Devoir 1, dû le 26 janvier 2023, à remettre par Turnin avant 23h59. Un devoir à remettre en format pdf par équipe de 3 ou 4 personnes.

1 Question 1

Soit $\Pi_{OTP} = (Gen, E, D)$, le schéma de chiffrement "one-time-pad" pour messages de longueur n bits. Écrivez le code pour les trois algorithmes Gen, E et D en langague C. Vos codes doivent fonctionner pour tout n entre 1 et 64. Fournissez le texte de ce code source avec la remise de votre devoir, comme texte dans le corps de votre devoir.

Dans votre une personne jouera Alice, une jouera Bob, et une/deux Eve dans ce qui suit.

1.1 Question 1.1

Pour la suite du numéro, nous travaillerons avec n=16.

Alice et Bob génèrent et partagent secrètement une clé k.

Pour un message m de son choix, Alice génère le cryptogramme $c = E(k, m)$, et envoie c à Bob en passant par Eve (qui ne modifie pas le cryptogramme c). Bob déchiffre c pour obtenir le message m. Laissez les traces de votre exécution: quelles informations sont vues par chaque participant.e.

Si Eve, n'a aucune information sur m et k avant de voir c, est-ce qu'elle en apprend en voyant seulement c ?

Si maintenant Eve apprend une telle paire (m, c), est-ce qu'elle apprend beaucoup d'information sur k ? De combien de telles paires aurait-elle besoin pour apprendre k ?

1.2 Question 1.2

Associez chacun des 16 bits du message à une question vrai-faux de votre choix. Est-il possible pour Eve de modifier c en c' tel que la réponse à la première question lorsque Bob décrypte c' est le contraire de ce que Alice avait répondu ? Comment ?

2 Question 2

Nous voulons qu'Alice et Bob puissent communiquer de façon sécurisé, disons Alice veut envoyer un message m à Bob de sorte à ce que la transmission de m soit faite de manière confidentielle, intègre et authentifié. Ils communiquent sur un réseau non-sécurisé, et donc, en particulier, il est possible qu'un adversaire puisse:

- lire toutes les communications transmises,
- modifier les communications,
- tenter de se faire passer pour Alice.

Ils veulent utiliser les systèmes cryptographiques suivants:

- $\Pi_{CPriv} = (Gen_{CPriv}, E_{CPriv}, D_{CPriv})$, un système de chiffrement à clés privées sécuritaire,
- $\Pi_{MAC} = (Gen_{MAC}, MAC, Verif_{MAC})$, un système d'authentification à clés privées sécuritaire,

2.1 Question 2.1

Vous pouvez supposer qu'Alice et Bob partagent une clé privée k qui est secrète, intègre et authentifié. Si vous désirer faire des suppositions sur k, prière de les noter ici. Donner le pseudo-code d'un protocole qui permet à Alice d'envoyer le message m à Bob avec les propriétés suivantes:

- robuste: si les messages transmis de Alice vers Bob et de Bob vers Alice ne sont pas modifiés lors de leur transmission, Alice et Bob n'abandonnent pas le protocole et Bob produit bien le message m qu'Alice lui envoyait en sortie de protocole,
- confidentialité: seulement Alice et Bob peuvent calculer de l'information sur m à la fin du protocole,
- intègre: si Alice et Bob n'abandonnent pas le protocole, Bob produit bien le message m d'Alice en sortie,
- authentifié: Bob peut être certain que m provient bien d'Alice.

Argumenter pourquoi votre protocole satisfait ces propriétés.

2.2 Question 2.2

Quelle entrée est-ce que l'algorithme Gen_{CPriv} prend ?
Et quelle est la sortie de cet algorithme ?
Roule-t-il en temps polynomial ? Pourquoi ?
Est-ce que cet algorithme pourrait être déterministe ? Pourquoi ?