4TC-CSC
05/04/2018

Durée : 2 heures.
Aucun document autorisé. Calculatrices autorisées.
2 pages. Le barème est donné à titre indicatif.

1 Mathématiques pour la cryptographie (5 points)

On considère un cryptosystème RSA avec les valeurs p = 53 et q = 11. Soit (e, N) une clé publique et d la clé privée qui lui correspond :

1. (a) Calculer la valeur publique N et la fonction indicatrice d'Euler $\phi(N)$.
   (b) Peut-on utiliser 5 comme clé publique e ? pourquoi selon vous ?

2. Sachant que $3 \times 347 = 1041$, proposez deux choix possibles des couples : clé publique (e,N), clé privée (d). Justifiez vos choix.

3. Considérons le cas où e est inférieur à d.
   (a) Calculez le chiffré c du message en clair m=10.
   (b) Pouvez-vous déduire la valeur de 417^{347} mod 583 sans la calculer ? Si oui, donnez le résultat et expliquez le.

4. A niveau égal de sécurité (temps de cryptanalyse équivalent), un cryptosystème à clé publique RSA avec des clés de taille 1024 bits est équivalent à un cryptosystème à clé privée AES avec des clés de taille 80 bits. Expliquez cette différence.

5. Expliquez pourquoi le problème RSA ("cassage" des clés RSA) est **au moins aussi facile** que le problème de factorisation.

6. Expliquez très brièvement l'impact des évolutions suivantes sur le cryptosystème RSA :
   — Découverte d'un algorithme de factorisation plus efficace que les algorithmes existants, de complexité sous exponentielle ;
   — Découverte d'un algorithme de factorisation plus efficace que les algorithmes existants, de complexité linéaire ;
   — Doublement des capacités de calcul
   — Découverte d'une approche qui permet de calculer la racine e-ième dans Z/nZ.

2 Usage d'algorithmes cryptographiques (6 points)

1. Dans le cadre d'une application web à développer, expliquez et justifiez les faiblesses du stockage de mots de passe sous la forme de :
   — hash MD5 non salé
   — hash SHA-512 salé
2. Telegram est une application de messagerie proposant le chiffrement des messages de bout-en-bout, messages qui ne sont alors pas stockés sur les serveurs de Telegram. Le chiffrement de bout-en-bout implique également que les clés ne sont pas connues/stockées par Telegram mais uniquement par les

utilisateurs. Depuis 2016 et actuellement suite à une évolution de la procédure le 20 mars 2018, l'état russe demande à Telegram (entreprise russe) de lui fournir des accès. Alors que le chiffrement est réalisé de bout-en-bout, quelles sont les possibilités et les conséquences potentielles pour la sécurité des communications des utilisateurs du service ? Comment cela peut-il être réalisé techniquement ?

3. Proposez un algorithme d'authentification mutuelle basé sur de la cryptographie asymétrique permettant à un serveur d'authentifier un client et au client d'authentifier le serveur. Vous devez décrire le matériel cryptographique initialement en possession du client et du serveur ainsi que les messages échangés lors de l'authentification mutuelle.

3 Autorités de certification (3 points)

Vous décidez d'ajouter du chiffrement sur les flux d'un serveur web en utilisant une CA **interne** (certificat côté serveur, pas d'authentification du client par certificat). Proposez un déploiement adapté de la CA et du certificat du serveur web (clés, certificats, procédures) et analysez ses limites éventuelles.

4 Secure boot (3 points)

D'après Wikipedia, Secure boot est *une fonctionnalité n'autorisant le démarrage qu'aux systèmes d'exploitation reconnus. Cette fonctionnalité vise à interdire le démarrage d'un système d'exploitation corrompu notamment par un virus ou un rootkit. [...] En mode « lancement sécurisé » (secure boot), l'UEFI utilise un mécanisme de vérification par signatures numériques. Le micrologiciel interdit tout chargement de driver ou de noyau dont la signature ne correspondrait pas à celle gravée en ROM.* Schématiquement, du matériel cryptographique est enregistré dans le matériel et sert à vérifier successivement le chargement du noyau, puis le chargement des pilotes par le noyau, puis le chargement des applications initiales par le noyau, puis le chargement des applications utilisateur par le système d'exploitation.

1. Décrivez la mise en œuvre cryptographique de ce système (quelles clés mises en œuvre, de qui sont elle connues, quelles données chiffrées/signées et avec quelle clé, quelle procédure de vérification lors du démarrage)
2. Imaginez qu'un attaquant installe un rootkit sur la machine sous la forme d'un pilote et tente de le charger. Que se passe-t-il ? De quoi l'attaquant a-t-il besoin ?
3. Imaginez maintenant que vous souhaitez installer et démarrer un noyau personnalisé (typiquement un noyau Linux ou autre système libre), de quoi avez-vous besoin ?

5 Enjeux éthiques (3 points)

Synthétisez vos lectures réalisées durant les 2 heures de préparation sur les enjeux éthiques liés à la cryptographie et à la sécurité des communications. Votre réponse doit être originale (pas de phrases retrouvables sur internet ou sur d'autres copies) ; dans le cas contraire, la note à cette question sera réduite en proportion. Vous devez être synthétique et pertinent (10 lignes maximum).