DS du 27 mai 2011

Durée 3h - documents de cours et calculatrices autorisés

Ce sujet comprends 4 exercices indépendants.

Exercice 1. *Protocole de Diffie-Hellman*

Dans cet exercice calculatoire, vous détaillerez les calculs.

Question 1. Dans le corps premier $\mathbb{F}_{193}$, lequel des deux nombres 2 ou 5 engendre le groupe multiplicatif ?

Question 2. Alice et Bob utilisent le protocole de Diffie Hellman pour établir une valeur secrète commune. Quelle est cette valeur commune si la valeur aléatoire choisie par Alice est $x_A = 3$ et celle de Bob $x_B = 5$?

Exercice 2. *A2U2*

À la conférence sur les RFID (Radio Frequency IDentification) organisée en avril dernier par IEEE, un système de chiffrement à flot nommé A2U2 a été présenté par M. David, D.C. Ranasinghe et T. Larsen.

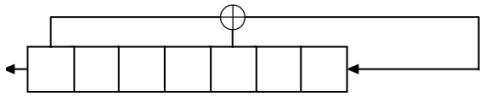

FIGURE 1 – Le chiffrement à flot A2U2

Ce système est construit autour de trois registres à décalage dont l'un est à rétroaction linéaire. Ce LFSR est celui de la figure 1. C'est sur ce LFSR que porte cet exercice.

Question 1. Donnez le polynôme de rétroaction de ce LFSR. Ce polynôme est-il irréductible ? primitif ?

Question 2. Quelle est la période de la suite binaire produite par un tel LFSR lorsqu'il est initialisé avec un état non nul ?

Question 3. Quelle est la longueur de la plus grande plage de bits nuls consécutifs dans une période de la suite chiffrante obtenue depuis un état initial non nul ?

Question 4. Donnez plusieurs arguments pour lesquels n'utiliser que ce seul LFSR pour produire une suite chiffrante n'assurerait aucune sécurité pour la confidentialité. En particulier, distinguez le cas où le LFSR est connu du cas contraire.

Exercice 3. *Protection des données sur la console de jeux WII*

La WII est une console de jeux. Les sauvegardes de jeux sur des cartes mémoires SD sont protégées. Voici ce qu'on peut lire sur un site consacré à cette console de jeux (`http://wiibrew.org/wiki/Wii_Security`)[1] :

> When you copy a savegame from your Wii system memory to an SD card (in "Data Management"), it encrypts it with an AES key known to all consoles (SD-key). This serves only to keep prying eyes from reading a savegame file. In crypto terminology, the SD-key is a "shared secret".
>
> Your Wii then signs the file on the SD card with its private (RSA) key. This is to prevent anyone from modifying the save file while it is on the SD card.
>
> If I then give you a copy of my savefile, your Wii can decrypt it because it knows the SD-key. However, it has no way of checking your Wii's signature, because it doesn't know my console's public key. To solve this problem, the savegame also contains a copy of my Wii's public key – the one that matches the private key it used to sign the savefile. (This copy of my Wii's public key is called a 'certificate'.)
>
> Now your Wii can verify that my Wii signed the file, but it has no way of knowing whether it was really a real Wii that signed it, or if I just made up a new random RSA key to try to fool it. To solve this problem, the certificate stored inside of the savegame is then signed with Nintendo's private key. All Wiis have Nintendo's public key stored in their firmware; your Wii can use that key to verify the signature on the certificate. If the certificate is valid, it can verify the signature on the savegame against my Wii's signature.

1. à une petite adaptation près pour le sujet de cette épreuve.

> We solved the chicken-and-egg problem with our original memory-dumping hack. We extracted a private RSA key from one console. Since any Wii can read any savefile, we only need to have one key – it doesn't need to be re-encrypted / re-signed every time.

Question 1. Les sauvegardes sur carte SD sont-elles chiffrées ? Si oui décrivez le plus précisément possible le système utilisé, et indiquez la clé utilisée.

Question 2. Les sauvegardes sont signées. Indiquez comment.

Question 3. Comment une autre console Wii peut-elle déchiffrer une sauvegarde ?

Question 4. Comment peut-elle vérifier la signature ? En particulier quel élément supplémentaire faut-il introduire ?

Question 5. De quelle façon des utilisateurs malicieux peuvent-ils fabriquer les données de leur choix, non nécessairement obtenues par une Wii, de sorte qu'elles soient acceptées par n'importe quelle Wii ?

Exercice 4. *Sécurité du WEP*

Le but de cet exercice est d'étudier quelques failles de sécurité dans le protocole WEP (Wired Equivalent Privacy) utilisé dans les réseaux 802.11 afin de protéger les données transmises dans les communications sans fil. WEP s'appuie sur une clé secrète de 40 bits partagées par les deux parties communicantes. Quand un utilisateur A veut transmettre un message M à B, il procède en suivant les trois étapes suivantes.

1. **Codage CRC :** étant donné un message M de n bits (n étant un entier fixé), A calcule un code de parité sur 32 bits $L(M)$, L étant une fonction linéaire qui ne dépend pas de la clé K (on rappelle que L est linéaire si pour tout message X et Y, on a $L(X \oplus Y) = L(X) \oplus L(Y)$). Le texte clair est alors un message de $n + 32$ bits $P = M||L(M)$ (où $||$ désigne la concaténation).
2. **Chiffrement :** A chiffre P avec le système de chiffrement RC4 en utilisant la clé K et un vecteur d'initialisation IV de 24 bits choisi pour le chiffrement de M. Le chiffré est alors $C = P \oplus RC4(IV, K)$.
3. **Transmission :** A envoie (IV, C) par ondes radio à B.

Question 1. Il a été parfois annoncé que le WEP offre une sécurité de $24 + 40 = 64$ bits. Qu'en pensez-vous ?

Question 2. Expliquez comment B retrouve le message M après avoir reçu (IV, C). Précisez en particulier le rôle du codage CRC.

Question 3. Dans certaines implantations, les 24 bits du vecteur d'initialisation sont choisis au hasard pour chaque message. Montrez qu'en collectionnant un nombre « raisonnable » de messages chiffrés échangés entre A et B, un attaquant peut gagner de l'information (par exemple le ou-exclusif entre deux messages clairs) sur certains messages clairs. Donnez des estimations du facteur de travail pour que l'attaquant réussisse sa tentative avec une probabilité de $0,9$. Que suggérez-vous pour une implantation ne souffrant pas de cette faille ?

Question 4. On examine dans cette question une autre faille de sécurité du WEP. Supposons qu'un adversaire intercepte un message chiffré (IV, C). Montrez comment il peut *facilement* construire un faux message chiffré valide (IV, C') sans même connaître la clé secrète K. Combien de tels faux chiffrés valides peut-il ainsi réaliser ?