4TC-CSC
09/04/2019

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

1 Mathématiques pour la cryptographie (5 points)

Soyez bref et concis dans vos réponses.

Alice souhaite mettre en place un chiffrement asymétrique RSA, pour assurer la confidentialité des messages qu'elle reçoit et pour qu'elle puisse signer ses messages. Elle annonce sa clé publique suivante (e=17,N=899). Les valeurs sont volontairement choisies petites pour vous simplifier les calculs.

1. Calculez le chiffré c du message en clair m=100.
   Indice : $10^{17} \equiv 131[899]$

2. Sachant que N est facteur de deux nombres premiers p et q (N=p.q), et que $\phi(N)= 840$, calculez les valeurs de p et q.

3. Nous supposons maintenant qu'un attaquant souhaite factoriser N=899 sans connaître $\phi(N)$.

   (a) D'une manière générale, montrez que N, facteur de deux nombres premiers p et q (N=p.q), peut aussi s'écrire sous la forme $N = x^2 - y^2$ avec x et y entiers.
   Indice : p peut s'écrire sous la forme $\frac{p+q}{2} + \frac{p-q}{2}$

   (b) Montrez que si p et q sont proches, x est légèrement supérieur à la racine de N et expliquez comment peut-on facilement factoriser N dans ce cas.

   (c) Appliquez votre proposition au cas N=899 en calculant les valeurs des deux facteurs p et q.

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

5. Pour les valeurs de p et q obtenus en question 2 et 3 (et qui sont logiquement les mêmes à l'ordre près des deux facteurs ☺) :

   (a) Vérifiez que 593 est bien la clé privée de Alice (On vous demande une simple vérification).

   (b) Sachant que $11^{17} \equiv 3[899]$, calculez le déchiffré (message en clair) associé au chiffré c=27.

2 Stockage des mots de passe (4 points)

Vous héritez de la maintenance d'une vieille application web dans laquelle les mots de passe des utilisateurs sont stockés sous forme de hash MD5. Ayant bien suivi le cours de 4TC-CSC, vous décidez d'améliorer ce point.

1. Pourquoi ce point pose-t-il problème ? Face à quel genre d'attaque ?
2. Comment les mots de passe devraient-ils être stockés ? Pourquoi ?
3. Sachant que vous ne disposez pas des mots de passe en clair mais uniquement des hash MD5, proposez une démarche de migration vers votre nouvelle solution.

3 Protocoles cryptographiques (4 points)

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 un protocole de chiffrement hybride respectant les contraintes suivantes :

— les 2 interlocuteurs doivent s'authentifier mutuellement au début de l'échange par des mécanismes de cryptographie asymétrique

— l'ensemble des utilisateurs du système fait confiance a une même autorité de certification pour certifier les usagers

L'autorité de certification est munie d'une paire de clés $Pub_{CA}/Priv_{CA}$. Chaque utilisateur possède également une paire de clés. Tous les utilisateurs connaissent la clé publique de la CA, ils ne connaissent par contre pas au départ de l'échange les clés publiques des autres utilisateurs.

Pour le protocole proposé, décrivez le matériel cryptographique nécessaire, les messages clairs originaux, le contenu des multiples messages envoyés, les clés, les opérations cryptographiques réalisées.

4 Cartes à puce (4 points)

Une carte à puce (carte bancaire, SIM, etc.) est un mini-ordinateur intégrant des clés cryptographiques et offrant des fonctions permettant d'utiliser ces clés. Un code PIN permet de débloquer l'usage de ces fonctions. Une fois débloquées, ces fonctions permettent de chiffrer, déchiffrer, signer, vérifier. Les clés cryptographiques restent toujours dans la puce, elles ne sont jamais exportées, c'est la puce uniquement qui les exploite et ne renvoie que le résultat des opérations demandées.

1. Proposez un système de cartes bancaires (il n'est pas nécessaire que cela corresponde au système réel, vous devez faire une proposition pertinente). Vous décrirez notamment la création initiale de la carte, son matériel cryptographique, qui le connaît, ce qui se passe lors d'un paiement.
2. Est-il possible, avec votre solution, de faire un faux-paiement avec une fausse carte ? Autrement dit, une carte créée indépendamment, non liée à une banque et à un compte, peut-elle tromper le terminal de paiement et lui faire croire que le paiement est valide (alors que le commerçant ne pourra pas être payé, la carte n'étant attachée à aucun compte bancaire) ? Si cela est possible, quelle solution pouvez-vous proposer ? Vous étudierez le cas où le terminal de paiement a accès au réseau (il peut typiquement interroger une banque de manière interactive) et le cas où le terminal n'a pas accès au réseau. On se concentrera ici sur les aspects réseaux et cryptographiques, pas sur l'aspect visuel de la carte.

Les YesCards étaient de fausses cartes qui permettaient ce type d'attaque. La vulnérabilité associée a bien sûr depuis été corrigée.

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).