Exercice N° 01: *(Concepts mathématiques)*

- Appliquer le test de Fermat sur p=11, avec a=2 et a=3.
- Calculer Φ (19), Φ (21), Φ (8)
- Calculer 5^{13} mod 71 en utilisant l'algorithme d'exponentiation rapide.

Exercice N° 02: *(Chiffrement RSA)*

Soit p = 7 et q= 19

1. Décrire le schéma de génération de clés, schéma de chiffrement, et schéma de déchiffrement.
2. Montrer que $D_{Kpv}(E_{Kpb}(m)) = m$.
3. Calculer N et Φ (n).
4. On propose e = 5. Calculer la clé privée d.
5. Chiffrer le message clair m =6.
6. Déchiffrer le message chiffré c= 62.

Exercice N°03: *(Protocole Diffie-Hellman)*

1. Quel est le but du protocole Diffie-Hellman ?
2. Déterminer la clé de session Diffie-Hellman, si Alice communique à Bob les nombres g = 3 et p = 23. Sachant qu'Alice tire le nombre aléatoire a = 5 et Bob le nombre b = 7 ?
3. Expliquez les faiblesses de protocole Diffie-Hellman.
4. Proposer un scenario d'attaque de type MITM.

Exercice N°04: (*Fonctions de hachage*)

1. Quelles sont les propriétés qui doivent vérifier les fonctions de hachage ?
2. Donnez des exemples d'applications des fonctions de hachage
3. Quelle est la différence entre la fonction de type MDC et HMAC.
4. Parmi ces fonctions de hachage lesquelles sont sûres : MD-5, SHA-3, SHA-1, SHA-512.
5. Pour quelle raison une fonction de hachage constitue-t-elle un meilleur moyen de vérifier l'intégrité qu'une somme de contrôle tel que le *checksum Internet* ?