TD noté 2

Date limite de remise du TD : vendredi 12 décembre 2014 à 23h59.

Le TD se fait par groupe de 2 étudiants (au maximum) et les fichiers à rendre doivent être envoyés au plus tard vendredi le 12 décembre à minuit par courriel à l'adresse électronique « cristina.onete@gmail.com ». Merci d'expliquer en détail le raisonnement suivi. Si vous devez programmer un algorithme, cela peut se faire en C, C++, Python ou Java. Merci de joindre le code de votre algorithme aux fichiers remis dans le cadre du TD.

Rappel : tout plagiat est formellement interdit et bien qu'il soit naturel que vous puissiez parfois discuter avec vos camarades oralement sur comment attaquer ou résoudre un problème, il est formellement interdit d'échanger des fichiers de code.

Le total des points du TD est de 20 + 2.5 points en bonus pour l'exercice, qui est optionnel car « difficile ». Si vous réussissez cet exercice, les 2.5 points de bonus peuvent compter en plus des 20 autres points pour la moyenne globale des TDs.

1. Supposons qu'Amélie, Baptiste, Christine et Denis veulent communiquer de manière sécurisée.

a. Supposons que ces quatre usagers veulent utiliser le chiffrement symétrique pour communiquer en pair-à-pair (chaque usager veut pouvoir communiquer de manière sécurisée avec chaque autre). Combien de clés doivent être générés dans le système dans ce cas? (0,5 points)

b. Supposons qu'ils souhaitent utiliser un chiffrement à clé publique. Combien de paires de clés doivent être générées pour permettre à chaque usager de pouvoir communiquer avec tous les autres? (0,5 points)

c. Plus généralement, supposons qu'on ait un système avec *N* usagers. Combien de clés symétriques doivent-ils avoir pour communiquer en pair-à-pair? Même question pour le nombre de paires de clés asymétriques? (1 point)

d. Que pouvez-vous en conclure quand à l'usage du chiffrement à clé publique et l'usage du chiffrement symétrique dans le cas de grands groupes d'utilisateurs? (1 point)

2. Implémentez l'algorithme de signature DSA. (4 points)

Est-ce que les signatures produites par cet algorithme-ci sont probabilistes ou déterministes ? (1 point)

Vérifiez les prochaines signatures pour les paramètres : p = 15811267, q = 541, g = 557069, pk = 12657825, et pour les messages suivants:

a. M = 52 ; $H(M)$ = 5836403135864276661 ; Signature = [344, 107] (0,5 points)

b. M = 19 ; $H(M)$ = 8654798746728582722 ; Signature = [374, 241] (0,5 points)

3. Supposons qu'Amélie et Baptitse partagent une clé privée sk utilisée danas le cadre d'un chiffrement par blocs. Supposons que ce chiffrement par blocs est chainé comme décrit dans l'équation suivante: $C_i = M_{i-1} \text{ XOR } Enc_{sk}(M_i \text{ XOR } C_{i-1})$, où « Enc » dénote le chiffrement symétrique et XOR représente l'opération de faire un OU exclusive bit-par-bit. Le message en entrée est noté $M_1 \dots M_N$ alors que le chiffré obtenu en sortie est $C_1 \dots C_N$, où C_0, M_0 sont des vecteurs d'initialisation (*starting vectors*) qui sont publiquement connus.

a. Dessinez un diagramme représentant le fonctionnement de ce chiffrement par blocs, en indiquant clairement le processus du chaînage. (1 point)

b. Si Amélie utilise ce chiffrement par bloc pour encrypter un message $M_1 \dots M_N$ pour Baptiste, comment celui-ci peut t'il déchiffré ce message? (1 point)

c. Si le 5ème bloc du chiffré, qu'on dénote C_5 , est corrompu pendant la transmission, quels autres blocs vont être affectés ? (1 point)

d. Suggérez une méthode permettant à Baptiste de vérifier s'il y a eu une corruption des chiffrés (en autres mots, on veut pouvoir vérifier l'intégrité du chiffré). (1 point)

4. Pour chacune des prochaines propositions, expliquez si elles sont vraies ou fausses en argumentant votre réponse.

a. Si une fonction de hachage a des valeurs en entrée de taille l_{input} et donne des valeurs en sortie de taille l_{output}, si $l_{input} > l_{output}$, alors il y aura toujours des collisions. (0,5 points)

b. Dans un protocole d'authentification, le but du prouveur est de démontrer sa légitimité. Par contre, dans un protocole d'identification, le prouveur cherche plutôt à établir son identité. (0,5 points)

c. Supposons qu'Amélie et Baptiste souhaitent générer une clé secrète commune. Amélie a une paire de clés de signatures certifiée par une autorité de confiance. Étant donné une fonction de hachage *H* à sens unique, supposons qu'Amélie choisit une clé à partager K avant d'envoyer le message $(H(K), Sign_{sk}(H(K)))$. Est-ce que ce message forme un protocole d'échange de clé sécurisé? (1.5 points)

d. Considérons un schéma d'engagement qui prend en entrée un secret x de 128 bits et un témoin de 128 bits, et qui donne en sortie une valeur : $c \coloneqq Commit(x, w) = H(x \text{ XOR } w)$. En supposant que la fonction de hachage est à sens unique, est-ce que l'engagement est camouflant? Est-il liant? Si la fonction de hachage donne des valeurs pseudo-aléatoires, est ce que l'engagement est à la fois liant et camouflant? (1.5 points)

5. Supposons qu'Amélie, Baptiste, Christine et Denis sont amis. Ils veulent aller dîner à un restaurant ce soir, mais ils n'ont pas encore décidé du lieu. Supposons qu'ils ont tous des clés de chiffrement à clé publique, et qu'en en plus chaque paire d'amis partage une clé symétrique pour un MAC. Ils utilisent un canal de diffusion, où tous les messages envoyés sont visibles par tous les autres. Pour chacune des situations suivantes, proposez une méthode qui garantit qu'ils déterminent de manière correcte le restaurant.

Exemple. Amélie est l'expert en matière de restaurants et donc son choix devrait être accepté par tous. Par contre, chacun des autres aimerait bien être capable d'influencer la décision finale vers leur restaurant favori. Garantissez que la bonne décision va être prise.

Solution. Amélie choisi un restaurant, disons $rest_A$. Elle envoie le message suivant sur le canal de diffusion: $rest_A \| MAC_{sk_{AB}}(rest_A) \| MAC_{sk_{AC}}(rest_A) | MAC_{sk_{AD}}(rest_A)$. Dans cette expression, sk_{AB} représente la clé symétrique de MAC partagée par Amélie et Baptiste, sk_{AC} est la clé partagée par Amélie et Christine, etc.

a. La connexion d'Amélie au canal de diffusion ne fonctionne plus. Par contre, elle a accès à un canal privé entre elle et Baptiste. Les autres ne pourront donc pas voir les messages échangés sur ce canal-ci. Montrez comment Amélie peut envoyer son choix d'experte à Baptiste et ensuite comment Baptiste peut envoyer le choix d'Amélie à Christine et Denis de manière à les convaincre que celui-ci

a vraiment été le choix d'Amélie (et non pas un restaurant qui aurait pu être proposé par Baptiste). (1 point)

b. Amélie et Christine sont en train d'organiser une fête surprise à Baptiste pour son anniversaire, dont le dîner fait partie de la surprise. Toutefois, les deux filles ne sont pas d'accord avec le choix du restaurant. Amélie préfèrerait aller à une crêperie, tandis que Christine préférerait une brasserie. Ils ont donc décidé que le vote de Dénis (qui doit choisir entre les deux possibilités) sera le vote décisif. (1 point)

c. (Difficile) Comme c'est l'anniversaire de Baptiste, ses amis ont décidé de lui laisser le choix du restaurant entre une crêperie et une brasserie. Les trois amis savent cependant que Baptiste va accepter le choix de la majorité de ses amis. Comment est-ce que vous pouvez empêcher qu'un de ces amis vote deux fois ? Comment pouvez-vous garantir que le vote soit équitable, c'est-à-dire qu'aucun participant ne connaisse les autres votes en avance même si les votes sont échangés par le canal de diffusion. Plus difficile encore que peut-on faire si on suppose que les amis n'ont même pas accès à un chiffrement à clé publique? (2.5 points)

6. Amélie et Baptiste ont des clés certifiées pour des signatures DSA. Ils veulent échanger une suite de messages authentifiés et confidentiels. Comment peuvent-ils réaliser cela? (1 point)