Examen Formatif - S3i – APP6 : Sécurité des systèmes informatiques

Professeur : Frédéric Mailhot

1. Pour les clés RSA, on choisit e et d de telle sorte que $d = e^{-1} \bmod \phi(n)$.
   a) Expliquez pourquoi.
   b) Expliquez ce qui arrive si e et $\phi(n)$ ne sont pas relativement premiers.
   c) Comment peut-on faire pour prédéterminer la valeur de e, avant même d'avoir trouvé n et $\phi(n)$?
   d) Pourquoi devrait-on choisir une petite valeur pour e?

2. Le théorème du reste chinois (TRC) est utilisé pour accélérer les calculs de la méthode RSA.
   a) Trouvez la représentation TRC de m = 18 avec la base n = p X q = 5 X 7 = 35.
   b) En supposant que p et q sont habituellement de tailles comparables (même nombre de bits), que pouvez-vous dire de la taille d'un message m comparé à la taille de sa représentation TRC? Supposez que m utilise le même nombre de bits que n.
   c) Soient deux nombres de 32 bits x et y, et deux nombres de 64 bits z et t. Le calcul du produit de z par t prendra 4 fois plus de temps que le calcul du produit de x par y. En quoi cela favorise-t-il l'utilisation du TRC?

3. La méthode de Miller-Rabin est utilisée pour déterminer si un nombre est premier
   a) Pourquoi cette méthode est-elle préférable à celle du petit théorème de Fermat?
   b) Est-on certain qu'un nombre identifié comme premier par la méthode de Miller-Rabin est effectivement premier? Pourquoi?
   c) Expliquer pourquoi on divise itérativement (p – 1) par 2 dans cette méthode. Pourrait-on diviser par un autre nombre premier? Expliquer pourquoi.

4. La méthode de Diffie-Hellman a été la première méthode à clé publique connue de tous. Est-ce que cette méthode aurait été utilisable sans l'existence de méthodes d'encryption symétrique? Expliquez votre réponse.

5. Expliquez pourquoi la méthode rho de Pollard utilise l'algorithme de Floyd. En effet, cette méthode requière 3 fois plus d'appels à la procédure de calcul du polynôme f(x) que la méthode de Pollard initiale.

6. Soit un échange de messages numériques signés entre Alice et Bob.
   a) Expliquez comment Alice peut utiliser un système à clé publique tel RSA pour signer un document électronique destiné à Bob.
   b) Maintenant Ève entre en scène : Alors qu'Alice envoie un message signé à Bob, Ève intercepte le message d'Alice, lui substitue son propre message signé, et fait croire à Bob qu'il est signé par Alice. Expliquez comment Ève a pu procéder pour faire accepter à Bob que sa signature est bien celle d'Alice.
   c) Supposons qu'Alice envoie à Bob des messages encryptés à l'aide de la clé publique qu'elle croit être celle de Bob. Comment Ève pourrait-elle procéder pour pouvoir lire les messages destinés à Bob? Dans ce cas, si le même

message parvient à Bob, va-t-il s'en apercevoir? Est-ce que Ève peut faire quelque chose pour cacher son jeu?

7. Soit un programme dans lequel existe une vulnérabilité au problème de « buffer overflow ».
   a) Si le problème est dû à strcpy(), croyez-vous qu'il serait possible de modifier cette procédure système pour éliminer le problème? Si oui, comment? Si non, quelle information supplémentaire devrait-on posséder? Est-il possible d'avoir accès à cette information?
   b) Si toutes les procédures systèmes étaient modifiées pour enrayer leur susceptibilité au problème de « buffer overflow », est-ce que les applications bâties à l'aide de ces procédures systèmes seraient alors sécuritaires?
   c) Selon vous, serait-il possible de recompiler la même application (sans modification de code source) à l'aide d'un compilateur différent, et d'éliminer le problème de « buffer overflow »? Si, oui, expliquez comment. Si non, expliquez pourquoi.

8. Vous êtes responsable de la sécurité dans une entreprise de moyenne envergure, où les usagers des systèmes informatiques sont peu connaissant des vulnérabilités liées aux mots de passe. Donnez quelques règles simples pour les aider dans le choix d'un mot de passe sécuritaire.