4TCA-CSC
01/03/2018

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

1 Mathématiques pour la cryptographie (5 points)

Alice souhaite mettre en place un chiffrement RSA avec Bob et elle choisit les facteurs premiers : p=11 et q=13. Soit N=p.q= 143, (e, N) une clé publique et d la clé privée qui lui correspond :

1. (a) Calculer la fonction indicatrice d'Euler $\phi(n)$, Quelle est le nombre d'entiers inférieurs à 143 qui sont premiers avec 143 ?
   (b) Pourquoi est-il nécessaire de choisir e premier avec $\phi(n)$ dans le cryptosystème RSA ?
   (c) Sachant que $7 \times 103 \equiv 1 \pmod{120}$, proposez deux choix possibles des couples : clé publique (e,N), clé privée (d).

2. (a) Quelle est la clé à utiliser pour chiffrer un message en clair m ? Donnez le chiffré c en fonction du clair m et des clés en question.
   (b) Quelle est la clé à utiliser pour déchiffrer un chiffré c ? Donnez le déchiffré m' en fonction du chiffré c et déduisez son expression en fonction de m.

3. Prouvez que pour n'importe quel entier m premier avec n, $(m^e)^d$ mod n = m (**prouvez seulement ce cas général où m est premier avec n**)

   Indices :
   - Puisque $e.d \equiv 1 \pmod{(p-1)(q-1)}$, il existe un entier l tq : $e.d = 1 + l \times (p-1) \times (q-1)$;
   - En TD nous avons utilisé le petit théorème de Fermat, mais pour le cas général il est plus facile d'utiliser le théorème d'Euler qui dit que : $m^{\phi(n)}$ mod n = 1 pour tout m premier avec n.

4. (a) Le problème de factorisation est-il du à l'inexistence d'algorithme qui permet de factoriser des très grand nombres ou l'inefficacité, en termes de temps d'exécution, des algorithmes existants ?
   (b) Est ce que la résolution du problème RSA ("cassage" des clés RSA) passera forcément par la résolution du problème de factorisation des grands nombres ? expliquez.

5. Pour chaque situation, proposez une des solutions :
   (s1) l'augmentation de la taille des clés RSA suffira ;
   (s2) l'augmentation de la taille des clés RSA n'est pas suffisante et il faudrait remplacer RSA par un autre algorithme.

   — 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 comment stocker et vérifier les mots de passe des utilisateurs inscrits.
2. Le principe de la cryptographie hybride est de combiner les cryptographies asymétrique (plus facile à déployer) et symétrique (plus rapide). Une clé symétrique (dite clé de session) est échangée en cryptographie asymétrique au début de l'échange, la suite de l'échange est ensuite chiffrée en cryptographie symétrique. Proposez une description précise d'un protocole de chiffrement hybride (message clair, contenu des multiples messages envoyés, clés, opérations cryptographiques réalisées). Pour le protocole proposé, explicitez les clés cryptographiques qui doivent être préalablement connues de chaque participant.
3. Proposez un algorithme d'authentification basé sur de la cryptographie symétrique permettant à un serveur d'authentifier un client. Vous devez décrire le matériel cryptographique initialement en possession du client et du serveur ainsi que les messages échangés lors de l'authentification. Vous devez considérer qu'un attaquant peut observer le canal mais ni jeter ni modifier les messages échangés.

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 Chiffrement de disque (3 points)

D'après Wikipedia, *le chiffrement de disque est une technologie qui protège l'information en la transformant en un code illisible qui ne peut pas être déchiffré facilement par les personnes qui n'y sont pas autorisées. Le chiffrement de disque utilise un logiciel de chiffrement de disque [...]. Le chiffrement de disque lutte contre les accès non autorisés au système de stockage de données. [...] Le chiffrement en temps réel, aussi appelé chiffrement à la volée (en anglais On-the-fly encryption ou OTFE), est une méthode utilisée par le logiciel de chiffrement de disque. Les données sont automatiquement chiffrées ou déchiffrées comme elles sont chargées ou sauvegardées. Avec le chiffrement à la volée, les fichiers sont accessibles immédiatement après avoir entré la clé de chiffrement, et le volume est normalement monté comme un disque physique, rendant les fichiers accessibles comme si aucun n'était chiffré. Aucune donnée stockée dans le volume chiffré ne peut être lue (déchiffrée) sans utiliser le bon mot de passe ou le bon fichier clé ou la bonne clé de chiffrement. Le système de fichiers entier dans le volume est chiffré (y compris les noms de fichiers et dossier, le contenu de ces derniers, et les autres métadonnées).*

1. Proposez une mise en œuvre permettant l'ouverture du volume par un mot de passe et une autre permettant l'ouverture du volume à l'aide d'une carte à puce (ici, nous considérerons qu'une carte à puce est un élément matériel qui, une fois débloqué par le code PIN, sait chiffrer et déchiffrer des données à faible débit, sans exposer les clés cryptographiques utilisées). Expliquez particulièrement les aspects cryptographiques.
2. Un même volume doit maintenant pouvoir être monté par plusieurs utilisateurs (non simultanément), chacun avec un mot de passe différent. Chaque utilisateur doit de plus pouvoir changer son mot de passe quand il le souhaite. Proposez une amélioration de votre mise en œuvre permettant cela. L'efficacité, la clarté et l'élégance de la solution seront évaluées.

5 Ouverture facultative au choix (3 points)

Synthétisez l'ouverture facultative que vous avez choisie (rappel, le choix était parmi "L'histoire de Dual_EC_DRBG", "Listen up, FBI : Juniper code shows the problem with backdoors, Fahmida Y. Rashid, InfoWorld", "SSL And The Future Of Authenticity, Moxie Marlinspike (aka Mr. Signal)", "Quantifying Untrusted Symantec Certificates, Arkadiy Tetelman"). 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).