Master 2ème année – SeCReTS

Examen "Sécurité des systèmes radiomobiles et protection des contenus"

Partie 2 : sécurité téléphonie mobile ; sécurité diffusion de contenus multimédia

9 mars 2021

Durée : 1h – Documents interdits, sauf une feuille A4 recto écrite de votre main. Aucun accès à un téléphone portable, une calculatrice, un PDA ou tout autre dispositif électronique, connectable ou non.

Exercice 1 [Téléphonie mobile]

1. Parmi les cinq mécanismes de sécurité suivants, lesquels sont mis en œuvre dans le système GSM ?
   - Authentification de l'abonné par le réseau
   - Authentification du réseau par la carte d'abonné
   - Intégrité du trafic
   - Confidentialité du trafic
   - Confidentialité de l'identité de l'abonné (anonymat)
2. Quelle sont (en bits) la taille de clé et la taille des entrées/sorties des algorithmes A3 et A8 utilisés dans le système GSM ?
3. Pour quelle raison, dans le système GSM, les algorithmes de chiffrement (A5) doivent-ils impérativement être normalisés alors que les algorithmes d'authentification et d'établissement de clé (A3/A8) ne le sont pas ? Rappeler dans la réponse dans quels équipements ces algorithmes sont implantés.
4. Quel est le nom de l'algorithme utilisé dans les fonctions de chiffrement (f8) et d'intégrité (f9) de l'UMTS ?

Exercice 2 [Protocole EAP-SIM]

Dans le standard Wi-Fi, afin de mettre en place une authentification mutuelle entre un client et un serveur, le protocole suivant a été proposé, en s'appuyant sur les protocoles A3 et A8 du standard GSM. Le client (que l'on appellera C) et le serveur d'authentification (que l'on appelera A) connaissent tous deux une clé Ki (de 128 bits, analogue à la clé utilisée pour le GSM). Le protocole d'authentification mutuelle est alors le suivant :

- C envoie à A une valeur aléatoire R_c de 128 bits ;
- A renvoie alors à C trois valeurs aléatoires R_1, R_2, R_3 de 128 bits chacune, ainsi que $\mathrm{MAC}_{\mathcal{K}}(R_1, R_2, R_3, R_c)$, où la clé $\mathcal{K}$ (de 128 bits) est égale à $\mathrm{MD5}(K_{c1}||K_{c2}||K_{c3}||R_c)$, avec $K_{c1} = A8_{Ki}(R_1)$, $K_{c2} = A8_{Ki}(R_2)$ et $K_{c3} = A8_{Ki}(R_3)$;
- C renvoie finalement $\mathrm{MAC}_{\mathcal{K}}(SRES_1, SRES_2, SRES_3)$ à A, où $SRES_1 = A3_{Ki}(R_1)$, $SRES_2 = A3_{Ki}(R_2)$ et $SRES_3 = A3_{Ki}(R_3)$.

(on suppose que l'algorithme MAC utilisé ici a une taille de sortie de 128 bits)

1. Montrer qu'un faux serveur d'authentification (A') peut réussir à s'authentifier auprès de C, ceci avec une probabilité de succès de $1/2^{64}$.
2. Donner une modification du protocole permettant de limiter cette probabilité de fraude à $1/2^{128}$.

Exercice 3 [Schéma de *broadcast encryption* révocable]

Les studios de cinéma consacrent beaucoup d'efforts à la réalisation de films à succès, puis vendent les films (sur DVD) à des millions de clients qui les achètent pour les regarder chez eux. Afin d'éviter que le film soit soit redistribué en clair par des pirates, ils cherchent une solution où le film est gravé sous forme chiffrée sur le DVD, afin de pouvoir être lu uniquement sur les lecteurs de DVD autorisés.

1. Dans la solution CSS (*Content Scrambling System*), chaque fabricant agréé reçoit une clé k_d et il incorpore cette clé dans chaque lecteur qu'il vend. S'il y a cent fabricants agréés, alors il y a cent clés $k_d^{(1)}, \ldots, k_d^{(100)}$.

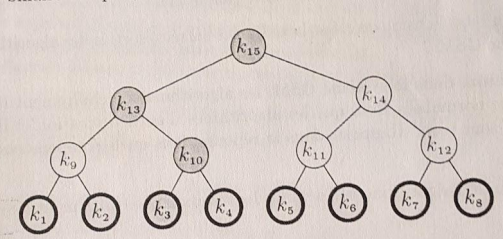
   Chaque DVD contient alors :

   - un en-tête $(c_1, c_2, \ldots, c_{100})$, avec $c_i = F_{k_d^{(i)}}(k)$ $(1 \leq i \leq 100)$, où k est une clé tirée aléatoirement, et F est un algorithme de chiffrement symétrique.
   - le film chiffré : $c = E_k(m)$, où m est le film en clair.

   (a) Expliquer comment chaque lecteur de DVD peut lire le film.

   (b) Donner des inconvénients de cette solution.

2. Une meilleure solution, AACS (*Advanced Access Content System*), propose de munir chaque lecteur de DVD de sa propre clé (qui est donc unique). Pour simplifier, on suppose ici que le nombre n de lecteurs est une puissance de 2. On considère que ces n lecteurs correspondent aux feuilles d'un arbre binaire complet, comme dans la figure ci-dessous (où $n = 8$).



   À chaque noeud de l'arbre est associé une clé générée aléatoirement. Dans le lecteur numéro i on place les clés qui sont sur le chemin allant de la feuille numéro i à la racine de l'arbre. Par exemple, le lecteur numéro 3 contient les clés k_3, k_{10}, k_{13} et k_{15}.

   (a) Quelle est (en fonction de n) la taille totale de la clé contenue dans chaque lecteur ?

   (b) Quel contenu suffit-il de mettre dans un DVD pour que tous les lecteurs autorisés $(1 \leq i \leq n)$ puissent reconstituer le film en clair ?

   (c) Supposons que $n = 8$ et que le lecteur numéro 3 soit compromis (par exemple son possesseur a pu accéder aux clés k_3, k_{10}, k_{13} et k_{15} qu'il contient et les a publiées). Comment peut-on produire de nouveaux DVD de telle sorte qu'ils puissent être lus sur tous les lecteurs **sauf** le lecteur numéro 3 (on dit ce cas qu'on a *révoqué* le lecteur numéro 3).

   (d) Plus généralement, expliquer comment on peut révoquer r lecteurs parmi n. Montrer que la taille de l'en-tête obtenue est $\mathcal{O}(r \cdot \log_2(n/r))$.