



INSTITUT SAINT JEAN

Tél : (+237) 657 07 98 07
(+237) 651 36 96 96
B.P : 749 Yaoundé Cameroun
Email : info@institutsaintjean.org
www.institutsaintjean.org

Contrôle Continu

Classe : ISJ M1

Epreuve de : INTRODUCTION A LA CRYPTOLOGIE

Durée : 2h30

Examinateur : Dr EKODECK Stéphane G. R.

Année académique : 2024-2025

Semestre : 2

Vous êtes autorisés à répondre dans la langue de votre choix entre le Français et l'Anglais.

Aucun support autorisé.

Problème 1 : Arithmétique modulaire (10 points)

- Q1. Calculer $7^4 \bmod 11$.
- Q2. Trouver l'inverse de 11 modulo 26 en utilisant l'algorithme d'Euclide étendu.
- Q3. Résoudre l'équation $17x \equiv 5 \bmod 26$.
- Q4. Calculer $\varphi(45)$, où φ est la fonction indicatrice d'Euler.
- Q5. Démontrer, par un exemple numérique, le petit théorème de Fermat avec $a = 3$ et $p = 7$.
- Q6. Résoudre le système :

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 2 \bmod 7 \end{cases}$$

- Q7. Déterminer tous les entiers x tels que $x^2 \equiv 1 \bmod 35$.
- Q8. Montrer que si a et n sont premiers entre eux, alors $a^{\varphi(n)} \equiv 1 \bmod n$ (exemple numérique avec $a = 4$, $n = 15$).
- Q9. Trouver la plus petite solution positive de $23x \equiv 7 \bmod 31$.
- Q10. Soient $a = 18$ et $n = 77$. Vérifier si a est inversible modulo n , et donner son inverse s'il existe.

Problème 2 : Cryptographie classique (11 points + 3 points bonus)

Partie A – Chiffrement et déchiffrement (11 points)

- Q1. Énoncer le principe de Kerckhoff.
- Q2. Chiffrer le mot **CLEF** avec un chiffre de César de clé +5.
- Q3. Déchiffrer le texte **KHOOR** chiffré avec une clé César de +3.
- Q4. Chiffrer le mot **MESSAGE** avec le mot-clé Vigenère **CODE**.
- Q5. Déchiffrer le texte **XQHNM** chiffré avec Vigenère et le mot-clé **CLE**.

- Q6. Chiffrer **BONJOUR** avec le chiffre affine $E(x) = 3x + 7 \pmod{26}$.
- Q7. Déchiffrer **HZDU** avec le chiffre affine $E(x) = 5x + 8 \pmod{26}$.
- Q8. Utiliser une grille Playfair avec mot-clé **SECRETS** pour chiffrer le message **PLAYNFAIR**.
- Q9. Chiffrer le mot **HELLO** avec une matrice Hill 2×2 : $A = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$.
- Q10. Déchiffrer le mot **IFMIMP** chiffré avec un César de +1.
- Q11. Retrouver le texte clair si **NEXUS** a été chiffré avec une clé César de -3.

Partie B – Cryptanalyse (3 points)

Le texte suivant a été chiffré avec un chiffre affine. La langue du message est le français :

XI KBUZHXYHDSXK JZIXIHGXQ LZAXZMQ VIC QMDXXZTM XQZBPZLZK. MZXX JMDZAG
ZASXAJ LZAX QMD ZKHTXZDZAXQ MZQ QMD ZMDXXZGZAXQ.

Informations utiles :

- Lettres fréquentes en français : E, A, S, I, N, R, T
- Digrammes fréquents : ES, LE, DE, EN, RE, ON
- Tentez de déterminer la lettre la plus fréquente dans le texte chiffré.
- Supposez qu'elle correspond à E, et identifiez une clé affine (a, b) plausible.
- Retrouver le texte clair en inversant le chiffrement affine.