Principe et Algorithme Cryptographiques : DS n°2

première session

Université de Lille-1
FIL — PAC

22 mai 2015

Ce sujet est composé de 3 pages. Tous les documents sont autorisés. Vos réponses doivent **absolument** être justifiées.

1 Cartes bleues

Une norme internationale nommée EMV spécifie le fonctionnement de la cryptographie dans les cartes bancaires contenant un microprocesseur (les plus répandues en Europe). On va admettre que ce microprocesseur contient une mémoire qui n'est pas facilement accessible, et qui permet donc de stocker des données secrètes. La carte bleue contient aussi des données non-secrètes, qui ont vocation à être communiquées au terminal de paiement : le numéro du compte bancaire à débiter, par exemple, ainsi que des clefs publiques et des certificats. Le système RSA est utilisé en toute circonstance.

L'usage de la cryptographie vise principalement à empêcher la fraude, par les clients (qui possède une carte bleue) ou par les marchands (qui possèdent un terminal de paiement). Dans ce système, chaque banque possède une ou des clef publiques. Une autorité de certification spécifique au système EMV fournit aux banques des certificats. Les marchands possèdent la clef publique de cette autorité.

On va supposer que des fraudeurs peuvent espionner les communications entre la carte et le terminal de paiement.

La norme prévoit deux niveau d'identification de la carte par le terminal.

Identification « statique ». Elle offre le niveau de sécurité le plus faible. La carte contient seulement une signature des données spécifiques à la carte (le numéro du compte, etc.) par la banque, ainsi que le certificat de la banque.

▷ **Question 1 :** Que doit vérifier le terminal ? Que doit-il contenir à l'avance pour cela ?

▷ **Question 2 :** Quelle manoeuvre de fraude est rendue impossible par cette vérification ?

▷ **Question 3 :** Quelle autre manoeuvre de fraude *n'*est *pas* rendue impossible par cette vérification ?

Identification « dynamique ». Elle offre un niveau de sécurité plus élevé. La carte contient ainsi des données bancaires, ainsi qu'une paire de clefs RSA. Pour authentifier la carte, le terminal lui envoie des données (le numéro de compte du marchand, la date, ainsi qu'un nombre aléatoire imprévisible), et la carte en renvoie une signature.

▷ **Question 4 :** Une partie des données présentes sur la carte doit toujours être signée par la banque. Lesquelles ?

▷ **Question 5 :** Que doit récupérer le terminal sur la carte ? Que doit-il vérifier ?

▷ **Question 6 :** Pourquoi cette méthode améliore-t-elle la sécurité par rapport à la précédente ?

Transaction. Une fois que la transaction a lieu (par exemple, l'utilisateur tape son code PIN pour l'approuver), la carte génère un Certificat de Transaction (CT) et le transmet au terminal. Celui-ci l'envoie à la banque pour obtenir le paiement.

Le Certificat de Transaction est constitué de la description de l'opération (numéros des comptes de départ et d'arrivée, montant, unité monétaire, *numéro de la transaction réalisé par la carte*, etc.) ainsi que d'un MAC de ces données. L'CBC-MAC est utilisé, dans lequel l'AES fait office de système de chiffrement par bloc. La clef qui sert à calculer ce MAC est stockée dans la mémoire secrète de la carte.

▷ **Question 7 :** Quelle fraude pourrait avoir lieu si le MAC n'était pas présent ?

▷ **Question 8 :** Quelle fraude pourrait avoir lieu si le numéro de la transaction en cours n'était pas inclu dans les données MACées ?

Dérivation de clef. La norme recommande que la clef de MAC de chaque carte soit obtenue en chiffrant le numéro de la carte par une clef « maitresse » détenue par la banque.

▷ **Question 9 :** Quel est l'intérêt de cette pratique (pour les banques) ?

▷ **Question 10 :** Pourquoi faut-il évidemment stocker la clef *dérivée* sur chaque carte, et pas la clef maitresse ?

2 Alice et Bob sont accusés de terrorisme

Alice, Bob, Charlie et Dorothée utilisent un échange de clef Diffie-Hellman *statique* pour communiquer entre eux. Ceci signifie que chacun possède une clef secrète (x_a pour Alice, x_b pour Bob, etc.). À chacune de ces clefs secrète correspond une clef publique $pk_a = g^{x_a} \bmod p$, etc. On précise qu'ils se sont mis d'accord, il y a longtemps, sur un grand nombre premier p et un « générateur » g de $\mathbb{Z}_p$ qui est d'ordre q (un nombre premier très grand).

Pour communiquer entre eux, Alice et Bob utilisent la méthode de Diffie-Hellman pour obtenir une clef partagée entre eux deux seulement : $s_{ab} = g^{x_a x_b} \bmod p$. Concrètement, nos amis utilisent ensuite l'AES en mode CBC pour chiffrer leurs échanges.

▷ **Question 11 :** Comment tirer une clef AES de s_{ab} ?

L'Etat intercepte tous les échanges chiffrés et possède les clefs publiques de tout le monde. La police accuse (à tort) Alice et Bob de participer à un complot terroriste. Trainés au tribunal, Alice et Bob sont sommés de révèler leurs clefs secrètes x_a et x_b pour que leurs conversations soient rélévées.

Alice et Bob refusent de révéler x_a et x_b, mais acceptent de révéler s_{ab}, au nom du droit à la vie privée de Charlie et Dorothée.

▷ **Question 12 :** Justifiez leur décision.

Alice et Bob, assez énervés par les tracas qu'ils subissent, décident de jouer aux plus malins : au lieu de transmettre s_{ab} au juge, ils lui donnent une valeur pseudo-aléatoire s_{bidon} qui est différente de s_{ab}. Le juge essaye de déchiffrer leurs échanges chiffrés avec s_{bidon}, et obtient du charabia incompréhensible. Alice et Bob tentent de se justifier en prétendant que depuis le début ils s'envoie des messages pseudo-aléatoires chiffrés, juste pour pour embêter les dispositifs d'espionnage de masse de la population.

Le juge se rend compte qu'il ne possède pas de moyen infaillible de démontrer qu'Alice et Bob lui mentent.

▷ **Question 13 :** Pourquoi ?

Le greffier propose alors le protocole suivant, pour établir l'éventuelle mauvaise fois d'Alice et Bob. Il s'agit d'un protocole qui sert à tester si un nombre s est bien égal à $g^{x_a x_b} \bmod p$, mais sans révéler ni x_a ni x_b.

1. Alice et Bob choisissent au hasard un nombre $u \in \mathbb{Z}_p$.
2. Ils calculent $\alpha \leftarrow g^u \bmod p$ et $\beta \leftarrow {pk_b}^u \bmod p$ puis envoient le tout au juge.
3. Le juge choisit au hasard un nombre $d \in \mathbb{Z}_p$ (le « défi ») et l'envoie aux suspects.
4. Alice calcule $r = u + dx_a \bmod q$ (la « réponse ») et l'envoie au juge.
5. Le juge vérifie que :
$$\begin{cases} g^r & \equiv \alpha \cdot {pk_a}^d & \bmod p \\ {pk_b}^r & \equiv \beta \cdot s^d & \bmod p \end{cases}$$
Si ce n'est pas le cas, c'est qu'Alice et Bob ont triché pendant l'exécution du protocole, ou bien que s n'est pas leur clef partagée.

Alice et Bob sont honnêtes

Dans ce cas-là, la valeur de s que le juge possède est bien $s = s_{ab}$, c'est-à-dire $s \equiv g^{x_a x_b} \bmod p$.

▷ **Question 14 :** Justifiez que le juge va toujours exécuter le protocole de manière satisfaisante.

▷ **Question 15 :** Expliquez pourquoi le juge n'apprend pas les clefs secrètes x_a et x_b.

Alice et Bob trichent

Note : *les 4 questions suivantes sont un peu plus mathématiques, mais vous êtes largement guidés...*

Dans ce cas-là, la valeur s que le juge possède n'est pas s_{ab}. On écrit donc $s = g^z \bmod p$ (avec $z \not\equiv x_a x_b \bmod q$).

On va voir que quoi que fassent Alice et Bob, le protocole échoue avec très forte probabilité. Alice et bob peuvent faire n'importe quoi, y compris calculer α, β et r autrement que ce qui est prévu. On supposer qu'ils renvoient $\alpha = g^{u_1} \bmod p$ et $\beta = g^{u_2} \bmod p$.

▷ **Question 16 :** Quelle est la valeur « normale » de u_2 qui devrait se présenter si Alice et Bob respectaient le protocole ?

▷ **Question 17 :** Le juge effectue d'abord la première des deux vérifications. Montrez que si cette première congruence est vraie, alors on a : $r \equiv u_1 + dx_a \mod q$.

▷ **Question 18 :** Le juge effectue ensuite la deuxième vérification. Montrez que si la deuxième congruence est vraie, alors on a : $u_1 x_b - u_2 \equiv d(z - x_a x_b) \mod q$.

▷ **Question 19 :** On rappelle qu'Alice et Bob doivent choisir u_1 et u_2 *avant* de connaître le défi d. Montrez qu'ils n'ont quasiment aucune chance de s'en sortir.

Le juge a autre chose à faire

Comme il ne veut pas avoir à s'occuper de cette affaire manifestement boiteuse, le juge propose la modification suivante du protocole : au lieu qu'il fournisse un défi aléatoire, Alice et Bob calculent de leur côté $d = H(pk_a \parallel pk_b \parallel s \parallel \alpha \parallel \beta)$. Du coup, il suffit qu'ils fassent les calculs dans leur coin, et le juge n'a plus qu'à vérifier la « preuve ».

▷ **Question 20 :** Est-ce raisonnable ?