4TC-CSC (rattrapage)
17/07/2018

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

1 Questions de cours (3 points)

1. En cryptographie asymétrique, avec 4 utilisateurs, quelles sont les clés qui doivent exister dans le système ?
2. Décrivez l'une des 3 conditions principales d'une fonction de hachage cryptographique
3. Dans le protocole Diffie-Hellman, un attaquant passif peut-il lire (et comprendre) les messages ?
4. Quelle garantie nous offre a priori une PKI ?
5. Parmi ces quatre ensembles, lesquels représentent la classe $Z/3Z$: {3,6,9} ;{0,4,8} ; {1,2,3} ; {0,1,2}.
6. Répondez par vrai ou faux. Si $a \equiv b \ mod \ n$ et $c \equiv b \ mod \ n$ et k est entier naturel alors :
   $a^k \equiv b^k \ mod \ n$
   $a^c \equiv b^d \ mod \ n$

2 Mathématiques pour la cryptographie (4 points)

1. On considère un cryptosystème RSA avec la clé public N = 187 et e=3.
   (a) Calculez le chiffré c du message en clair m=15.
   (b) Sachant que $\phi(N) = 160$, retrouvez la factorisation de N et expliquez comment on peut calculer la clé privée d.

2. Considérons le cas général d'un cryptosystème RSA avec $p > q$. Nous posons $x = \frac{p+q}{2}$ et $y = \frac{p-q}{2}$.
   (a) Montrez que $N = x^2 - y^2$
   (b) Montrez que si p et q sont proches, x est légèrement supérieur à la racine de N.
   (c) A la lumière des réponses précdentes, expliquez comment peut-on facilement factoriser N dans certains cas.
   (d) Quelle recommandation doit-on respecter lors du choix de p et q ?
3. Pourquoi la recherche exhaustive de la clé privée dans un cryptsystème RSA n'est la cryptanalyse la plus appropriée alors que c'est le cas pour un cryptosystème à clé privée bien concu ?

4. Expliquez la relation entre le problème RSA ("cassage" des clés RSA) et le problème de factorisation de nombres entiers.

3 Usage d'algorithmes cryptographiques (6 points)

1. Dans le cadre d'une application web à développer, expliquez les qualités et faiblesses du stockage de mots de passe sous la forme de hash SHA-512 non salé.
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 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.

4 Autorités de certification (2 points)

Proposez le déploiement d'une autorité de certification (CA) interne à une entreprise certifiant les employés de cette entreprise (des utilisateurs, donc). Décrivez le matériel cryptographique utilisé (clés, certificats).

RAPPEL : Un certificat associe un nom (de site type `www.insa-lyon.fr` ou de personne type `Franck.Dupont@insa-lyon.fr`) à une clé publique. Certifier un nom de personne est donc similaire à certifier une adresse de site web.

5 Messagerie sécurisée (3 points)

Proposez et analysez un système de messagerie mondial, ouvert à tous les utilisateurs souhaitant s'inscrire et proposant le chiffrement des messages. Vous devez décrire le fonctionnement de la PKI (pas forcément centralisée) ainsi que le fonctionnement de l'application de messagerie. Vous devez identifier les garanties offertes par votre application ainsi que les hypothèses de travail associées, puis les risques potentiels.

Fonctionnellement, votre système de messagerie doit permettre à deux personnes quelconques de communiquer ensemble (similaire donc au mail, Jabber, Signal, WhatsApp, etc.)

6 Ouvertures et enjeux éthiques (2 points)

Au choix (1 seul item à traiter) :

— Synthétisez vos lectures réalisées durant les 2 heures de préparation sur les enjeux éthiques liés à la cryptographie et à la sécurité des communications.

— 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).