Examen terminal de MAT239 (2 heures)

Documents et calculatrices interdits. Les téléphones portables doivent rester éteints.

Question 1.

Soit le nombre premier $p = 257$.

1. *Question de cours :* Rappeler brièvement le protocole de Diffie-Hellmann. Quel est son intérêt ?
2. Alice, Bob et Eve décident d'utiliser p et $g = 60$ pour initier le protocole de Diffie-Hellmann.
   (a) Alice choisit l'exposant secret 5 et Bob l'exposant secret 9. Que s'échangent-ils sur le canal, et quel est leur secret partagé à l'issue du protocole ? Faire tous les calculs.
   Charlie qui observe les échanges, peut-il en déduire des informations ?
   (b) Est-ce que 60 est une racine primitive de p ?
   (c) Eve choisit l'exposant secret 32 pour initier le protocole de Diffie-Hellmann avec Bob (celui-ci garde le même exposant secret que précédemment). Que s'échangent-ils sur le canal et quel est leur secret partagé à l'issue du protocole ? Faire tous les calculs.
   Charlie observe les échanges, peut-il en déduire des informations ?
3. La situation aurait-elle été différente si Alice, Bob et Eve avaient pris p et $g = 101$ pour initier le protocole ? Justifier en détail votre réponse et détailler tous vos calculs.
4. S'inspirer du protocole de Diffie-Hellman pour construire un protocole permettant à Alice, Bob et Eve de convenir, sans communication préalable, d'un secret S commun entre eux. Les communications se font sur un canal non confidentiel, mais protégé contre les attaques actives (interception, insertion de message et impostures).

Question 2.

Pour envoyer un message à Alice, Bob utilise le protocole suivant : il attribue une valeur numérique à chaque lettre de son message ($A = 1, B = 2, \dots$) , encrypte chacun des nombres entre 1 et 26 ainsi obtenus à l'aide de la clé publique RSA d'Alice puis les transmet à Alice.
Par exemple, pour chiffrer NON avec la clé $(10001, 257)$, il remplace N par 14 et O par 15, calcule $14^{257} = 8435 \mod 10001$ et $15^{257} = 4570 \mod 10001$, puis envoie 8435 4570 8435. Que pensez-vous de la sécurité de ce protocole ?

Question 3. Au début de l'informatique (IBM 7070 par exemple), une case mémoire était représentée par une série de cinq ampoules. Pour repérer facilement les erreurs, on imposait que exactement deux des cinq ampoules soient toujours allumées.

1. Expliquer pourquoi ceci peut être considéré comme un code détecteur d'erreurs.
2. Combien de mots ce code possède-t-il ? Enumérer tous les mots du code.
3. Combien d'erreurs peut-on détecter ? corriger ?
4. Est-ce un code linéaire ? polynomial ?

Question 4.

Soit C un code linéaire de matrice génératrice $G = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$

1. Donner une matrice génératrice standard et une matrice de contrôle de C.
2. Le code C est-il polynomial ? cyclique ?
3. Construire la liste des syndromes pour ce code.
4. Donner la distance minimale $d(C)$ de ce code.
5. Coder systématiquement les mots suivants : 0011, 0110, 0101.
6. Corriger éventuellement et décoder chacun des mots reçus suivants : 0100101, 0111010, 1101010.

Question 5. On s'intéresse à un code polynomial $C \subset \mathbb{F}_2^n$ de polynôme générateur $g(X) = X^5 + X^4 + X^2 + 1$ et on souhaite transmettre des mots binaires de longueur 4 avant codage ($p = 4$).

1. Quelle est la longueur n des mots du code correspondant ?
2. Coder le mot à transmettre $M = 1011$.
3. Construire la matrice génératrice G du code. Est-ce un code systématique ? Est-ce un code cyclique ? Justifiez vos réponses.