UNIVERSITÉ DE SHERBROOKE

Université de Sherbrooke

Département d'informatique

IFT 606

Sécurité et cryptographie

Chargés de cours :

Mohammed Ouenzar

Marc Verreault

ACÈS OK

Examen final

Mardi 23 juin 2015, 15h30 à 17h20

Cryptographie et Attaque

Consignes :

- Répondez sur les feuilles réponses se trouvant à la fin de l'examen;
- Cet examen comprend quatre questions réparties sur dix-sept pages;
- Assurez-vous que toutes les questions s'y retrouvent;
- Aucune documentation n'est permise;
- L'évaluation compte pour 25% de la note finale.

Nom : _____ Prénom : _____

Signature : _____ Matricule : _____

Question 1 : Les principes de la cryptographie — 25pts

1) Expliquez brièvement les concepts suivants :

   a. Cryptographie *(1pt)*;

   b. Cryptanalyse *(1pt)* ;

   c. Cryptologie *(1pt)*.

2) Expliquez en détail la différence entre la cryptographie symétrique et la cryptographie asymétrique *(2pts)*.

3) Donnez un critère primordial définissant une fonction du chiffrement *(2pts)*.

4) Dans le contexte de la cryptographie symétrique, donnez les caractéristiques d'un algorithme efficace *(2pts)*.

5) Expliquez la différence entre le chiffrement par bloc et le chiffrement par flot *(2pts)*.

6) Expliquez l'attaque par le milieu («Man-in-the-middle») appliqué sur le DDES (double DES) *(2pts)*.

7) Si vous aviez à faire un choix entre TDES et AES, quel serait votre choix *(1pt)*? Justifiez *(2pts)*.

8) Expliquez le problème mathématique complexe sur lequel la sécurité de RSA se base. Donnez un exemple *(2pts)*.

9) Donnez une définition mathématique de l'inverse modulaire *(2pts)*.

10) Décrivez le processus (algorithme) du chiffrement RSA en partant de la génération des clés jusqu'aux échanges de messages *(2pts)*.

11) Expliquez la différence entre une signature électronique et un certificat électronique *(2pts)*.

12) Vrai ou faux : Un réseau de Feistel repose sur des principes simples dont les permutations, les substitutions, les échanges de blocs de données et une fonction prenant en entrée une clé intermédiaire à chaque étage *(1pt)*.

Question 2 : La cryptographie au service de la santé 25pts

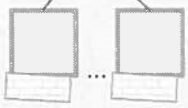
Lieu	Hôpital	Entre Sherbrooke/Québec	Ministère de la Santé et des Services sociaux
Fonction	Dossier clinique informatisé	Transmission	Dossier Santé Québec
Serveurs			
Clients			
Données	Données médicales ++	Identité Utilisateur (UID) Identité Organisation (OID)	Données médicales
Formats	Base de données SQL	XML/SOAP	Base de données SQL

Figure 2.1 : Illustration d'un dossier clinique informatisé. Au niveau de l'hôpital (à gauche), on saisit des données médicales des patients dans une base de données médicale (Dossier clinique informatisé). Des personnes de l'hôpital y ont accès par des clients (postes de travail). Au niveau du ministère de la Santé et des Services sociaux(à droite), on conserve une partie ces données médicales dans une base de données SQL (le Dossier Santé Québec). Des personnes au ministère y ont accès par un client (poste de travail). Entre Sherbrooke et Québec (au centre), il y a transmission de données médicales dans des messages. Ces messages incluent entre autres l'Identité Utilisateur (UID) et l'Identité Organisation (OID). Ces messages de format XML/SOAP doivent assurer la *confidentialité, l'intégrité, l'irrévocabilité* et *la non-répudiation.*

Basé sur vos connaissances de cryptographie, comment peut-on assurer la *confidentialité (2pts), l'intégrité (2pts), l'irrévocabilité (2pts)* et *la non-répudiation (4pts)* dans ce cas d'utilisation? Justifiez *(10pts).*

Question 3 : Du risque aux conséquences — 25pts

Énumérez et expliquez les risques associés aux six attaques suivantes :

1) «Cross-site scripting» (XSS) *(4pts)*;

2) Dépassement de tampon («Buffer overflow») *(4pts)*;

3) Déni de services («Denial of services») *(4pts)*;

4) Injection SQL («SQL injection») *(4pts)*;

5) Attaque par le milieu («Man-in-the-middle») *(5pts)*;

6) Ingénierie sociale/«science of persuasion» *(4pts)*.

Question 4 : Sécuri-Maturité 25pts

Considérant les notions de sécurité apprises dans le cours (attaque), comment pensez-vous adapter vos pratiques professionnelles afin de réduire le risque dans les domaines ci-dessous?

Indice : songez aux vulnérabilités et attaques possibles qui s'appliquent à chacun de ces domaines qui requièrent d'adapter vos pratiques professionnelles.

1) Programmation *(5pts)*;

2) Bases de données *(5pts)*;

3) Réseautique *(5pts)*;

4) Relations humaines/sociales *(5pts)*;

5) Du monde physique/matériel *(5pts)*.