Initiation à la cryptographie

Correction TD de cryptographie n°2

—TELECOM Nancy 2A Formation par Apprentissage—

1 Chiffrement à flot

▸ **Exercice 1.** Malléabilité des chiffrements par flot

Dans cet exercice, nous considérons un chiffrement par flot, noté E, paramétré par une clé secrète K et un vecteur d'initialisation IV.

1. Rappelez le principe général de fonctionnement d'un chiffrement par flot. Étant donnés un message en clair M, une clé K et un vecteur d'initialisation IV, comment le chiffré C est-il obtenu ?

   Supposons qu'Alice ait envie de faire un virement bancaire de 100 euros à Mallory. Pour cela, elle utilise un système de chiffrement par flot E dont seules elle et sa banque connaissent la clé privée K. Alice chiffre donc l'ordre de virement M qu'elle envoie alors à sa banque.

   Mallory est capable d'intercepter et de modifier ce message chiffré C avant que la banque d'Alice ne le reçoive. Elle ne connaît pas M, mais elle sait que les ordres de virement sont des chaînes de caractères de la forme suivante :

$$M = \langle \textit{date} \rangle\texttt{:}\langle \textit{nonce} \rangle\texttt{:}\langle \textit{émetteur} \rangle\texttt{:}\langle \textit{destinataire} \rangle\texttt{:}\langle \textit{montant} \rangle\texttt{:}\langle \textit{commentaire} \rangle$$

   où *nonce* est une chaîne aléatoire de 8 chiffres décimaux, que la banque aura transmise à Alice juste avant que celle-ci ne prépare son ordre de virement.

2. À quoi sert ce *nonce* ?

   Dans le cas d'Alice et Mallory, le message est donc de la forme suivante :

$$M = \texttt{2019-01-28:}\langle \textit{nonce} \rangle\texttt{:Alice:Mallory:100:}\langle \textit{commentaire} \rangle$$

3. Comment Mallory peut-elle faire pour obtenir 999 euros de la part d'Alice ?
4. Quelle contre-mesure est-il possible de mettre en œuvre pour empêcher ce genre d'attaque ?

✂ -

Correction :

1. *Le chiffrement par flot est un générateur pseudo-aléatoire, initialisé par K et IV, et qui génère une suite de bits, appelée* suite chiffrante, *notée Z. Le message M est alors chiffré en utilisant la suite chiffrante comme un masque : $C = M \oplus Z$.*
2. *À éviter le rejeu : la banque distribue un nonce unique à chaque transaction d'une même journée, et refuse toute transaction qui porterait le même nonce qu'une transaction déjà effectuée.*
3. *Mallory construit les chaînes de caractères*

$$M_1 = \texttt{xxxxxxxxxx:xxxxxxxx:xxxxx:xxxxxxx:100:}$$
$$M_2 = \texttt{xxxxxxxxxx:xxxxxxxx:xxxxx:xxxxxxx:999:}$$

   Elle calcule alors le chiffré $C' = C \oplus M_1 \oplus M_2$ et envoie celui-ci à la banque.
   La banque va alors déchiffrer C' comme $M' = C' \oplus Z = C \oplus M_1 \oplus M_2 \oplus Z$. Puisque $C \oplus Z = M$, on a donc $M' = M \oplus M_1 \oplus M_2$, d'où

$$M' = \texttt{2019-01-28:}\langle \textit{nonce} \rangle\texttt{:Alice:Mallory:999:}\langle \textit{commentaire} \rangle$$

4. *Un code d'authentification du message (MAC), paramétré par une clé secrète commune entre Alice et sa banque, permettrait de s'assurer que le message reçu provient bien d'Alice et qu'il n'a pas été modifié par une tierce personne.*

- ✂

2 Chiffrement par blocs et modes opératoires

▸ **Exercice 2.** Electronic Code Book

Le mode de chiffrement ECB (*Electronic Code Book* ou *Dictionnaire de code*) est le mode de chiffrement le plus simple que l'on puisse imaginer : chaque bloc de données est chiffré indépendamment par la fonction de chiffrement.

1. Ce mode de chiffrement n'est pas sûr, expliquer pourquoi.
2. Jack, qui gagne 105000€ par an[1], a retrouvé l'entrée chiffrée qui lui correspond dans la base de donnée des salaires de son entreprise :

   `Q92DFPVXC9IO`

   Sachant que la fonction de chiffrement utilisé a des blocs de deux caractères et que le service informatique de son entreprise ne comprend aucun expert en cryptographie (entendre par là, utilise le mode ECB !), retrouver le salaire de Jane la patronne de Jack parmi le reste de la base de donnée :

   `TOAV6RFPY5VXC9, YPFGFPDFDFIO, Q9AXFPC9IOIO, ACED4TFPVXIOIO, UTJSDGFPRTAVIO.`
3. Exemple 2. Imaginer à quel point ce mode chiffrement est déplorable pour les photographies.

✂ ----------

Correction :

1. *Deux blocs identiques auront le même chiffré, ainsi de l'information peut fuir.*
2. *On peut supposer que l'entrée de Jack donne la correspondance suivante :*

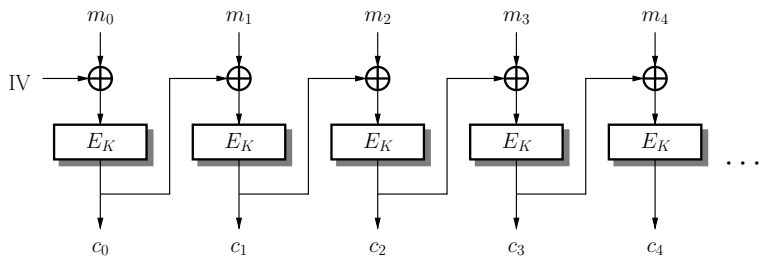
   `Ja|ck|??|10|50|00`
   `Q9|2D|FP|VX|C9|IO`

   `FP` doit correspondre au séparateur de champ. Jane a aussi un prénom de 4 lettres qui commence par «Ja» donc son entrée chiffrée commence par `Q9??FP`, c'est `Q9AXFPC9IOIO`. Son salaire est ainsi `C9IOIO`, soit 500000€ par an.
3. *Cela correspond à remplacer les couleurs si la taille du bloc correspond à un pixel, ou des blocs d'image par d'autre, on reconnaitra la forme de l'image : par ex les pixels noir deviendront tous rouges.*

---------- ✂

▸ **Exercice 3.** Cipher Block Chaining

Le mode de chiffrement CBC (*Cipher Block Chaining* ou *Enchaînement des blocs*) suit le schéma suivant :

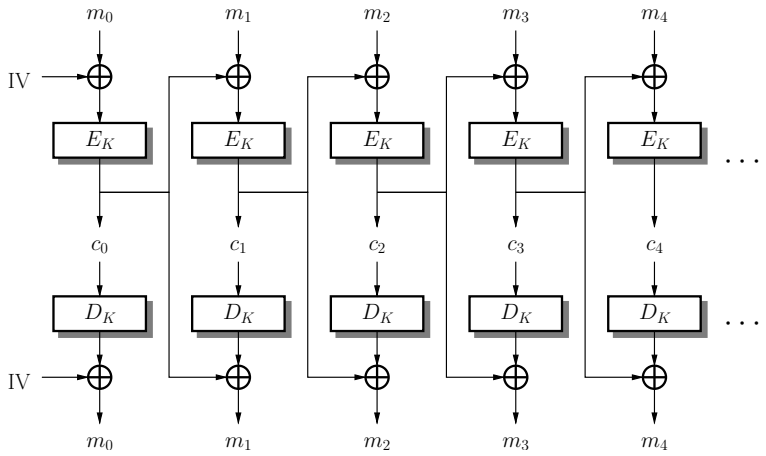


1. Dessiner le schéma de déchiffrement correspondant à ce mode de chiffrement.
2. À quoi sert le vecteur d'initialisation (IV) ? Doit-il rester secret ?
3. Que se passe-t-il lors du déchiffrement si l'un des blocs chiffrés a été altéré ?

1. Exemple de `https://fr.wikipedia.org/wiki/Mode_d\%27op\%C3\%A9ration_(cryptographie)`.

Correction :

1. *Le voilà :*



2. *Si il n'y avait pas d'IV deux fichiers identiques auraient les mêmes chiffrés.*
3. *Seulement deux blocs sont altérés.*

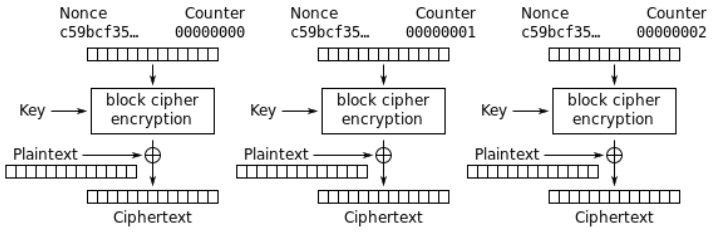
▸ **Exercice 4.** CounTeR

Le mode de chiffrement CTR (*mode compteur*) consiste à chiffrer un compteur qui est incrémenté à chaque bloc, puis à en calculer le ou exclusif avec le message. Le compteur est initialisé à une valeur choisie au hasard appelée le *nonce*.

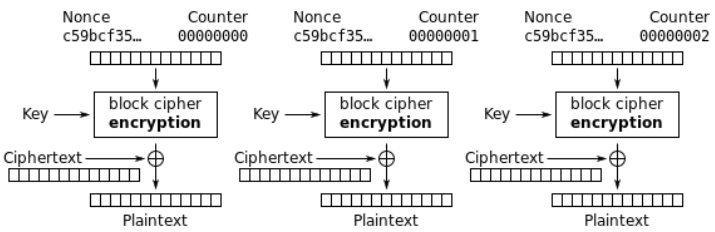
1. Dessiner les schéma de chiffrement et déchiffrement de ce mode opératoire.
2. Expliquer l'intérêt du *nonce*.
3. Quel intérêt voyez-vous à ce mode de chiffrement quant à son implémentation ?

Correction :

1. *Voici les schémas.*



Counter (CTR) mode encryption



Counter (CTR) mode decryption

2. *C'est un IV, sinon toujours le même stream.*
3. *Facilement parallélisable. De plus il n'y a pas besoin de fonction de déchiffrement ! C'est avantageux dans certain cas : pour AES le déchiffrement est plus cher que le chiffrement.*

▸ **Exercice 5.** Modes opératoires et authentification

1. Un message chiffré avec un chiffrement par blocs et un mode opératoire quelconque garantit-il l'authentification du message reçu ?
2. Par exemple, soit un chiffré AES-CBC : $(\mathrm{IV}, c_0, c_1, \ldots)$ intercepté par un attaquant. Que peut-il retransmettre au destinataire pour se faire passer pour l'émetteur officiel ?
3. Que faut-il ajouter au système pour obtenir une garantie d'authenticité du message reçu.

Correction :

1. *Non.*
2. *S'il coupe le message chiffré à n'importe quel bloc, le destinataire ne verra pas la différence.*
3. *On ajoute un MAC.*
