

Durée : 3h

Niveau: Licence professionnelle Réseaux et Télécoms

EPREUVE DE CRYPTOGRAPHIE

Exercice 1: Question de cours (5,5pts)

1. Qu'est-ce qu'un certificat numérique? Donner deux exemples d'information qu'on y trouve.
2. Donner deux raisons qui peuvent provoquer la révocation d'un certificat.
3. Quelles sont les propriétés d'une fonction de hachage? Citer deux exemples de fonction de hachage en précisant pour chacune d'elles la taille de l'empreinte.
4. Quel est le principal inconvénient des algorithmes symétriques? Citer les deux classes de chiffrement symétrique.
5. Donner les principaux avantages et inconvénients des algorithmes asymétriques.

Exercice 2: Chiffrement affine (6pts)

1. Voici un texte chiffré obtenu avec la clé H:

SLJHT LYVBU HKLJY VJOLB ULWSH JLLUO
HSALY VWOPS PLWVB YSLZQ LBEVS FTWPX
BLZ

Retrouvez le texte clair.

2. Voici un texte chiffré dont on ne connaît pas la clef utilisée:

Retrouvez le texte clair

WLNST YPAZC EPWPO PFTWO PDGTN ETXPD
OFDPT DXF

Exercice 3: Vigenère (2,5pts)

1. On considère le message suivant: « la bagarre ne fait que commencer »
En utilisant la méthode de chiffrement de vigenère, on obtient le message:
« xa mettveh hq flmg jyr fimprpxv »
Retrouvez la clef.

Exercice 4: Signature RSA (6pts)

1. Que signifie le sigle RSA ?
2. Calculer le module n et l'entier $\varphi(n)$ associés aux nombres $p=19$ et $q=53$
3. Quel est l'exposant secret de signature d associé à $e=17$?
4. Quelle est la signature de $m=10$? Vérifier cette signature
5. Quel est le chiffré de $m'=66$? Vérifier le résultat obtenu en le déchiffrant