N° d'ordre : IRS / TCO

Année Universitaire : 2022 / 2023

UNIVERSITÉ D'ANTANANARIVO

ÉCOLE SUPÉRIEURE POLYTECHNIQUE

MENTION TELECOMMUNICATION

RAPPORT SUR NOTRE APPLICATION

Domaine : Sciences de l'Ingénieur

Mention : Télécommunication

Parcours : Système et Traitement de l'Information

APPLICATION DE CHIFFREMENT ET DE DECHIFFREMENT RSA

Etudiants :

ANDRIANOMANANA Nomenjanahary Radoniaina

FANASINARIMINO Nirhy Andriantsoa

RAJHONSON Sedra Riantsoa Lala

Enseignant :

Monsieur ANDRIANARISON Asafa Miradontsoa

TABLE DES MATIÈRES

L'APPLICATION MOBILE RSA

1.1 Introduction

L'application RSA est conçue pour aider l'utilisateur à chiffrer et/ou à déchiffrer une information grâce à laquelle il pourra sécuriser sa transmission.

RSA est très populaire en télécommunication, connue par sa forte technique de sécurisation lors d'une transmission entre un émetteur et un récepteur, d'où le choix de notre groupe sur le développement de cette application.

Avec RSA, on peut facilement générer des clés, nécessaire pour le chiffrement et le déchiffrement de l'information.

1.2 Notion sur le chiffrement RSA

1.2.1 Définition

Un système de chiffrement RSA est une méthode de chiffrement asymétrique simple d'utilisation, très populaire dans de nombreux domaines nécessitant des transferts de données par Internet. Il se compose de deux clés de chiffrement RSA, l'une publique et l'autre privée. Alors que la clé publique est utilisée pour le chiffrement, la clé privée sert à déchiffrer les données. Étant donné qu'aucun algorithme n'est capable de décoder la clé privée à partir de la clé publique, cette méthode est vue comme un processus sûr. En plus du chiffrage, le système de chiffrement RSA permet également de générer ses propres signatures numériques.

1.2.2 Fonctionnement

1.2.2.1 Fonctionnement général

Le chiffrement RSA est asymétrique, il utilise une paire de clés (des nombres entiers) composée d'une clé publique pour chiffrer et d'une clé privée pour déchiffrer des données confidentielles. Les deux clés sont créées par une personne, souvent nommée par convention Alice, qui souhaite que lui soient envoyées des données confidentielles. Alice rend la clé publique accessible. Cette clé est utilisée par ses correspondants (Bob, etc.) pour chiffrer les données qui lui sont envoyées. La clé privée est quant à elle réservée à Alice, et lui permet de déchiffrer ces données. La clé privée peut aussi être utilisée par Alice pour signer une donnée qu'elle envoie, la clé publique permettant à n'importe lequel de ses correspondants de vérifier la signature. Une condition indispensable est qu'il soit « calculatoires impossible » de

déchiffrer à l'aide de la seule clé publique, en particulier de reconstituer la clé privée à partir de la clé publique, c'est-à-dire que les moyens de calcul disponibles et les méthodes connues au moment de l'échange (et le temps que le secret doit être conservé) ne le permettent pas.

Le chiffrement RSA est souvent utilisé pour communiquer une clé de chiffrement symétrique, qui permet alors de poursuivre l'échange de façon confidentielle : Bob envoie à Alice une clé de chiffrement symétrique qui peut ensuite être utilisée par Alice et Bob pour échanger des données.

1.2.2.2 Fonctionnement détaillé

La seule description des principes mathématiques sur lesquels repose l'algorithme RSA n'est pas suffisante. Sa mise en œuvre concrète demande de tenir compte d'autres questions qui sont essentielles pour la sécurité. Par exemple le couple (clé privée, clé publique) doit être engendré par un procédé vraiment aléatoire qui, même s'il est connu, ne permet pas de reconstituer la clé privée. Les données chiffrées ne doivent pas être trop courtes, pour que le déchiffrement demande vraiment un calcul modulaire, et complété de façon, c’est pourquoi la sécurité du RSA repose sur le fait de savoir bien créer les clés de chiffrement et déchiffrement.

L'étape de création des clés est à la charge d'Alice. Elle n'intervient pas à chaque chiffrement, car les clés peuvent être réutilisées. La difficulté première, que ne règle pas le chiffrement, est que Bob soit bien certain que la clé publique qu'il détient est celle d'Alice. Le renouvellement des clés n'intervient que si la clé privée est compromise, ou par précaution au bout d'un certain temps (qui peut se compter en années). Pour ce faire, il faut suivre les étapes suivantes :

- Choisir p et q, deux nombres premiers distincts ;
- Calculer leur produit n = pq, appelé module de chiffrement ;
- Calculer $\varphi(n) = (p - 1)(q - 1)$ (c'est la valeur de l'indicatrice d'Euler en n) ;
- Choisir un entier naturel e premier avec $\varphi(n)$ et strictement inférieur à $\varphi(n)$, appelé exposant de chiffrement ;
- Calculer l'entier naturel d, inverse modulaire de e pour la multiplication modulo $\varphi(n)$ et strictement inférieur à $\varphi(n)$, appelé exposant de déchiffrement ; d peut se calculer efficacement par l'algorithme d'Euclide étendu.

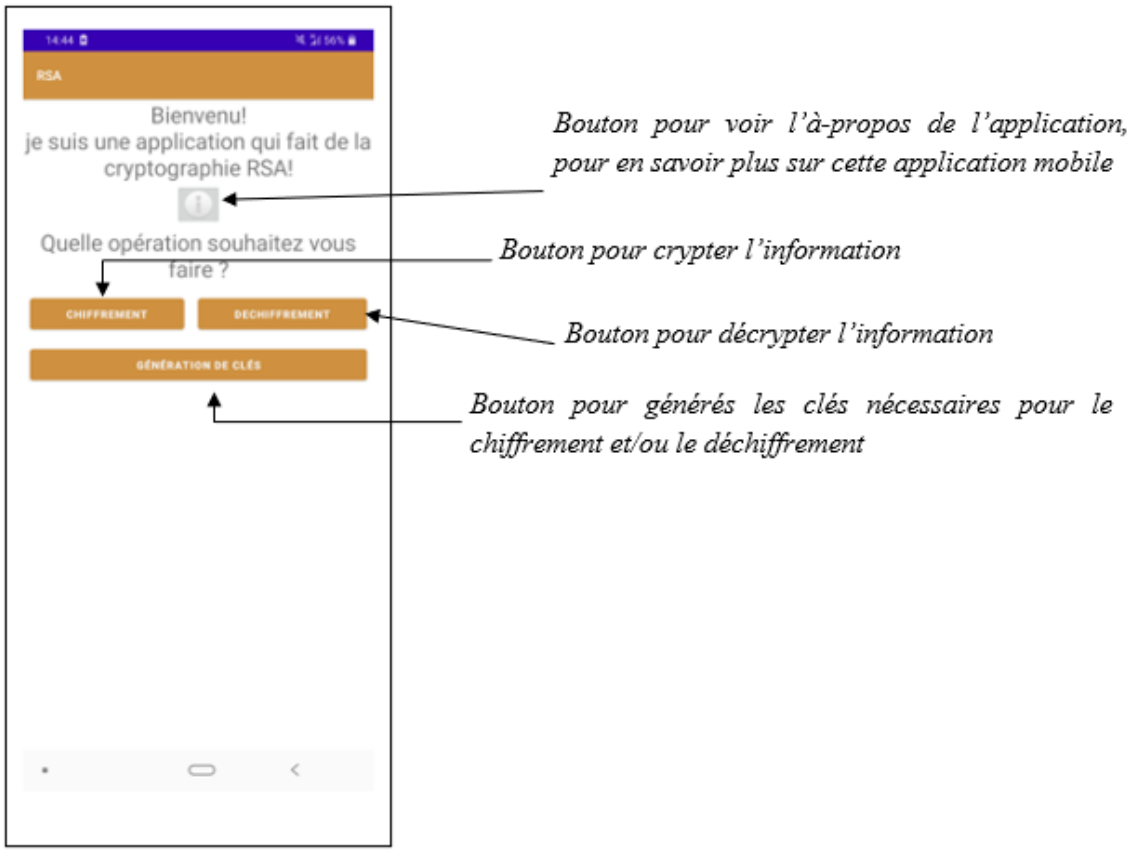
- Comme e est premier avec φ(n), d'après le théorème de Bachet-Bézout il existe deux entiers d et k tels que ed = 1 + kφ(n), c'est-à-dire que ed ≡ 1 (mod φ(n)) : e est bien inversible modulo φ(n).

Le couple (n, e) ou (e, n) est la clé publique du chiffrement, alors que sa clé privée est le nombre d sachant que l'opération de déchiffrement ne demande que la clef privée d et l'entier n, connu par la clé publique (la clé privée est parfois aussi définie comme le couple (d, n) ou le triplet (p, q, d).

1.3 Cahier de charge

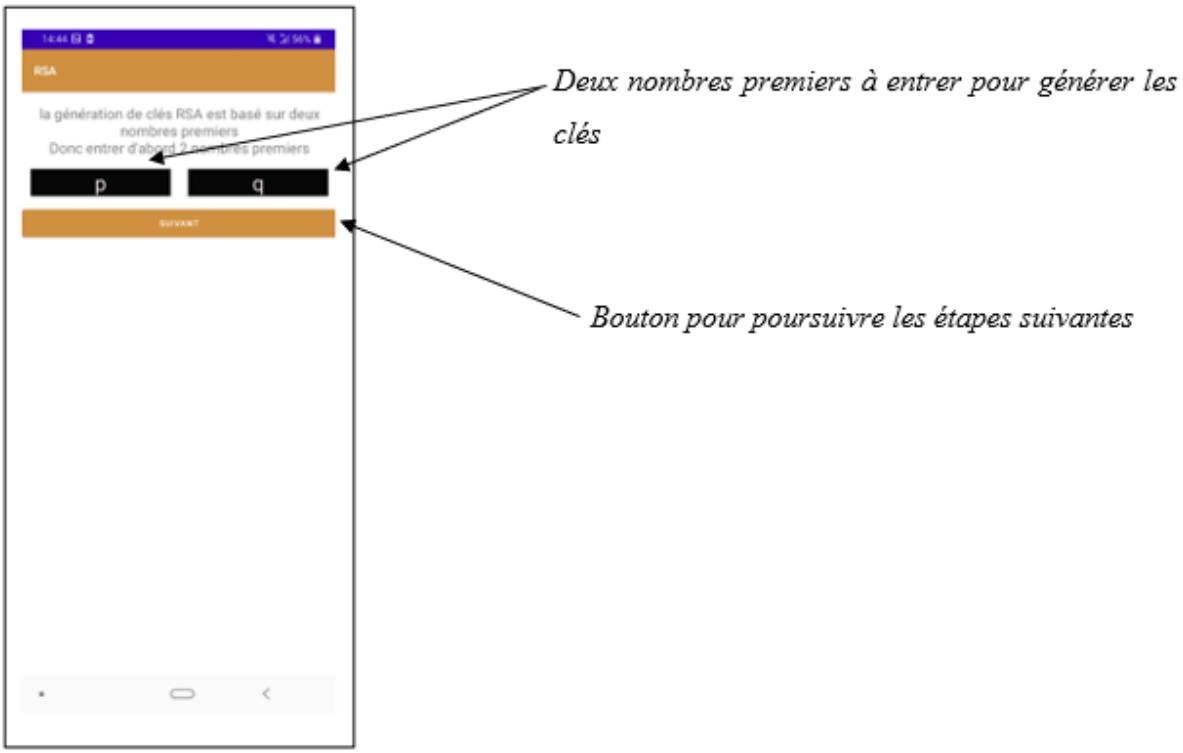
Pour mieux vous expliquer sur le fonctionnement de notre application, voici des images suivies de quelques explications sur l'utilité des boutons présents dans les interfaces de l'application RSA.

- Au premier contact de notre application mobile appelé RSA, voici la fenêtre qui accueil l'utilisateur :



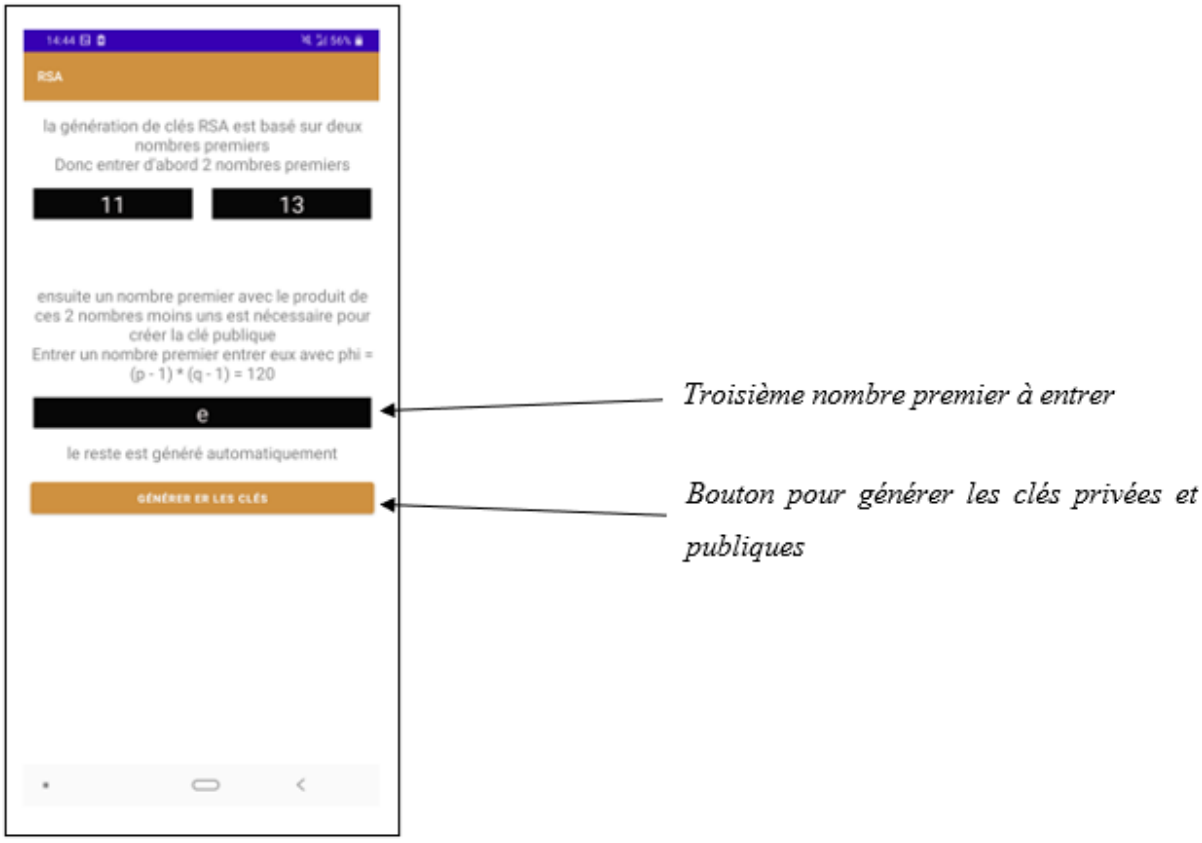
- Lorsqu'on clique sur le bouton information, une fenêtre s'affichera, comme celle présentée suivante :

- En faisant retour aux fenêtres principales, nous pouvons alors débuter le traitement de notre information, c'est-à-dire passer au cryptage ou au décryptage d'une information. Mais avant, on doit d'abord générer les clés que ce soit celui du chiffrement ou celui du déchiffrement. Pour ce faire, on clique sur le bouton « Génération des clés », qui nous ouvre la fenêtre suivante :



Cette fenêtre est nécessaire pour demander à l'utilisateur d'entrer deux nombres premiers nécessaires pour la génération de la clé publique utile pour le chiffrement des informations.

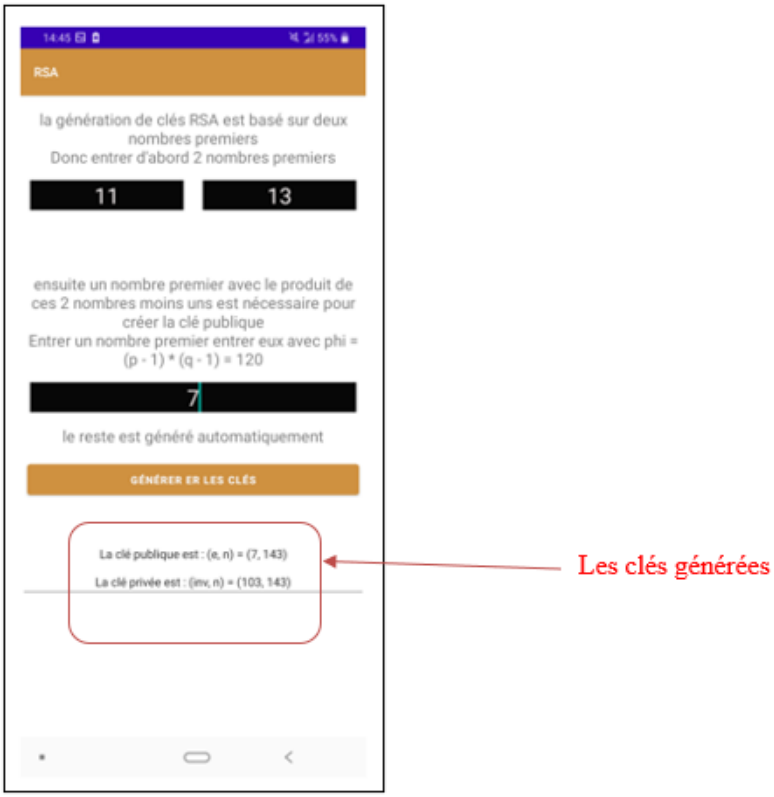
- Une fois que l'étape précédente est validée, on peut passer au suivant en cliquant sur le bouton « suivant », qui va nous présenter la fenêtre :



Qui demande l'entrée d'un troisième nombre premier, qui respect cette formule :

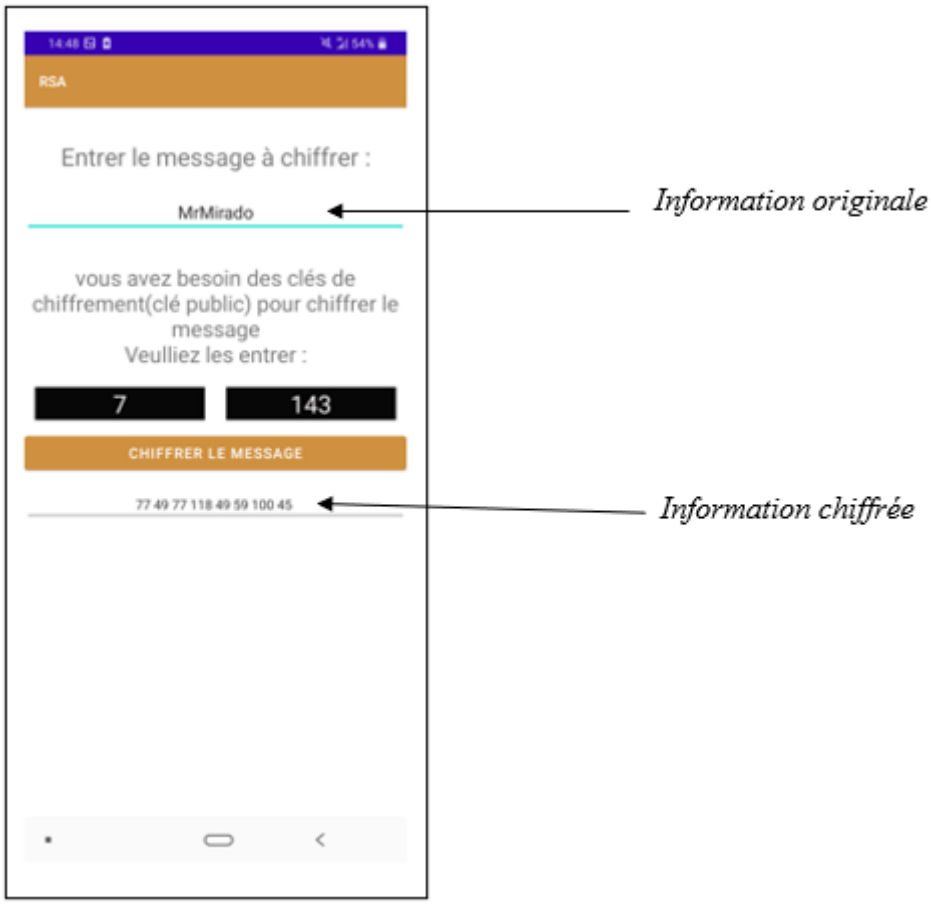
(P-1) *(q-1) =120 avec p et q les nombres entrés précédemment.

- Les trois nombres validés, on peut à présent générer à la fois les deux clés utiles pour le chiffrement et le déchiffrement qui sont respectivement la clé publique et clé privée. La fenêtre suivante montre un exemple des clés générées grâces aux nombres p = 11, q = 13 et e = 7.

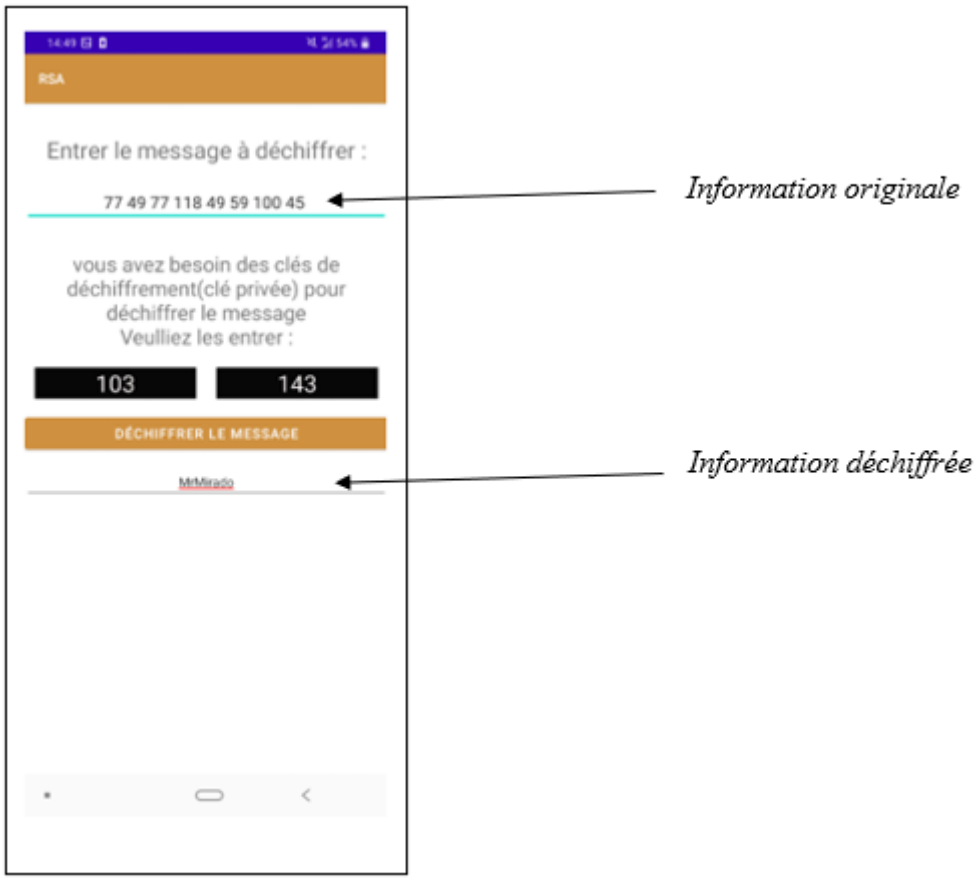


- Dès qu'on obtient les clés, on peut alors revenir à la fenêtre principale et choisir sur genre de traitement qu'on veut faire, c'est-à-dire chiffrement et/ou déchiffrement. Si notre choix se porte sur le cryptage de l'information, alors on clique sur le bouton « chiffrement », qui nous ouvre la fenêtre suivante :

La fenêtre demande à l'utilisateur d'entrer l'information à crypter, puis d'entrer la clé publique générée précédemment dans la fenêtre « génération des clés ». Toutes les informations complétées, on peut passer au chiffrement du message en cliquant sur le bouton « chiffrer le message ». La figure suivante illustre un exemple de chiffrement d'une information :



- On effectue également la même étape pour celui du déchiffrement, sauf que la clé devient la clé privée qui est elle aussi générée précédemment. Une figure qui illustre un exemple pour une meilleure compréhension :


RSA
Entrer le message à déchiffrer :
77 49 77 118 49 59 100 45
vous avez besoin des clés de déchiffrement(clé privée) pour déchiffrer le message
Veulliez les entrer :
103
143
DÉCHIFFRER LE MESSAGE
MrMirado
Information originale
Information déchiffrée