



SUJET D'EXAMEN

Concours de Doctorat LMD 2019/2020

26/10/2019

Épreuve : Techniques cryptographiques

Filière : Informatique

Spécialité : Réseaux et Sécurité

Partie 1 :

1. Qu'est ce qui compose l'algorithme DES ? (1.5 pt)
2. Pour quelles raisons DES a-t-il été remplacé ? (1 pt)
3. Quels sont les propriétés principales des fonctions de hachage ? (1.5 pt)
4. Dans les différents systèmes, les clés ont des rôles particuliers. Par exemple, une clé secrète est le lien entre différents acteurs qui assure la confidentialité. Quels rôles jouent les autres types de clés ? (1 pt)
5. Quel est le nom du standard utilisé couramment pour les certificats de clés publiques ? Quel est le contenu général d'un certificat ? (1.5 pt)
6. Trouver le chiffrement de M : LESMAISONSBLANCHES par un chiffrement de Vigenère avec la clé SECURITE. Qu'est-ce se passe aux fréquences des caractères dans un texte chiffré avec un chiffrement de Vigenère ? (1,5 pt)



SUJET D'EXAMEN

Concours de Doctorat LMD 2019/2020

Epreuve : Cryptographie

Date : 26/10/2019

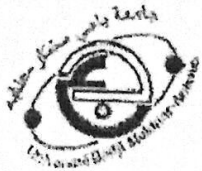
Filière : Informatique

Spécialité : Réseaux et sécurité Informatique (RSI)

Partie 2 (6 points):

L'algorithme RSA est le premier algorithme de chiffrement asymétrique proposé, sa sécurité repose sur la difficulté de factoriser un entier.

- 1) Décrivez les étapes à suivre pour générer le couple de clefs (clef publique, clef privée) dans l'algorithme de chiffrement RSA.
- 2) Si on souhaite déchiffrer un message M chiffré avec la clef publique (e, n) . Comment peut-on factoriser n .
- 3) Sachant que $n = 11 \times 13$, calculer la clef privée associée à la clef publique $(103, 143)$



SUJET D'EXAMEN

Concours de Doctorat LMD 2019/2020

26/10/2019

Epreuve : Techniques Cryptographiques

Filière : Informatique

Spécialité : Réseaux et Sécurité

Partie 3 : (6pt) : Soit le protocole cryptographique suivant :

$I \rightarrow S : ID_i \parallel ID_r \parallel N_1$
$S \rightarrow I : \{ID_i \parallel ID_r \parallel N_1 \parallel K_{ir}\}_{K_i} \parallel \{ID_i \parallel K_{ir}\}_{K_r}$
$I \rightarrow R : \{ID_i \parallel K_{ir}\}_{K_r}$
$R \rightarrow I : \{N_2\}_{K_{ir}}$
$I \rightarrow R : \{f(N_2)\}_{K_{ir}}$

Note: I (Initiateur); R (Répondeur); S(Serveur)

1. Quel est le rôle de ce protocole, expliquez brièvement son déroulement ?
2. Quel est le type de faille dans ce protocole ?
3. Décrivez un scénario d'attaque contre ce protocole.
4. Proposer une solution permettant de résoudre cette faille.
5. Donnez deux outils de vérification formelle qui servent à dégager les failles existantes dans les protocoles cryptographiques.
6. On dit qu'un protocole communication est sécurisé, s'il résiste à plusieurs types d'attaques et les clés utilisées satisfaites plusieurs propriétés de sécurité. Citez deux propriétés de sécurité.