Master 1 Info 2015 - 2016

Introduction à la Sécurité **Examen**

Toutes les réponses doivent être justifiées. N'hésitez pas à passer une question, quitte à y revenir ensuite.

Exercice 1 (3 points) - Expliquer en une ou deux phrases les termes suivants :

1. Confidentialité des messages.
2. Authenticité des messages.
3. Intégrité.
4. Certificat.
5. Différence entre cryptographie à clef publique et cryptographie à clef secrète.
6. Taille de clef AES/RSA.

Exercice 2 (3 points) - Compléter le texte à trous (IPSec)

Pour cette exercice, il vous faut compléter le texte à trous en reportant les numéros, présent dans le texte, sur votre copie avec le mot (expression ou morceau de phrase) manquant correspondant.

Alice et Bob sont à l'université et ils ont tous deux eut un cours extrêmement passionnant sur la sécurité des réseaux et plus particulièrement sur IPSec. Alice et Bob souhaitant s'envoyer des messages de manière sécurisée ont décidé de tester entre leurs propres équipements ce protocole. En effet, IPSec permettant l'interconnexion, de manière ...(1)... et ...(2)..., de deux sites distants cela leur permet d'échanger des messages où l'...(3)... des données est vérifiée et de se prémunir des attaques par ...(4)... (sous-protocole ...(5)...). Ils pourraient donc s'envoyer des messages pour terminer le compte rendu de leur TP en s'assurant que Alice et Bob sont bien ceux qu'ils prétendent être.

Pour cela, ils ont mis en place des a...(6.1)... de s...(6.2)... (AS) permettant de définir quel sous-protocole (AH), quel mode (...(7)... ou ...(8)...) et quel algorithme d'...(9) utilisé. Une AS est ...(10)... C'est-à-dire qu'il faut qu'Alice et Bob définissent chacun deux AS : une pour le flux ...(11)... et une pour le flux ...(12)... .

Le ...(13.1)... ...(13.2)... ...(13.3)... (SPI) permet d'identifier de façon unique une AS. Il est transporté dans chaque paquet pour que l'équipement au bout du tunnel puisse ...(14)...

Cependant, ces deux brillants étudiants, ont vite remarqué qu'Éve, qui ne finit jamais ces TP pourrait écouter leur canal de communication pour récupérer leurs réponses et copier leur

travail. Pour éviter cela, ils ont décidé de ne plus utiliser AH mais ESP qui permet en plus des propriétés de AH d'assurer la ...(15)... des ...(16)... Il ont donc dû modifier leur AS pour modifier le sous protocole utilisé (ESP) et choisir l'...(17)... de ...(18)... à utiliser.

Exercice 3 (3 points) - Confidentialité et authentification

Est-ce que si Alice et Bob disposent pour communiquer d'une méthode de chiffrement assurant une sécurité inconditionnelle au niveau de la confidentialité des messages (par exemple la méthode du masque jetable ou one-time pad en anglais) cela implique aussi la propriété d'authentification ? Si oui, expliquez pourquoi. Sinon, décrivez une attaque sur cette méthode de chiffrement qui démontre clairement que la propriété de confidentialité n'implique pas celle d'authentification.

Exercice 4 (3 points) - Calcul RSA

Dans cet exercice on se propose d'énumérer tous les couples (clé publique / clé privée) pour RSA avec $p = 5$ et $q = 7$.

1. Définir et déterminer $\varphi(35)$.
2. Déterminer tous les entiers x tels que $\text{PGCD}(x, \varphi(35)) = 1$.
3. Déterminer tous les couples (e, d) tels que $ed = 1 \bmod \varphi(35)$.
4. Pour le couple $(5, d)$, calculer le chiffré de 3 et déchiffrer 4.

Exercice 5 (3 points) - Utilisations des fonctions cryptographiques

Soit M un message. Dans la table ci-dessous, les valeurs dans la première colonne représentent les entrées envoyées par Amélie à Baptiste. Baptiste dispose d'une paire de clés publique-privée ($\mathsf{sk_B}$,$\mathsf{pk_B}$) utilisée pour le chiffrement, et lui et Amélie partagent une clef secrète de MAC $\mathsf{sk_{MAC}}$. Chacune des colonnes suivantes correspond à un des trois objectifs principaux de la cryptographie.

Dans le tableau, H représente une fonction de hachage cryptographique, $\mathsf{Enc_{pk_B}}$ correspond à un mécanisme de chiffrement à clef publique utilisant la clef publique de Baptiste et | dénote la concaténation. remplissez le tableau avec oui ou non pour dire si la propriété est assurée et commentez.

Propriété / Message	Confidentialité du message	Authenticité du message	Intégrité du message
$M,H(M)$			
$Enc_{pk_B}(M)$			
$Enc_{pk_B}(M\|H(M))$			
$Enc_{pk_B}(M)\|H(M)$			

Exercice 6 (3 points) - étude d'un protocole d'authentification

Le protocole d'authentification suivant se déroule entre Alice et Bob. Il suppose que ces deux participants partagent déjà une clé secrète K_{AB} et qu'ils souhaitent l'utiliser pour s'authentifier ainsi que pour générer une nouvelle clé K'_{AB}.

1. A $\rightarrow$ B : $\{N_A\}K_{AB}$
2. B $\rightarrow$ A : $\{N_A + 1, N_B\}K_{AB}$
3. A $\rightarrow$ B : $\{N_B + 1\}K_{AB}$
4. B $\rightarrow$ A : $\{K'_{AB}, N'_B\}K_{AB}$

1. Traduisez le protocole tel qu'il est écrit en notation de protocole de sécurité dans des phrases en langue naturelle expliquant son déroulement.
2. Une fois que l'étape 3 est terminée peut-on considérer qu'Alice et Bob sont mutuellement authentifiés ?
3. Décrivez une attaque par rejeu contre le protocole. Pourquoi est-ce que cette attaque est possible ?
4. Comment peut-on modifier le protocole pour se prémunir contre cette attaque ?

Exercice 7 (3 points) - Vulnérabilités web

Les failles XSS (Cross-Site Scripting) permettent d'injecter des scripts dans un site internet. Par exemple, il peut être possible de commenter une discussion sur un forum en ajoutant du javascript. Le script étant stocké pour être affiché à tout les utilisateurs du forum on parle alors de faille XSS permanente. Pour vérifier qu'une faille XSS est présente, il suffit de déposer de script suivant en tant que commentaire sur le forum :

```
<script>alert('bonjour')</script>
```

Si celui-ci affiche une pop-up contenant la chaîne de caractère *bonjour*, alors le forum est vulnérable. Pour contrer ce type de vulnérabilité il faut vérifier ce qui est transmis au navigateur web ou avant insertion dans la base de données. Pour cet exercice, nous nous plaçons dans le cadre d'audit de code. Vous devez auditer le code suivant pour trouver des vulnérabilités avant sa mise en production.

Lorsque l'on attaque le site avec une faille XSS en injectant le code suivant :

```
<script>
location.replace('http://mon_site_qui_ressemble_a_l_original_mais_qui_ne_l_es_pas');
</script>
```

rien ne se passe car la fonction **strip_tags()** supprime les balises *<script>* et *</script>*.

1. Et-il possible de contourner la protection mise en place (**strip_tags()**) pour injecter du javascript ? Si oui, donner un code javascript fonctionnel.
2. Trouver une autre faille (qui n'a rien à voir avec une vulnérabilité XSS) dans le code php fournie et expliquer comment l'exploiter. D'après vous, quels sont les risques d'une telle attaque ?

(code page suivante)

ajoutCommentaire.php :

```
<?php
include($_GET['monFichier']);
.....
?>
<html>
    <head>
        <link rel="stylesheet" type="text/css" href="../CSS/pagePrinc.css" />
      <title>Site</title>
    </head>
    <body background="../Images/background.jpg">........</body>

    <?php echo "<form action=\"./ajoutcom.php\"".$id." method=\"post\">";?>
        <div>
            <label for="message">Message :</label>

            <?php
      echo "<input type=\"hidden\" name=\"id\" id=\"id\" value=\"".$id."\">";
            ?>

            <textarea row="10" cols="50" id="commentaire" name="commentaire">
        </textarea>
      <div class="button">
          <button type="submit">Envoyer votre message</button>
      </div>
  </div>
    </form>
</html>
```

ajoutCom.php :

```
<?php
    session_start();
    $com=$_POST["commentaire"];
    .........
    $nom = $user->getNom($id);
    $ligne = $user->fetch($nom);
    $coms = $com->insertion($ligne["Nom"],strip_tags($com));
    echo "Insertion faite";
    echo "<form enctype=multipart/form-data action=\"./welcome.php"\" method=\"post\">"
        ;
    echo "<input type=\"submit\">Valider.</submit>";
    echo "</form>";
?>
```