M1 informatique - UE réseau et sécurité

Année universitaire : 2018-2019

Consignes : documents interdits, calculatrices interdites, téléphones portables interdits.

Examen terminal – première session

Exercice 1 : Cryptanalyse du chiffrement de Vigenère (5 points)

Soit le texte suivant, chiffré avec Vigenère et une clé inconnue *K* :

```
zseso sjoag kratc oaqvn abzca gvooh yobzv kookv aojdz sesos tyqzu
cjsvj aoenb svnwb upnsv jahyo bzvko
```

Question 1.1 (3 points) : Quelle est la taille de la clé *K* ?

Question 1.2 (1 point) : Dans un chiffrement par substitution, la clé est une permutation des caractères, et chaque caractère du texte initial est remplacé par le caractère correspondant dans la permutation. Est-ce qu'un message chiffré avec un chiffrement par substitution puis avec Vigenère est plus difficile à déchiffrer qu'un message chiffré uniquement avec Vigenère ?

Question 1.3 (1 point) : Que se passe-t'il si un message est chiffré deux fois avec Vigenère, la première fois avec une clé de longueur 10 et la deuxième fois avec une clé de longueur 15 ?

Exercice 2 : Signatures (5 points)

Considérons dans un premier temps le mécanisme de signature RSA sans hachage. Dans ce mécanisme, la signature S d'un message M est $S=M^d\ [n]$, où (n,d) est la clé privée d'Alice.

Question 2.1 (1 point) : Montrez qu'à partir de (M_1,S_1) et (M_2,S_2), un attaquant peut produire facilement une signature valide pour le message $M_1 \times M_2$.

Question 2.2 (1 point) : Supposons qu'un attaquant veut signer à la place d'Alice un message MA, et qu'il peut demander à Alice de signer des messages M qu'il choisit, avec bien entendu $M \neq MA$. Comment l'attaquant peut-il utiliser le résultat de la question précédente pour produire la signature de MA ?

Considérons dans un deuxième temps le mécanisme de signature RSA avec hachage.

Question 2.3 (1 point) : Rappelez comment on calcule la signature S d'un message M.

Question 2.4 (1 point) : Rappelez comment on vérifie la signature S d'un message M.

Question 2.5 (1 point) : À partir de (M_1,S_1) et (M_2,S_2), est-ce qu'un attaquent peut produire facilement une signature valide pour le message $M_1 \times M_2$.

Exercice 3 : Attaque de broadcast sur RSA (10 points)

L'attaque décrite ci-après a été proposée par J. Hastad [1]. Supposons que Alice envoie un même message M, chiffré avec RSA, à plusieurs destinataires Bob, Bernard, Bobby, Bertrand, etc. Nous nommerons ces destinataires B_1, B_2, ..., B_k. Chaque destinataire B_i possède sa propre clé publique (N_i, e_i). Nous faisons l'hypothèse que l'attaquant peut obtenir le message chiffré transmis à chacun des destinataires.

Question 3.1 (1 point) : Avec RSA, il n'est pas possible de chiffrer des messages qui sont plus grand que le modulo N_i de la clé publique. Pourquoi ?

Question 3.2 (1 point) : Rappelez comment e_i est choisi dans RSA. Est-ce que e_i doit être grand ?

Question 3.3 (1 point) : Montrez que s'il existe $i \neq j$ tel que $gcd(N_i, N_j) \neq 1$, alors l'attaquant peut trouver M. Rappelons que *gcd* calcule le plus grand diviseur commun : par exemple, $gcd(20,15)=5$.

Dans la suite, nous faisons l'hypothèse que $e_i=3$, pour tout i. Le théorème des restes chinois indique que étant donné k entiers n_1, n_2, ..., n_k qui sont deux à deux premiers entre eux, pour toute séquence a_1, a_2, ..., a_k, il est possible de déterminer (efficacement) un unique entier x modulo $n_1 \times n_2 \times ... \times n_k$ tel que $x \equiv a_1\ [n_1]$, $x \equiv a_2\ [n_2]$, ..., et $x \equiv a_k\ [n_k]$.

Question 3.4 (1 point) : Montrez que soit les k entiers N_1, N_2, ..., N_k sont deux à deux premiers entre eux, soit l'attaquent peut trouver M facilement.

Question 3.5 (1 point) : Montrez que si les k entiers N_1, N_2, ..., N_k sont deux à deux premiers entre eux, l'attaquant peut calculer $M^3\ [N_1 \times N_2 \times ... \times N_k]$ avec le théorème des restes chinois.

Question 3.6 (1 point) : Montrez que dans ce cas, et si $k \geq 3$, l'attaquant peut calculer M^3 (sans le modulo).

Question 3.7 (1 point) : Montrez que dans ce cas, et si $k \geq 3$, l'attaquent peut calculer M.

Question 3.8 (1 point) : Décrivez l'attaque complète.

Question 3.9 (1 point) : Proposez une première manière d'empêcher cette attaque.

Question 3.10 (1 point) : Proposez une deuxième manière d'empêcher cette attaque.

Références

[1] J. Hastad. Solving simultaneous modular equations of low degree. SIAM Journal of computing, 17:336—341, 1988.