AL 5 ppa - Cryptographie - Contrôle continu

Nom : _____

Prénom : _____

- Durée : 1 heure 30. Documents interdits, calculatrices interdites.
- Écrivez toutes les réponses directement sur le sujet. Si vous n'avez pas suffisamment de place, écrivez au dos d'une feuille en le **précisant dans la question**.

1 Vigenère (6 points)

N'oubliez pas pour les questions suivantes que le A dans une clé correspond à un décalage d'une lettre.

1. [3 points] Chiffrez le message MESSAGE avec la clé KP en utilisant la méthode de Vigenère

   Solution: XUDILWP

2. [3 points] Déchiffrez le message CKOIP, chiffré avec la clé AB

   Solution: BINGO !

2 RSA (14 points)

1. [1 point] Posons $n = 35$. Déterminez $\phi(n)$.

   Solution: $\phi(n) = \phi(35) == \phi(5 \times 7) = \phi(7)\phi(5) = 6 \times 4 = 20$

2. [1 point] Calculer $pgcd(20, 15)$ en utilisant l'algorithme Euclide.

   Solution: $pgcd(20, 15) = pgcd(15, 5) = pgcd(5, 0) = 5$

3. [1 point] Pourquoi ne peut-on pas utiliser $(15, 35)$ comme clé publique RSA ?

Solution: Parce que l'exposant de chiffrement et $\phi(n)$ doivent être premiers entre eux.

4. [2 points] Prenons $(7, 35)$ comme clé de chiffrement. Chiffrez le message $M = 8$. Nous noterons M' le message chiffré.

Solution: $M' = 8^7 \equiv (8^2)^3 \times 8 \equiv (64)^3 \times 8 \equiv (-6)^3 \times 8 \equiv 22 \equiv (-6)^2 \times (-6) \times 8 \equiv 36 \times (-6) \times 8 \equiv 1 \times (-48) \equiv (70 - 48) \equiv 22 \pmod{35}$

5. [2 points] Déterminer l'exposant de déchiffrement utilisant l'algorithme d'Euclide étendu.

Solution: Solution avec gmp...

```
20 = 7 * 2 + 6
7 = 6 * 1 + 1
6 = 1 * 6 + 0
-----------------------------------------
1 * (1) + 0 * (0) = 1
-----------------------------------------
1 * (1) + (6 - 1 * 6 ) * (0) = 1
6 * (0) + 1 * (1) = 1
-----------------------------------------
6 * (0) + (7 - 6 * 1 ) * (1) = 1
7 * (1) + 6 * (-1) = 1
-----------------------------------------
7 * (1) + (20 - 7 * 2 ) * (-1) = 1
20 * (-1) + 7 * (3) = 1
```

L'exposant de déchiffrement est 3.

6. [1 point] Vérifiez que l'exposant de déchiffrement est bien l'inverse de 7 dans $Z/20Z$.

Solution: $7 \times 3 \equiv 21 \equiv 1 \pmod{20}$, ok.

7. [2 points] Déchiffrez le message 22 avec votre clé privée.

Solution: $22^3 \equiv (-13)^2 \times 22 \equiv (13)^2 \times 22 \equiv (10+3)^2 \times 22 \equiv (100+60+9) \times 22 \equiv (-5-10+9) \times 22 \equiv (-6) \times (-13) \equiv 78 \equiv 8 \pmod{35}$

8. [3 points] La clé publique d'une personne que vous n'appréciez pas est $(27, 55)$. Déterminez sa clé privée.

Solution: Pour commencer on a $\phi(55) = \phi(5 \times 11) = 4 \times 10 = 40$. Ensuite calculons l'inverse de 3 modulo 55. Comme $111 = 2 \times 55 + 1$ et $27|111$, alors $111 = 3 \times 27$ et 3 est l'exposant de déchiffrement. La clé privée de la cible est $(3, 55)$.

9. [1 point] Cette personne a reçu le message 12, déchiffrez-le.

Solution: $12^3 \equiv 12^2 \times 12 \equiv 144 \times 12 \equiv 34 \times 12 \equiv 340 + 68 \equiv 10 + 13 \equiv 23 \pmod{55}$.