FACULTÉ DES SCIENCES

Formulaire pour reprographie d'examen

Le questionnaire d'examen doit parvenir au Centre de reprographie 5 jours ouvrables avant la date de l'examen.

INFORMATIONS POUR LE SECRÉTARIAT DE LA FACULTÉ
(Attacher à chaque questionnaire)

☒ **INTRA**
☐ **FINAL**

Sigle : IFT606 (H-15)

Titre : Sécurité et cryptographie

Professeur : OUENZAR, Mohammed et VERREAULT, Marc

Date et heure de l'examen : Mercredi 25 février, 13h30 à 15h20, D3-2031,39

Nombre de pages : 16

Nombre d'étudiants : 48

☐ **Je désire prendre possession des questionnaires d'examen la veille de l'activité et je me rends responsable de leur mise en sécurité.**

Signature : _____

L'étudiant devra répondre

☐ dans un cahier d'examen
☒ sur le questionnaire

Veuillez inclure

40 feuilles blanches additionnelles
_____ feuilles de papier graphique

Je consens à ce que deux (2) copies du questionnaire de cet examen soient remises à l'AGES (Association générale des étudiants en sciences) après la fin de la période des examens.

☒ **OUI** ☐ **NON**

Signature : _____

Université de Sherbrooke
Département d'informatique

IFT 606
Cryptographie et sécurité

Chargés de cours :
Mohammed Ouenzar
Marc Verreault

Examen périodique
Mercredi 25 février 2015, 13h30 à 15h20

Consignes :

- Cet examen comprend six questions réparties sur 16 pages.
- Assurez-vous que toutes les questions s'y retrouvent.
- Aucune documentation n'est permise.
- L'évaluation constitue 25% de la note finale.
- Répondez sur le questionnaire.

Nom : _____ Prénom : _____

Signature : _____ Matricule : _____

Question 1 : XOR — 10pts

La méthode *simple XOR* consiste à faire un OU exclusif (dénoté par le symbole ⊕) entre un message *m* et une clé *k* tous deux de *l* bits (*l* est donc déterminé à partir de la longueur du message à encoder exprimée en bits) pour obtenir un cryptogramme *c*.

$$c = m \oplus k.$$

a. À partir du cryptogramme c et de la clé k, donnez la façon de retrouver le message original m. Justifiez votre réponse (3pts).

b. Donnez deux inconvénients de cette méthode (4pts).

c. À l'instar de *Triple-DES*, considérons maintenant le *triple XOR*, c'est-à-dire que :

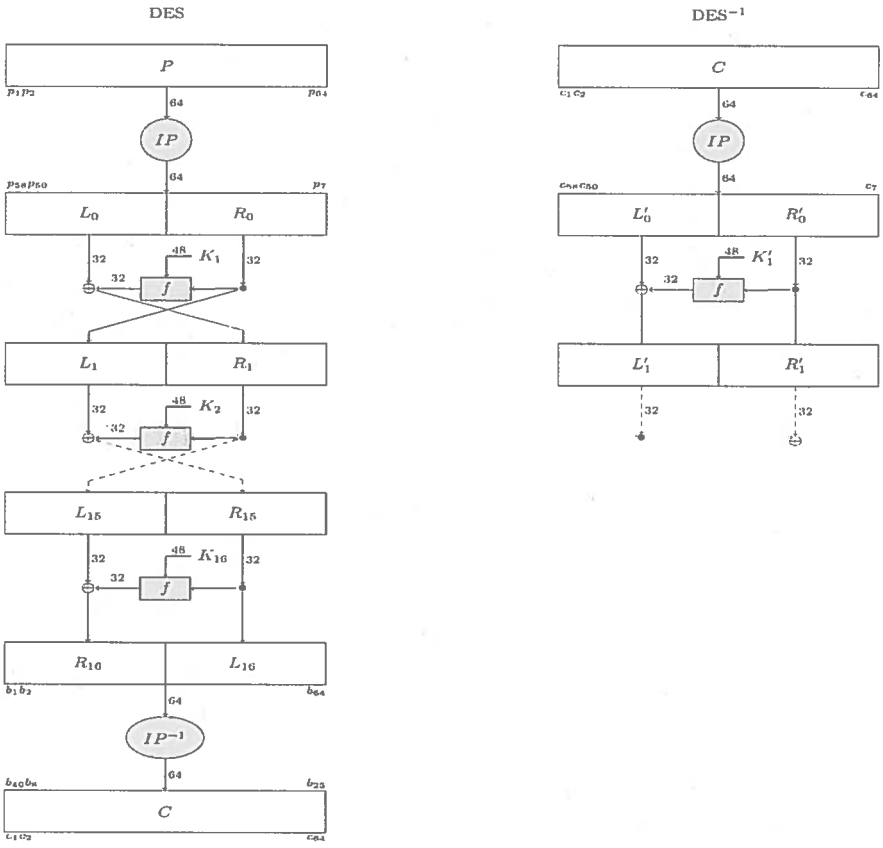
$$c = (((m \oplus k_1) \oplus k_2) \oplus k_3)$$

Où k_1, k_2 et k_3 sont trois clés distinctes de longueur l.

Est-ce que *triple XOR* est plus sécuritaire que simple *XOR*? Justifiez votre réponse (3pts).

Question 2 : DES 10pts

La figure suivante montre les seize tours de la partie encodage de l'algorithme DES (*Data Encryption Standard*), incluant les permutations IP et IP^{-1}, et le premier tour de la partie décodage (DES^{-1}) de l'algorithme DES, incluant la permutation IP (le symbole ⊕ dénote le OU exclusif).



En particulier, il y a le calcul du cryptogramme *c* à la fin de DES:

$$C = IP^{-1}(\langle R_{16}, L_{16}\rangle) = IP^{-1}(\langle L_{15} \oplus f(R_{15}, K_{16}), R_{15}\rangle)$$

Et les calculs suivants pour la partie visible de DES^{-1}:

$$\langle L'_0, R'_0 \rangle = IP(C) \text{ et } \langle L'_1, R'_1 \rangle = \langle L'_0 \oplus f(R'_0, K'_1), R'_0 \rangle.$$

a. Montrez que $L'_0 = R_{16}$ et que $R'_0 = L_{16}$ (3pts).

b. Montrez que $L'_1 = L_{15}$ et que $R'_1 = R_{15}$ sous la condition que $K'_1 = K_{16}$ (3pts)

c. À partir de l'énoncé de la question b), que peut-on conclure sur les seize clés internes de 48 bits utilisées dans la partie d'encodage (DES^{-1}) (2pts)?

d. Expliquez la raison de l'absence de substitutions dans les seize tours de l'algorithme DES et de l'algorithme DES^{-1} si l'on exclut le calcul de *f*. (2pts)

Question 3 : RSA — 10pts

Voici une description de l'algorithme RSA :

Génération de la clé publique et de la clé privée:

1. Générer aléatoirement deux grands nombres premiers distincts p et q grossièrement de même taille.
2. Calculer $n = p * q$ et $\varnothing = (p-1) * (q-1)$.
3. Choisir un nombre entier e, $1 < e < \varnothing$, tel que et $\varnothing$ soient premiers entre eux , c'est à dire que $pgcd(e, \varnothing) = 1$.
4. Calculer l'unique entier d, $1 < d < \varnothing$ tel que $e * d \equiv 1 \pmod{\varnothing}$.

La clé publique est <n,e> et la clé privée est <n,d>.

Encodage par Bob d'un message m destiné à Alice:

5. Bob obtient la clé public <n,e> d'Alice.
6. Bob représente le message comme un entier $m \in [0,n-1]$.
7. Bob calcule $c = m^e \bmod n$.
8. Bob transmet le cryptogramme c à Alice

Décodage du cryptogramme par Alice :

9. Alice utilise sa clé privée <n,d>.
10. Alice calcule $m' = c^d \bmod n$.
11. Alice lit le message m'.

La courte preuve à la page suivante montre que le message lu par Alice m' correspond bien à celui encodé par Bob, c'est-à-dire que m' = m. Elle utilise la définition suivante :

> Si a et b sont des entiers, alors a est *congruent* à b *modulo* n, dénoté $a \equiv b \pmod{n}$, si n divise a−b. L'entier n est appelé le *modulo de la congruence*. Par exemple, $15 \equiv 7 \pmod{4}$ et remarquez que $15 \bmod 4 = 7 \bmod 4 = 3$.

Nous avons les propriétés suivantes :

P1 $a \equiv b \pmod{n}$ ssi a et b ont le même reste lorsque divisés par n.

P2 Si $a \equiv a_1 \pmod{n}$ et $b \equiv b_1 \pmod{n}$, alors $a + b \equiv (a_1 + b_1) \pmod{n}$ et $a \times b \equiv (a_1 \times b_1) \pmod{n}$

Pour n fixe, la relation *congruence modulo* n partitionne $\mathbb{Z}$ en classes d'équivalence.

Preuve que $m' = m$.

1	$e \times d = 1 + k\phi$ pour un entier k	par **4)**, $e \times d \equiv 1 \pmod{\phi}$
2	$m^{p-1} \equiv 1 \pmod{p}$	théorème de Fermat sous la condition que $\text{pgcd}(m, p) = 1$
3	$m^{(p-1)k(q-1)} \equiv 1^{k(q-1)} \pmod{p}$	élever à la puissance $k(q-1)$ de chaque côté de la congruence de l'étape 2 et **P2**
4	$m^{1+k(p-1)(q-1)} \equiv m \pmod{p}$	multiplier par m de chaque côté de la congruence de l'étape 3 et **P2**
5	$m^{1+k\phi} \equiv m \pmod{p}$	par **2)**, $\phi = (p-1) \times (q-1)$
6	$m^{e \times d} \equiv m \pmod{p}$	par de l'étape 1.

Si $\text{pgcd}(m, p) = p$, alors la congruence de l'étape 6 est encore valide puisque chaque côté est congruent à 0 modulo p, c'est-à-dire que $m^{e \times d} \equiv 0 \pmod{p}$ et $m \equiv 0 \pmod{p}$.

7	$m^{e \times d} \equiv m \pmod{q}$	répéter les étapes 2 à 6, mais avec q à la place de p et vice versa
8	$m^{e \times d} \equiv m \pmod{n}$	par **1)**, p et q sont premiers et $n = p \times q$
9	$(m^e)^d \equiv m \pmod{n}$	
10	$c \equiv m^e \pmod{n}$	par **9)** et **P1**
11	$c^d \equiv (m^e)^d \pmod{n}$	élever à la puissance d de chaque côté de la congruence de l'étape 10 et **P2**
12	$c^d \equiv m \pmod{n}$	par les étapes 9, 11 et symmétrie, transitivité des congruences

a. Terminez la preuve à partir de l'étape 12, c'est-à dire montrez que m' = m. Suggestion : utilisez P1. Toutes vos étapes doivent être justifiées. (2pts)

b. Est-ce que la somme (première partie du « alors ») ou la multiplication (deuxième partie du « alors ») de la propriété P2 qui est utilisée dans le point 4 de la preuve ? (2pts)

c. La condition pgcd(m,p) = 1 dans l'étape 2 de la preuve est nécessaire puisqu'elle est une hypothèse du théorème de Fermat. Mais, la condition pgcd(m,p) = p juste après l'étape 6 de la preuve est aussi considérée. Pourquoi? (2pts)

d. Pourquoi l'algorithme RSA est-il si efficace, c'est-à-dire difficile, voire impossible à briser, avec les technologies connues aujourd'hui? (2pts)

e. Peut-on envisager un jour où il sera possible de briser RSA? Justifiez votre réponse. (2pts)

Question 4 : Signature — 20pts

a. Remplissez les espaces blancs : la signature digitale assure (5 pts) :
   i. La non-répudiation.
   ii. _____
   iii. _____
   iv. _____

b. Expliquez comment Alice peut signer un message et l'envoyer à Bob à l'aide de Trent sous les contraintes suivantes (5pts) :

- Alice et Bob utilisent que des algorithmes symétriques.
- Trent est une personne de confiance.
- Trent partage une clé K_A avec Alice.
- Trent partage une clé K_b avec Bob.

_____
_____
_____
_____
_____
_____
_____
_____
_____

c. Expliquez en quoi l'utilisation des clés symétriques dans le cadre d'une signature digitale est qualifiée de contraignante. (5pts)

_____
_____
_____
_____

d. En utilisant la cryptographie asymétrique, expliquez le processus de la délégation de signature. (5pts)

Question 5 : Attaque 25pts

a. Décrivez les particularités des types d'attaques suivantes. *(10pts)*

- Direct access
- Probe/scan
- UDP spoofing
- Distributed denial of service (DDoS)
- IP spoofing
- Sniffing
- Buffer overflow
- Identity spoofing
- Man-in-the-middle

b. Identifiez (et expliquez pourquoi) parmi les attaques précédentes, celles qui:

b.1) sont le plus difficile à détecter. (*3pts*)

b.2) sont le plus facile à utiliser/réaliser. (*3pts*)

b.3) sont le plus fréquemment utilisées. (*3pts*)

b.4) ont le plus de conséquences/impacts. (*3pts*)

c. À quel niveau du modèle OSI retrouve-t-on les attaques «ARP-poisoning/ARP-spoofing»? (*3pts*)

Application
Presentation
Session
Transport
Network
Data Link
Physical

Question 6 : UQAM 25pts

On a décrit en classe l'attaque à l'UQAM de 2009. Dans cette attaque, on avait un scénario similaire à celui décrit dans la figure ci-dessous.

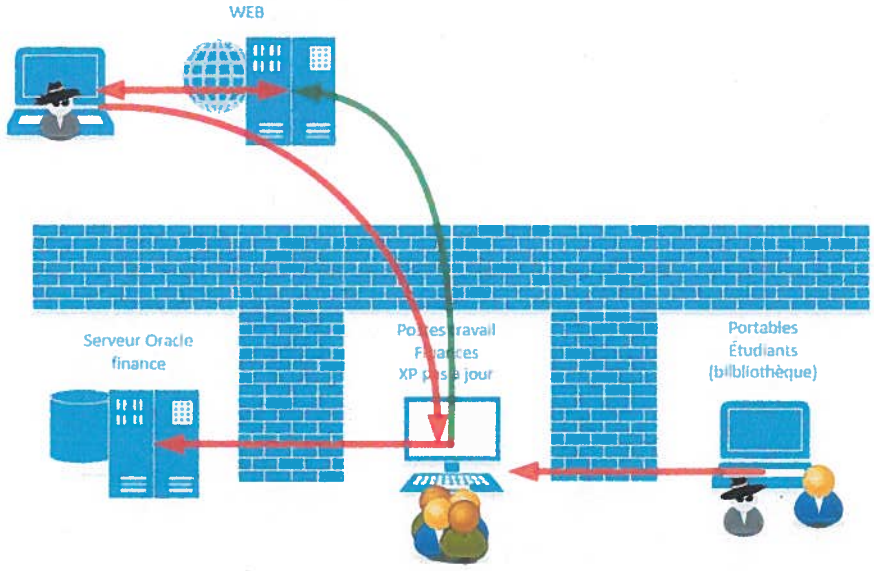


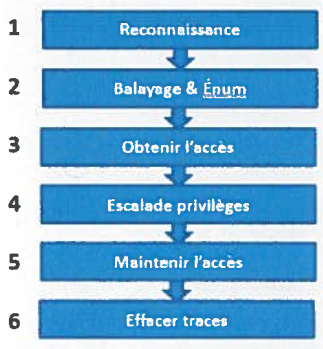
Figure 6.1 : Le «hacker» est parvenu à prendre le contrôle total d'un poste de travail aux finances, un Windows XP pas à jour. Depuis ce poste, il est parvenu à identifier le service de la base de données Oracle des finances (IP et port TCP). Par des tentatives répétées d'authentification à la base de données, il a entraîné la désactivation des pratiquement tous les comptes utilisateurs locaux dans le serveur de cette base de données.

a. Expliquez, en démontrant les techniques et principes d'attaque que vous avez acquis dans ce cours, comment l'attaque au poste de travail XP a pu réussir, compte tenu de la présence du firewall qui bloque les accès de l'externe. Examinez les flèches de la figure 4.1 pour vous laisser pister. (*10pts*)

   L'évaluation de votre réponse sera basée sur la compréhension des techniques et principes que vous saurez expliquer de manière claire. (*suite sur la page suivante*)
   Attention, souvent les explications courtes sont plus convaincantes que les longues! Attention, assurez-vous de décrire comment cette attaque a pu réussir en référant à des principes et techniques qui sont pertinents dans ce contexte! Soyez spécifique (ex. « j'ai utilisé metasploit » n'est pas suffisant et n'attribuera pas de point!)

b. Donnez un scénario d'attaque possible à partir du PC XP vers le serveur Oracle finances. (*10pts*)

c. Nommez au moins cinq pratiques d'attaques à adopter dans ce type de contexte (*5pts*)
Identifiez des pratiques en fonction des étapes du processus d'attaque de la figure suivante.
Figure 6.2) Étapes du processus d'attaque vues en cours.



Exemples de pratiques (*trouvez d'autres pratiques*) :

1) Installer un «sniffer» USB (matériel) sur le clavier d'un ordinateur d'administrateur réseau (étape 2/3 du processus d'attaque);
2) Utiliser *nmap* avec l'option «-T 5» afin de réduire sa visibilité au niveau de la détection des intrusions (système IPS, ou IDS) (étape 2 du processus d'attaque).

Fin de l'examen