Introduction à la Cryptographie

Télécom Nancy, 2A Apprentissage — Examen 2021/2022 — 29/03/2022, 16h-18h

Une feuille de notes manuscrite recto/verso autorisée. La calculatrice est le seul appareil électronique toléré. **Ce sujet comporte quatre exercices distincts**, indépendants, et pouvant être traités dans n'importe quel ordre. Au sein d'un exercice, les questions dépendent généralement les unes des autres (pas tout le temps). On appréciera les réponses **argumentés**, rédigées avec **soin** et **précision**.

Exercice 1 Chiffrement de César

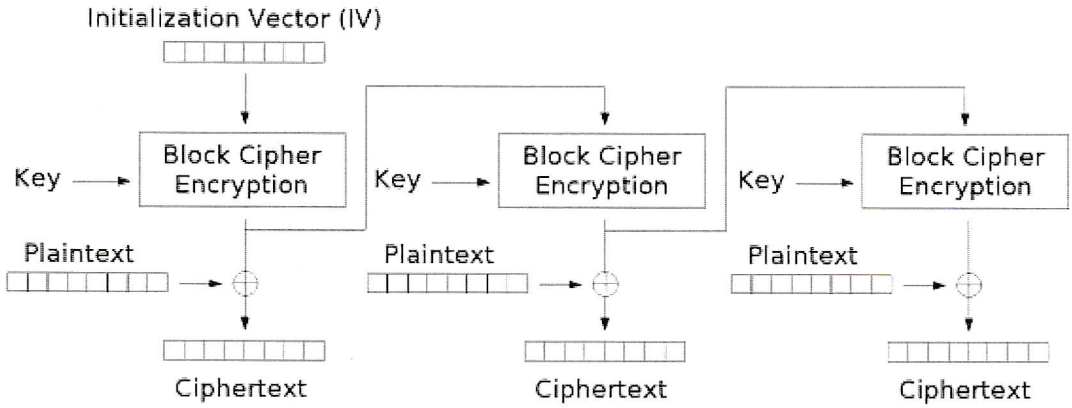
Soit le chiffré de César suivant : mrkirmiyvw hy ryqivmuyi

1.1 Quel est le message clair, étant donné la clé $K = 4$?

1.2 Pourquoi le chiffrement de César n'est-il pas sûr ? Donner deux raisons.

Exercice 2 Modes opératoires

Le mode de chiffrement OFB (*Output FeedBack*) suit le schéma suivant :



Output Feedback (OFB) mode encryption

2.1 Pourquoi y a-t-il un vecteur d'initialisation (IV) ? Doit-il rester secret ?

2.2 Dessiner le schéma de déchiffrement correspondant à ce mode de chiffrement.

2.3 Que se passe-t-il lors du déchiffrement si un seul bit d'un des blocs chiffrés a été altéré ?

2.4 Ce mode d'opération garantit-il l'intégrité du message ? Si oui, expliquez pourquoi. Si non, montrez que pouvez altéré le message reçu sans que cela ne pose problème lors du déchiffrement.

Exercice 3 Fonctions de hachage cryptographiques

3.1 Rappeler les trois propriétés de sécurité d'une fonction de hachage cryptographique.

3.2 Supposons qu'on utilise une fonction de hachage cryptographique afin de vérifier l'intégrité d'un fichier télécharge comme suit :

— Le fichier est téléchargé en utilisant un canal public.
— Le haché du fichier original est téléchargé en utilisant un canal authentifié.
— On vérifie si le haché du fichier téléchargé correspond au haché du fichier original.

Laquelle des trois propriétés des fonctions de hachage garantit l'intégrité du fichier ici ?
Pourquoi doit-on utiliser un canal authentifié pour télécharger le haché du fichier original ?

3.3 Supposons maintenant qu'un utilise une fonction de hachage pour le stockage des mots de passe d'un site web : au lieu de stocker le mot de passe directement, on stocke son haché.
Comment authentifier un utilisateur dans ce cas ?
Supposons qu'un attaquant récupère la liste de tous les hachés, et veut retrouver les mots de passe. À quelle propriété des fonctions de hachage doit-il s'attaquer ?

3.4 Pourquoi utilise-t-on (en plus de du hachage "simple") généralement du "sel" dans le cadre du stockage des mots de passe ?

Exercice 4 Cryptographie asymétrique : RSA

Considérons le système RSA construit à partir des entier $p = 7$ et $q = 13$.

4.1 Calculer N et $\varphi(N)$.

4.2 Calculer l'exposant de déchiffrement d associé à $e = 5$ en utilisant l'algorithme d'Euclide étendu.

4.3 Calculer le chiffré associé au message $m = 4$.

Considérons maintenant la clé publique $e = 3$ et $N = 3901$.

4.4 Vous avez observé le message chiffré $c = 27$, dont vous savez qu'elle a été chiffré avec cette clé. En supposant que le message clair m était *très* petit, pouvez-vous retrouver m ? Comment ? Que vaut m alors ?