Introduction à la Cryptographie

Télécom Nancy, 2A Apprentissage — Examen 2022/2023 — 24/03/2023, 14h-16h

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 historique (4 points)

Soit le chiffré : diomjypxodji v gv xmtkojbmvkcdz

1.1 Quel est le chiffrement utilisé ?

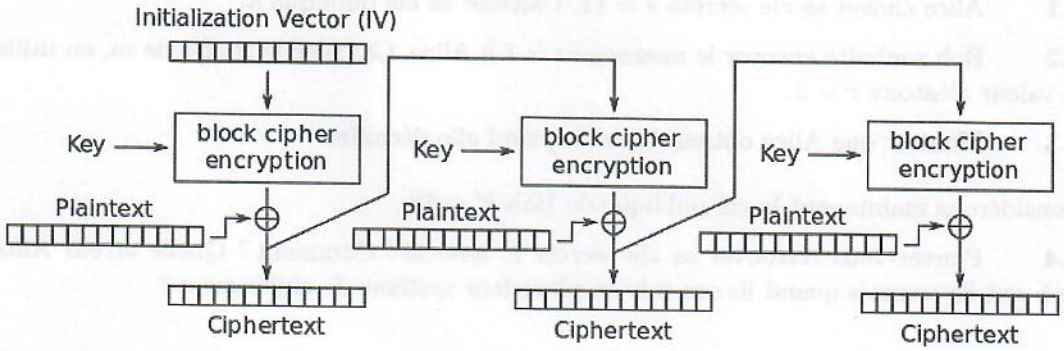
1.2 Quel est le message clair, sachant qu'il commence par « INTRO » ? Quelle est la clé utilisé ?

1.3 Comment appelle-t-on ce type d'attaque ? Combien de lettres connus faut-il pour pouvoir retrouver la clé ?

1.4 Pourquoi ce type de chiffrement n'est-il pas sûr ? Donner deux raisons.

Exercice 2 Modes opératoires (5 points)

Le mode de chiffrement CFB (*Cipher FeedBack*) suit le schéma suivant :



Cipher Feedback (CFB) 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 Supposons qu'un attaquant intercepte le chiffré AES-CFB $(\text{IV}, c_0, c_1, c_2, \ldots, c_n)$ du message $(m_0, m_1, m_2, \ldots, m_n)$. Que peut-il retransmettre au destinataire, pour quel message reçu à la fin ? Un message chiffré avec ce mode opératoire garantit-il donc l'authentification du message reçu ?