $Z/pZ^\times$
- 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:

Message Encoding:

- The message M must be an integer such that $1 \le M \le p-1$
- 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.

Question **1**

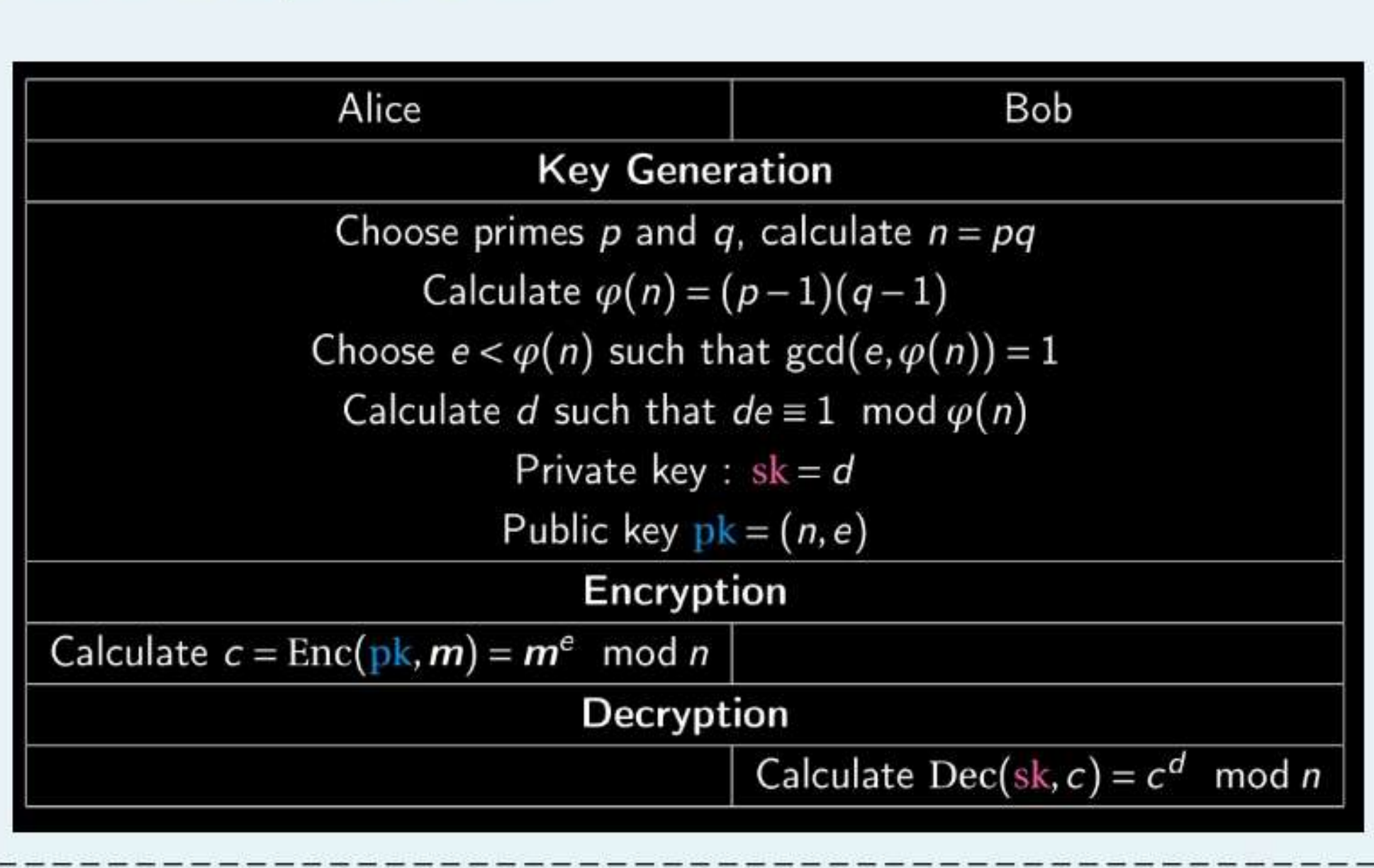
Terminé

Noté sur 2,00

Marquer la question

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?"

● a. 35

○ b. 54

○ c. 45

○ d. 27

○ e. autre / other

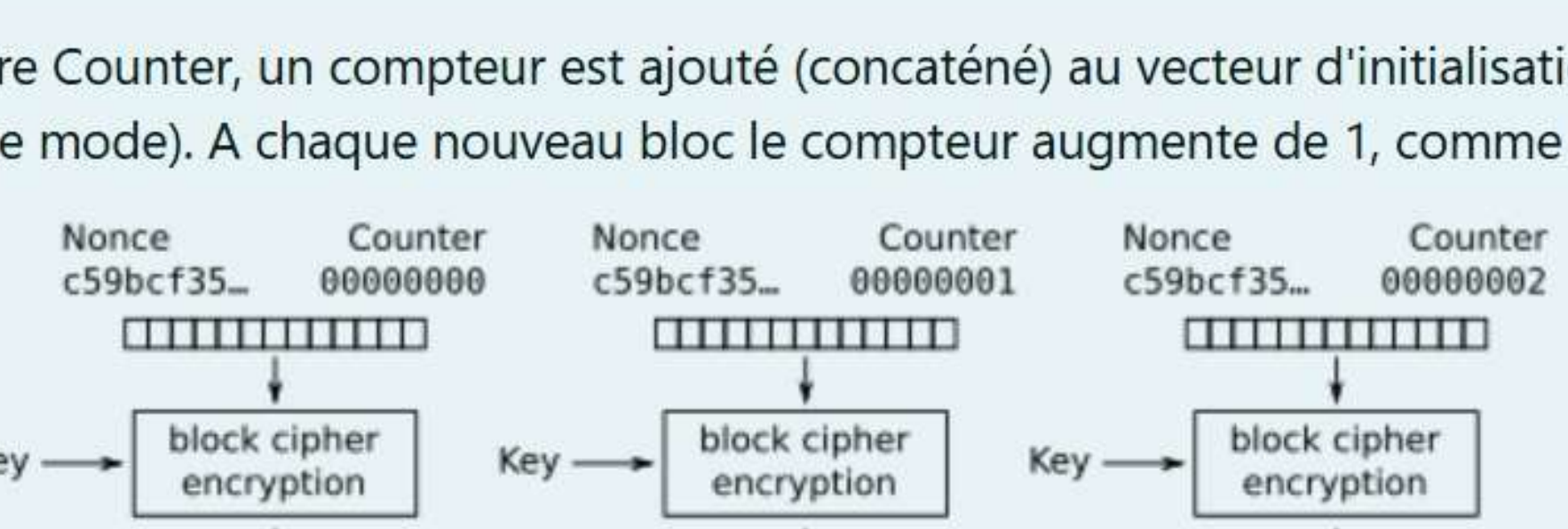
Question **2**

Terminé

Noté sur 2,00

Marquer la question

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.



Counter (CTR) mode encryption

Une erreur de transmission s'est produit sur le message chiffré c_2 . Combien de blocs de messages claires seront impactés lors du déchiffrement?

=================================

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?"

● a. 1

○ b. 3

○ c. 0

○ d. autre

○ e. 2

Question **3**

Terminé

Noté sur 2,00

Marquer la question

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

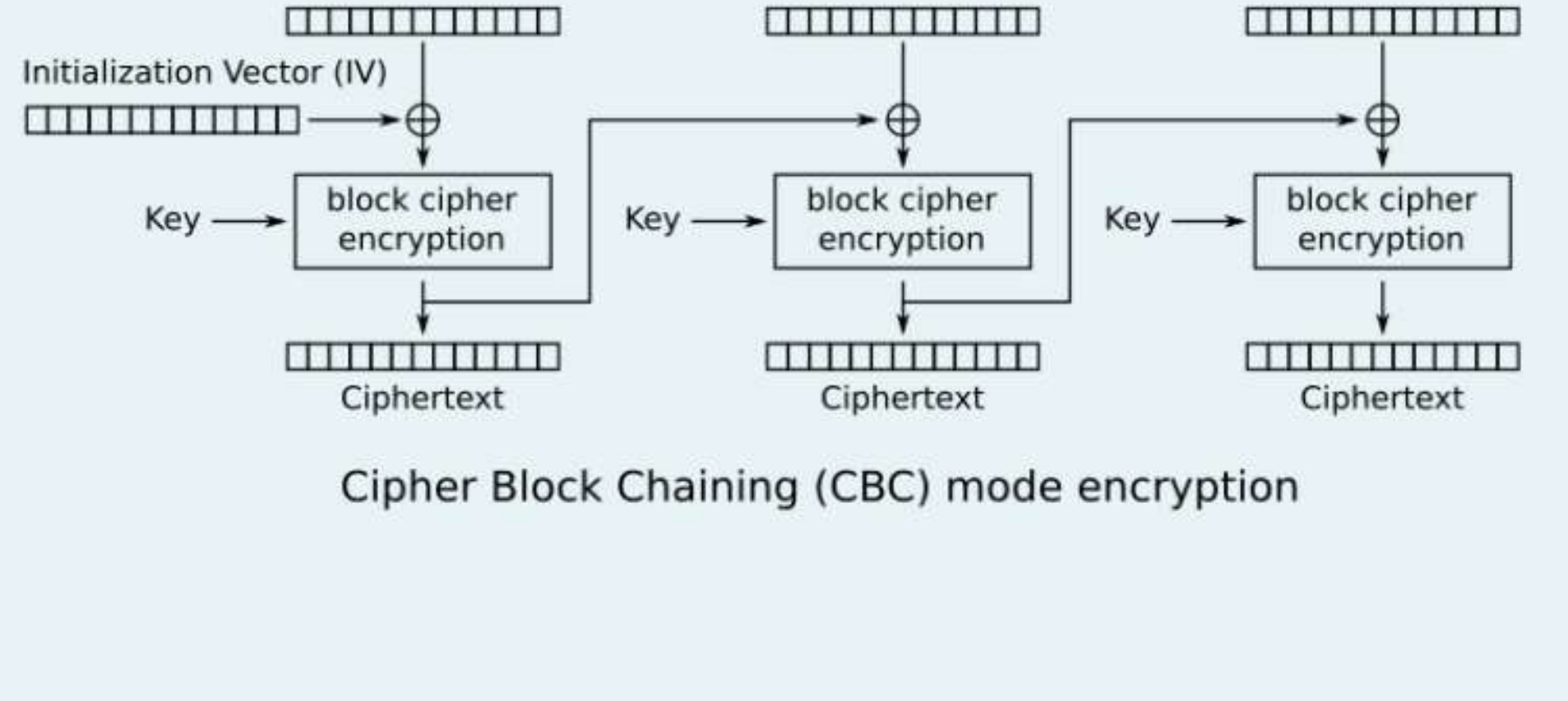
Quel est le message d'origine? (rajouter -base64 à la fin de votre instuction openssl)

===

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

Réponse : Z2BNUuhf8CF+wY0Yi6aXYAa8Nu+LMnlJlPrBMuVjr3U=

Terminer la relecture