Université Guelma
Département Informatique
3 ISIL & SI
Année Universitaire : 2020/2021 **Dr. M. A. Ferrag**

TD 2. Sécurité Informatique

Pour chaque description ci-dessous, indiquez le terme (<4 mots) qui la décrit le mieux.

Question 1. Cela garantit que les données ne peuvent être lues que par le récepteur prévu.

Question 2. Cela garantit que toute modification des données est détectée par le récepteur prévu.

Question 3. Cela garantit que les données reçues ont été envoyées par l'expéditeur spécifié.

Question 4. Cela garantit qu'un tiers peut vérifier que les données ont été envoyées par l'expéditeur spécifié.

Question 5. Ce type de crypto utilise différentes clés pour le cryptage et le décryptage.

Question 6. The attack model in which the attacker has access to an encryption oracle but not a decryption oracle.

Question 7. Ce chiffrement par blocs symétriques prend en charge une seule taille de clé.

Question 8. Ce chiffrement par blocs symétriques prend en charge plusieurs tailles de clé.

Question 9. Propriété d'une fonction de hachage qui rend difficile la recherche d'un message m haché sur un nombre donné.

Question 10. C'est l'ensemble des entiers en 1; ...; n - 1 qui sont relativement premiers à n.

Question 11. C'est le nombre d'entiers dans 1; ...; n - 1 qui sont relativement premiers à n.

Question 12. Une attaque qui passe par un ensemble de mots de passe candidats.

Question 13. Cela signifie qu'après qu'une clé de session a été oubliée par les principaux qui l'ont utilisée, personne ne peut déchiffrer les données chiffrées avec cette clé.

Question 14. Alice a un compte sur un serveur. Le serveur lui fait changer son mot de passe tous les quelques mois, auquel Alice incrémente simplement un nombre dans son mot de passe, par exemple, pwd1, pwd2,. Pourquoi le serveur ne se plaint-il pas que le nouveau mot de passe ressemble beaucoup à son ancien?

Question 15. Soit $[e;\ n]$ être la clé publique RSA d'un serveur. Supposons que quelqu'un vous donne les facteurs premiers de n, disons p et q. Pouvez-vous obtenir la clé privée $[d;\ n]$? Sinon, expliquez brièvement. Si oui, indiquez brièvement les étapes.

Question 16. Une fonction de hachage H () génère un hachage de 256 bits. Combien de messages aléatoires en moyenne faudrait-il hacher avant de trouver deux messages distincts hachés à la même valeur.

Question 17. Un mot de passe fort est nettement meilleur qu'un mot de passe faible contre une attaque par dictionnaire en ligne. Expliquer brièvement

Question 18. Un mot de passe fort est nettement meilleur qu'un mot de passe faible contre une attaque par dictionnaire hors ligne. Expliquer brièvement.

Question 19. Protocoles d'authentification

$[sk_A; pk_A]$ Alice's public-key pair. Bob has pk_A.
$[sk_B; pk_B]$ Bob's public-key pair. Alice has pk_B.
$E_P(pk; x)$ public-key encryption of x with public key pk
Sgn(sk; x) public-key signing of x with secret key sk
E(s; x) symmetric-key encryption of x in CBC mode using AES with key s
D(s; x) symmetric-key deryption of x in CBC mode using AES with key s
MAC(s; x) symmetric-key MAC (ECBC) of x using key s
H(x) SHA-256 hash function of x
HMAC(k; x) HMAC of x using key k and H

A: generate a new symmetric key s send $[E_P(pk_B; s); E(s;m);Sgn(sk_A;H(m))]$	B: receive message extract m

- Analysez la confidentialité, l'intégrité, l'authenticité et la non-répudiation.