M2 - Cryptographie et applications

17 février 2020 - deux feuilles manuscrites autorisées

Questions de cours:

a. Qu'est-ce qu'un certificat, rappeller son utilisation.

b. Qu'est-ce qu'une chaine de certificats ? Dans quel cas l'utilise-t-on ?

c. Qu'est-ce qu'un tiers de confiance, donner des exemples de telles entités.

d. Est-ce que le chiffrement permet de faire: de la signature ? de l'échange de clés ? de l'authentification ? Si oui comment ?

e. A quoi sert un schéma de Retrait d'Information Privé (PIR en anglais) ? Donner des exemples d'applications.

f. Donner des applications spcifiques des algorithmes de couplages sur les courbes elliptiques.

Exercice 1 (Authentification):

On considère le protocole de Schnorr. Soit p et q deux entiers (grands) tels que q divise $p-1$, et soit g un entier d'ordre q modulo p. Le secret détenu par Alice est un entier $a \in [0, q-1]$ et la donnée de $A = g^{-a} mod\, p$ est rendue publique. Le protocole est alors le suivant: (1) Alice fournit un engagement aléatoire k dans l'intervalle $[0, q-1]$ et calcule $K = g^k mod\, p$. Elle transmet K à Bob. (2) Bob choisit un défi r au hasard dans $[0, q-1]$ et le transmet à Alice. (3) Alice calcule la réponse $y = (k + ar) mod\, q$ et la transmet à Bob. Bob vérifie que $g^y A^r = K mod\, p$.

a. Faire un schéma de ce protocole

b. Montrer que le protocole fonctionne (en ce sens que si on connait le secret on répond convenablement quoiqu'il arrive).

c. Donner un exemple ou en anticipant un défi un tricheur peut se faire passer pour Alice avec une probabilité $1/q$. En déduire que la probabilité de tricher est supérieure à $1/q$. (On admet par la suite que cette probabilité est exactement $1/q$).

d. Quel est l'intérêt de ce protocole par rapport au protocole de Fiat-Shamir (en terme de nombre de passes).

e. Ce protocole vérifie-t-il la propriété de zero-knowledge ?

Exercice 2 (Partage de secret) :

On rappelle qu'un schéma de partage de secret permet à plusieurs personnes qui ont en commun un (ou des) bout de secret de retrouver un secret donné.

a. Quel est la différence entre le partage de secret et l'échange de clé ? Donner un exemple d'application du partage de secret.

b. Rappeler le schéma de partage de secret de Shamir.
c. On suppose qu'un état major (composé de 2 généraux, de 4 colonels et de 16 capitaines) a la possibilité de faire tirer un missile ultra-destructeur, le code du missile est un secret partagé, qui ne peut être activé que dans certains cas: 1-les généraux le souhaitent, 2-les deux colonels le souhaitent et un seul general, 3- les 16 capitaines le souhaitent, 4- 1 general et 8 capitaines le souhaitent. Proposer une solution en utilisant le schéma de partage de secret de Shamir qui permet de résoudre ce problème.
2)Dans votre solution, combien faudrait-il de colonels avec 12 capitaines pour retrouver le secret ?
3) Avec ce type d'approche, on aura toujours le cas ou un grand nombre de capitaine pourra toujours trouver le secret, comment pourrait-on faire pour que quoiqu'il arrive il y ait au moins un general qui collabore pour retrouver le secret ?

Exercice 3 (Courbes elliptiques)

a. Quel est l'intérêt des courbes elliptiques en cryptographie ? Rappeler par un schéma le fonctionnement de l'addition et du doublement pour le groupe des points de la courbe.
On consière la courbe définie sur le corps à 5 éléments $K = Z/5Z$ par $y^2 = x^3 + x + 2$.
b. Combien y a-t-il de points sur la courbe et quels sont-ils ?
c. Pour tous les points P de la courbe calculer 2P et 4P.
d. Donner un générateur du groupe (un point P, tel que 0P,P,2P,etc.. engendre le groupe). En déduire la structure du groupe de la courbe.

N.B. On rappelle que dans ce cas, si la courbe a pour équation $y^2 = x^3 + ax + b$, le doublement de $P(x_1, x_2)$ est $2P(x_3, y_3)$ avec:

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$$

$$y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1.$$

Exercice 4 (Fonction de hachage et signature) :

Soit h une fonction de hachage à valeur dans F_2^n. On considère le cas d'un attaquant qui pour abuser une signature souhaite construire deux messages ayant le même haché mais avec deux significations **choisies** différentes.

a. Donner une attaque en $O(2^{n/2})$ pour la fonction de hachage h qui permet de construire deux messages avec deux significations choisies différentes mais avec le même haché.

b. Montrer comment l'attaque du a. peut être utilisée pour abuser un verificateur de signature (exemple: "faites un virement de 100 euros", au lieu de "faites un virement de 10000 euros").

c. Comment choisir n pour resister à cette attaque.

Exercice 5 (Un échange de clé léger.... trop léger) :

Un protocole d'échange de clés pour les téléphones portables a été proposé par Park, basé sur DH. Le système a un module premier p et un générateur commun aux deux partis. Chauqe parti i a une clé secrete x_i et une clé publique $X_i = g^{x_i} \pmod p$. Pour faire une clé de session entre le client M et la base B, on execute le protocole suivant:

$$1.B \to M : g^{x_B + N_B}$$

$$2.M \to B : N_M + x_M$$

ou N_B et N_M sont des entiers random (nonces utilisés une seule fois).
B calcule ensuite sa clé de session comme:

$$K_{MB} = (g^{x_M + N_M} X_M^{-1})^{N_B}$$

et M calcule sa clé comme:

$$K_{MB} = (g^{x_B + N_B} X_B^{-1})^{N_M}$$

Ils finissent le protocole en faisant un defi/réponse utilisant K_{MB}.
1) Montrer que le protocole fonctionne et que c'est bien la même clé commune qui est calculée. Pourquoi ce protocole est-il potentiellement plus intéressant qu'un DH classique pour le telephone mobile ?

2) Montrer que si un attaquant connait une clé de session d'un tour précédent (il connait une clé commune K_{MB}) pour lesquels il a enregistré des messages, alors il peut se faire passer pour B (indication: l'attaquant peut rejouer des messages de la session précédente).

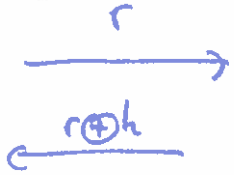
3) Montrer qu'en fait un attaquant peut se faire passer pour B connaissant simplement les clés publiques X_B et X_M. Qu'en concluez vous pour le protocole ?

Exercice 6 (Authentification)

ALice et Bob partagent un secret k et on décidé de l'utiliser dansle protocole suivant qui permet à Alice d'authentifier Bob.

1. Alice choisit une suite de bits aléatoire r et l'envoie en tant que défi á Bob. 2. Bob repond en renvoyant $r \oplus k$.

L'analyse de Bob et Alice du protocole est celle-ci: le protocole permet d'obtenir l'authentification puisque Alice peut vérifier que l'envoyeur du message 2. connait le secret partagé k. Il est aussi sécurisé car seul des suites de bits aléactoires sont envoyées sur le canal de communication.



a) Comment est-ce qu'Alice verifie que l'envoyeur du message 2. connait k ?
b) Etes-vous d'accord avec Bob et Alice sur la Sécurité du protocole ? Justifiez.

Exercice 7 (Chiffrement):

Etant donnés deux protocoles pour lesquels l'envoyeur procède de la manière suivante:

Protocole A:

$$y = e_{k_1}(x||H(k_2||x)),$$

où x est le message, H est une fonction de hachage comme SHA-1, e est un algorithme de chiffrement à clé symétrique, "||" est la concaténation, et k_1 et k_2 des clés secrètes connues seulement de l'emetteur et du receveur.

Protocole B:

$$y = e_{k_1}(x||sig_{k_{pr}}(H(x))),$$

où k est une clé partagée et k_{pr} est la clé privé de l'emetteur.

a) Donner une description étape par étape, de ce que le receveur doit faire en recevant y pour retrouver le message.

b) Préciser en les justifiant si les propriétés suivantes sont vérifiées pour chacun des protocoles:
confidentialité, intégrité , non répudiation.