Mathématiques et technologie

Examen final – hiver 2025

Faculté des arts et des sciences – Département de mathématiques et de statistique

Enseignant : Jonathan Godin
Sigle : MAT2450A
Date : Vendredi le 25 avril 2025

/66

L'examen dure 170 minutes. Vous avez droit au livre du cours (en papier ou en pdf) et à vos notes personnelles. Vous pouvez utiliser un ordinateur (sans Internet) ou une tablette, mais pas un téléphone. La calculatrice est permise. **Justifiez vos réponses.**

Question 1. On veut utiliser le code de Hamming $C(7,4)$ avec la matrice de contrôle H suivante

$$H = \begin{pmatrix} a & 1 & 0 & 1 & 1 & 0 & b \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix},$$

où $a, b \in \{0,1\}$ sont des inconnues. Soit $w = (1,0,1,0,0,1,0)$ un message encodé reçu. Les parties a), b) et c) sont indépedantes, mais elles utilisent toutes le même H et w.

(3pts) a) On suppose que w possède exactement une erreur. Trouver a et b dans ce cas.

(3pts) b) On suppose que w ne possède aucune erreur. Trouver a et b dans ce cas.

(6pts) c) On suppose que $a = 1$ et $b = 0$. Trouver la matrice de contrôle G associé à H. Ensuite, pour le message reçu w, décoder *en utilisant* la matrice G pour obtenir le message de départ $u \in \mathbb{F}_2^4$.

Question 2. Afin de recevoir des messages encryptés, Bob prépare les clés publics et privés : il choisit p, q des nombres premiers, il calcule $\varphi(n) = (p-1)(q-1)$, il choisit $e \in \{1, \ldots, n-1\}$ avec $\text{pgcd}\big(e, \varphi(n)\big) = 1$, il calcule d avec $ed \equiv 1 \pmod{\varphi(n)}$. Le a) et le b) sont indépendants.

(9pts) a) Bob rend n et e public. Supposons qu'une personne malveillante réussise à calculer $\varphi(n)$. Cette personne peut-elle casser le code de Bob ? Si oui, expliquer comment. Sinon, expliquer pourquoi.

(12pts) b) Bob rend n public comme d'habitude, mais il se trompe et rend d public, plutôt que e (donc e est considéré comme étant privé pour cette partie).

i) Le code fonctionne-t-il toujours ? C'est-à-dire si Alice encrypte son message m en utilisant n et d (elle calcule donc $m^d \pmod{n}$), Bob pourra-t-il décrypter son message ?

ii) Le code est-il sécuritaire ? Autrement dit, une personne malveillante pourrait-elle décrypter le message d'Alice ?

(Suite au verso)

Question 3. On utilise un générateur de nombres aléatoires linéaire congruentiel avec $p = 7$.

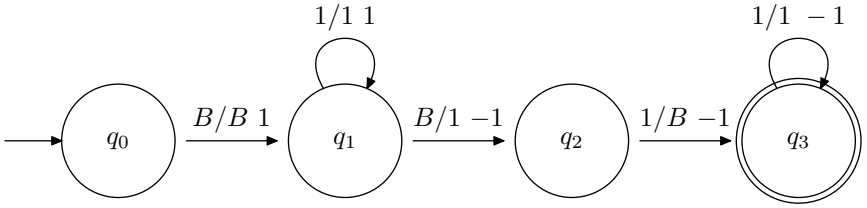
(6pts) a) Montrer que $a = 5$ est une racine primitive.

(6pts) b) Expliquer comment on peut utiliser ce générateur, avec $p = 7$ et $a = 5$, pour générer aléatoirement un nombre $n \in \{0, 1, 2, 3\}$. Les nombres $0, 1, 2, 3$ ont-ils tous la même probabilité d'être choisi ?

Question 4. Les questions a), b) et c) sont indépendantes.

(6pts) a) Soit $g(x) = 5x$ et $h(x, y, z) = z + 2$. Identifier la fonction $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ obtenue par récurrence de base g et de pas h.
(Précision : trouvez une formule pour f ; il n'est pas nécessaire de faire une preuve par récurrence, mais expliquez bien votre raisonnement.)

(6pts) b) On considère le programme suivant



Appliquer ce programme au ruban q_0B111B en indiquant, à chaque étape intermédiaire, l'état du ruban. (Chaque étape devrait indiquer dans quel état est la machine et où pointe le pointeur, p.ex. Bq_1111B.)

(9pts) c) Écrire une machine qui calcule la fonction $f(x) = (x - 2, 2)$ pour $x \geq 2$. P.ex. pour $x = 3$, la machine part dans l'état $q_0B1111B$ et se termine dans l'état $q_fB11B111B$. Expliquer aussi en mot ce que votre machine fait.