4TCA-CSC
28/02/2019

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,N=1271). Les valeurs sont volontairement choisies petites pour vous simplifier les calculs.

1. Pour e=7,
   (a) Calculez le chiffré c du message en clair m=192 en utilisant la méthode d'exponentiation rapide. Indice : $192^2 \equiv 5[1271]$
   (b) Comparez le nombre d'opérations nécessaires pour calculer ce chiffré en utilisant une méthode ordinaire basée sur des simples multiplications et en utilisant l'exponentiation rapide.

2. Pourquoi, selon vous, l'exposant $e = 2^{16} + 1$ est souvent choisi en pratique avec des clés de 1024 ou 2048 bits.

3. Sachant que N est facteur de deux nombres premiers p et q (N=p.q) :
   (a) Montrez que N 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=1271. Donnez les valeurs de p et q et le nombre d'itérations nécessaires pour factoriser 1271.

4. Pour les valeurs de p et q trouver dans la question précédente :
   (a) Calculez $\phi(N)$ et expliquez si on peut-on choisir e=5, e=11 ? Justifiez vos réponses.
   (b) Reprenons le cas de e=7, sahcant que $7 * 343 = 2401$, pouvez-vous déduire la valeur de $5 \times (1122)^{343}$ *mod* 1271 ?

5. 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 conçu ?

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

2 Mots de passe (2 points)

Dans le cadre d'une application web à développer, expliquez les qualités et faiblesses du stockage de mots de passe sous la forme de chiffré AES puis de hash SHA-512 salé. Comment vérifier les mots de passe des utilisateurs inscrits ?

3 Protocoles cryptographiques (4 points)

1. Proposez un protocole basé sur de la cryptographie asymétrique permettant l'authentification d'un client par un serveur. Vous devez décrire le matériel cryptographique initialement en possession du client et du serveur ainsi que les messages échangés lors de l'authentification. Un attaquant peut observer ou modifier le canal, ce qui peut faire échouer l'authentification. Si l'authentification réussit, le serveur est certain de communiquer avec le bon client et un canal de communication sûr (chiffré) a été mis en place.
2. D'après Wikipedia, *la confidentialité persistante (forward secrecy en anglais), est une propriété en cryptographie qui garantit que la découverte par un adversaire de la clé privée d'un correspondant (secret à long terme) ne compromet pas la confidentialité des communications passées.*. Ce système est donc robuste à une attaque dans laquelle l'attaquant a observé les échanges puis volé une clé privée d'un des participants. Votre protocole précédent a-t-il cette propriété ? Si oui, justifiez pourquoi. Si non, proposez une amélioration ayant cette propriété.

4 Autorités de certification (2 points)

Vous décidez d'ajouter du chiffrement sur les flux d'un serveur web en utilisant une CA **externe tierce** (type Verisign). Vous souhaitez avoir un certificat côté serveur, pas d'authentification du client par certificat. Proposez un déploiement adapté (clés, certificats, procédures, matériel côté serveur, matériel nécessaire côté client) et analysez ses limites éventuelles.

5 Messagerie chiffrée de bout en bout (4 points)

D'après Wikipedia, *le chiffrement de bout en bout (en anglais, End-to-end encryption ou E2EE) est un système de communication où seules les personnes qui communiquent peuvent lire les messages échangés. En principe, il empêche l'écoute électronique, y compris par les fournisseurs de télécommunications, par les fournisseurs d'accès Internet et même par le fournisseur du service de communication. Avec le chiffrement de bout en bout, personne n'est en mesure d'accéder aux clés cryptographiques nécessaires pour déchiffrer la conversation. Les systèmes de chiffrement de bout en bout sont conçus pour résister à toute tentative de surveillance ou de falsification, car aucun tiers ne peut déchiffrer les données communiquées ou stockées. En particulier, les entreprises qui offrent un service de chiffrement de bout en bout sont incapables de remettre une version déchiffrée des messages de leurs clients aux autorités.*

Proposez la conception cryptographique d'une telle messagerie chiffrée (inscription des utilisateurs, échange de messages, sauvegarde d'un historique de communication). Le serveur ne doit pas pouvoir espionner ou falsifier les communications, même sous la contrainte. Analysez ensuite votre solution, en particulier son ergonomie, sa facilité d'utilisation, ce qui reste éventuellement espionnable, les risques restants et la gestion du changement de périphérique d'un utilisateur (remplacement du *smartphone*, typiquement). L'évaluation prendra en compte l'utilisabilité de la solution proposée et la qualité de son analyse critique

6 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).