ISEC - Partie 1, Session 2
2020-2021

Énoncé

Numéro d'anonymat :

Durée : 2 heures

Notes manuscrites et documents de cours autorisés

Une rédaction claire et concise sera appréciée. Toute affirmation devra être justifiée.
Une question non résolue n'empêche pas de faire les suivantes
(dans ce cas indiquez clairement que vous admettez le(s) résultat(s) de la question non faite).

Exercice 1 : Masque jetable et variantes

Alice et Bob partagent une clé binaire aléatoire uniforme de 128 bits. Ils peuvent donc utiliser le chiffrement par masque jetable (ou chiffrement de Vernam) pour qu'Alice envoie un message de 128 bits à Bob avec une confidentialité parfaite.

1.a] Est-ce qu'Alice peut utiliser cette clé pour chiffrer un message de longueur quelconque inférieure ou égale à 128 bits ? Justifier votre réponse.

1.b] Alice souhaite envoyer un message de 256 bits à Bob ; elle veut utiliser le chiffrement par masque jetable en mode CBC pour chiffrer deux blocs de 128 bits. Décrire en détail les opérations de chiffrement et de déchiffrement.

1.c] Est-ce que le chiffrement assure la propriété de sécurité sémantique ? Justifier votre réponse.

Exercice 2 : Chiffrement authentifié

Alice et Bob partagent une clef secrète k de 128 bits et s'échangent des messages chiffrés avec un mécanisme de chiffrement E supposé sûr (comme l'AES par exemple).

Pour garantir la confidentialité et l'authenticité des messages, ils utilisent aussi une fonction de hachage cryptographique H. Pour transmettre le message m, Alice calcule : $c = E(k, m)$ et $h = H(c)$, puis envoie (c, h) sur le canal de communication. Lorsqu'il reçoit le chiffré, Bob vérifie que $H(c) = h$; si c'est le cas, il déchiffre c grâce à k pour retrouver m et sinon il considère que le chiffré est invalide.

2.a] Expliquer comment un adversaire actif peut altérer le contenu des messages transmis sans être détecté.

2.b] Proposer une méthode pour l'en empêcher et justifier sa sécurité.

Exercice 3 :

Une entreprise décide d'utiliser la cryptographie à clé publique pour garantir la confidentialité de ses communications et souhaite utiliser le système RSA. Comme la génération des clés est coûteuse, elle décide de générer pour chaque employé i une clé publique $N_i = p \cdot q_i$ où p est un nombre premier fixe et q_i est un nombre premier différent pour chaque utilisateur.

3.a] Montrer qu'un attaquant extérieur à l'entreprise (et ne disposant que de peu de moyens de calcul) peut casser la confidentialité de toutes les communications s'il dispose de deux clés publiques d'employés différents.