M2 - Cryptographie et applications

12 février 2015 - une feuille manuscrite autorisée

Questions de cours:

a. Quel est l'interet des courbes elliptiques par rapport a un algo de type RSA ?

b. Qu'est-ce qu'un certificat ? Dans quel cas l'utilise-t-on ?

c. Quel est la difference entre anonymat et protection de la vie privée, donner des exemples de protocoles de protection de la vie privée.

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

e. Qu'est-ce qu'un protocole PIR (Private Information Retrieval) ?

f. Expliquer le type de procédure à mettre en place pour qu'une signature signée aujourd'hui soit encore valide dans 99 ans ?

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 d'un général, de deux colonels et de 5 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-le général le souhaite, 2-les deux colonels le souhaitent, 3- les 5 capitaines le souhaitent, 4- 1 colonel et 3 capitaines le souhaitent. Proposer une solution en utilisant le schéma de partage de secret de Shamir qui permet de résoudre ce problème.

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. Quelle est la structure du groupe de la courbe elliptique ?
d. Y a-t-il un élément générateur ?, si oui en donner un.

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 (Avant la clé publique)

James H. Ellis (1924-1997) etait un ingenieur et un mathematicien travaillant au GCHQ (Government Communications HeadQuarters), les grandes oreilles britanniques.

Il raconte, dans une note publiee juste aprs son deces (The Story of Non-Secret Encryption, http://www.cesg.gov.uk/ellisdox.ps), comment il a eu des 1970 lidee du principe de la communication a cles publiques et comment deux de ses collegues, C. Cocks et M. Williamson, lont mise en uvre en dcouvrant les mecanismes du cryptage RSA et du schma de Diffie-Hellman plusieurs annees avant leurs auteurs.

Il decrit en particulier un schema de communication ou S (l'emetteur) desire faire passer un message M a R (le destinataire) :

"In terms of modular arithmetic the scheme was for S and R each to choose a large number, x and y respectively. (...) S sends M^x and R returns $(M^x)^y =$