MP2 - Cryptographie et applications

1er Decembre 2015 - 1h30 - une feuille manuscrite autorisée

Questions de cours:

a. Quels sont les avantages et inconvénients du chiffrement à flot par rapport au chiffrement par blocs. Donner des exemples d'algorithmes.

b. Expliquer pourquoi si on utilise du chiffrement à flot, réutiliser le même flot quasi-aléatoire sur différents message est une mauvause idée.

c. Est-ce que la factorisation est un problème difficile à résoudre ? Comparer ce problème à la résolution du problème du log discret sur un anneau de type Z/nZ ou sur des courbes elliptiques.

d. Comment doit-on procéder pour échanger de façon optimale en temps avec qqu'un une grande taille de données chiffrées, sans avoir de clé secrete partagé au préalable ?

e. Expliquer le principe de l'attaque par le paradoxe des anniversaires pour les fonctions de hachage. Quelle taille de sortie protège de cette attaque à priori.

f. Les documents qui sont signés chez un notaire doivent être conservés 99 ans, décrivez de manière sommaire une manière pour arriver à garder la validité d'une signature pour une période de 99 ans (sans prendre une seule clé trs importante). Quels sont les problèmes auxquels vous pensez pour votre proposition ?

Exercice 1 (Partage de secret):

a. On suppose qu'Alice partage une clé de chiffrement par bloc K_{AB} avec Bob et une clé K_{AC} avec Charlie. Donner une méthode pour qu'Alice chiffre un message de m blocs qui ne soit déchiffrable que par une coopération entre Bob et Charlie. On peut supposer que Bob et Charlie partage un canal secret pour leur communication. Le chiffré devra être de taille fixe, plus grand que m blocs et Alice ne devra chiffrer les m blocs qu'une seule fois.

b. On suppose maintenant que Alice partage une clé de chiffrement par bloc avec Bob (K_{AB}), Charlie (K_{AC}) et David (K_{AD}). Donner une méthode de chiffrement de telle sorte qu'Alice envoie un message de m blocs chiffrés par une seule clé mais que pour déchiffrer le message il y a besoin qu'au moins deux personnes parmi Bob,Charlie et David coopérent pour déchiffer le message. (Indice: il faut ajouter simplement trois blocs chiffrés bien choisis aux m blocs chiffrés).

c. Donner une idée de la méthode pour généraliser cette idée au cas de n personnes dont tout sous groupe de k personnes puissent dechiffrer le message.

Exercice 2 (Cryptographie à clé symétrique):

a. Rappeler le principe du schéma de Feistel. Quel est l'autre type de schéma utilisé, notamment pour l'AES.

b. Montrer que si on remplace les boites-S du DES par la fonction identité (ie une fonction qui à toute entrée de 6 bits renvoie les 4 bits de poids faibles) alors on peut facilement casser le système avec quelques couples de clairs/chiffrés. D'une façon générale pourquoi dit-on que la sécurité du DES repose sur les boites-S ?

c. Citer une famille de boites-S qui peut être cassée très facilement.

d. Pourquoi est-ce que l'AES est un algorithme rapide par rapport à des algorithme de la génération du DES ?

e. Pourquoi ne peut-on pas utiliser deux fois de suite le DES en chiffrement pour doubler la longueur de la clé ? Rappeler le principe de l'attaque.

Exercice 3 (Cryptographie à clé publique):

a. Rappeler le schéma d'échange de clés de Diffie-Hellman

b. A quel type d'attaque ce schéma est-il vulnérable, rappeler le principe de cette attaque.

c. On souhaite se protéger de cette attaque. On suppose que A et B possède des couples de clé publique/clé privée de type RSA (et qu'ils connaissent leur clés publiques respectives), proposer une variation sur le schéma de Diffie-Hellman en utilisant la signature RSA qui permet de contrer l'attaque de la question précédente (le justifier).

d. On suppose maintenant que A et B ont en commun un mot de passe avec suffisamment d'entropie et une fonction de chiffrement symétrique. Proposer alors une variante de Diffie-Hellman, qui permet aussi de se protéger contre l'attaque du b.

Exercice 4 (Problème du chevalier et de la princesse)

Une princesse veut faire passer un message secret à un chevalier. Elle peut naturellement échanger des objets et des documents avec le chevalier par l'intermediaire des gardes mais souhaite que les gardes ne puissent pas avoir accés au message. La princesse et le chevalier disposent séparément de cadenas avec des clés, et la princesse dispose d'un coffre qui peut être fermé avec plusieurs cadenas à la fois. Comment doivent-ils s'y prendre ?

Exercice 5 (LFSR):

On intercepte un message chiffré avec un système de chiffrement à flot produit par une suite chiffrante récurrente de type LFSR.

Le message binaire intercepté est: 0000011011110010

On sait d'autrepart que les six premiers bits du message clair sont 110101. On admet que la complexité linéaire de la suite chiffrante du LFSR est au plus 3.

Déchiffrer le message en entier.

Exercice 6 (Cryptographie à clé publique):

a. On suppose que A et B utilise le même module RSA n avec deux clés publiques e_A et e_B premières entre elles. On suppose que C envoie le même message chiffré m^{e_A} et m^{e_B} à A et B. Montrer que E qui écoute les communications peut retrouver facilement alors le message m.

b. AFin d'améliorer la sécurité des messages Bob choisit deux exposants e_1 et e_2 et demande à ALice de chiffrer d'abord son message par e_1, pour obtenir $c_1 = m^{e_1}$ puis de rechiffrer par e_2 pour obtenir $c_2 = c_1^{e_2}$. Et d'envoyer c_2. Est-ce que ce double chiffrement améliore la sécurité. Si oui pourquoi, si non pourquoi.