NOM :

GROUPE :

Vannes iut : Université Bretagne Sud

R3.09 - Cryptographie et sécurité
Contrôle Terminal

Université Bretagne Sud ubs :

Nom du responsable :	A. Ridard
Date du contrôle :	Mercredi 19 octobre 2022
Durée du contrôle :	1h30
Nombre total de pages :	4 pages
Impression :	A4 recto-verso agrafé (1 point)
Documents autorisés :	A4 recto-verso manuscrit
Calculatrice autorisée :	Oui
Réponses :	Directement sur le sujet

Exercice 1. (4)

1. En utilisant **l'algorithme d'Euclide étendu**, déterminer $pgcd(255, 141)$ et une identité de Bézout.

k	r_k	u_k	v_k	q_k	div. euclid.
0	255	1	0		
1	141	0	1	1	$255 = 141 \times 1 + 114$
2	114	1	-1	1	$141 = 114 \times 1 + 27$
3	27	-1	2	4	$114 = 27 \times 4 + 6$
4	6	5	-9	4	$27 = 6 \times 4 + 3$
5	3	-21	38	2	$6 = 3 \times 2 + 0$
6	0				

Conclusion :

- $pgcd(255, 141) = 3$ 1
- $3 = -21 \times 255 + 38 \times 141$ 1

2. (a) Décomposer en facteurs premiers 120 et 252.

$120 = 2^3 \times 3 \times 5$ 0,5

$252 = 2^2 \times 3^2 \times 7$ 0,5

(b) En déduire le pgcd et le ppcm de 120 et 252.

$pgcd(120, 252) = 2^2 \times 3 = 12$ 0,5

$ppcm(120, 252) = 2^3 \times 3^2 \times 5 \times 7 = 2520$ 0,5

Exercice 2. (6)

1. Dresser la table de multiplication de $\mathbb{Z}/8\mathbb{Z}$.

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

1

2. Résoudre les équations suivantes **modulo 8** :

(a) $5x+2 \equiv 4$

$5x+2 \equiv 4 \iff 5x \equiv 4-2$

$\iff 5x \equiv 2$

$\iff x \equiv 5^{-1} \times 2$

$\iff x \equiv 5 \times 2$ d'après la table

$\iff x \equiv 2$

1

$\mathcal{S} = \{m \in \mathbb{Z} \mid m \equiv 2 \bmod 8\} = \{2+8k, k \in \mathbb{Z}\}$

Dans $\mathbb{Z}/8\mathbb{Z}$, $\mathcal{S} = \{\bar{2}\}$.

(b) $6x-3 \equiv 0$

$6x-3 \equiv 0 \iff 6x \equiv 3$

D'après la table de multiplication de $\mathbb{Z}/8\mathbb{Z}$, on a :

$\mathcal{S} = \emptyset$.

1

(c) $2x-6 \equiv 6$

$2x-6 = 6 \iff 2x \equiv 6+6$

$\iff 2x \equiv 4$

$\iff x \equiv 2$ ou $x \equiv 6$ d'après la table

$\mathcal{S} = \{\overline{2}, \overline{6}\}$.

1

(d) $x^2-6 \equiv 3$

$x^2-6 \equiv 3 \iff x^2 \equiv 3+6$

$\iff x^2 \equiv 1$

$\iff x \equiv 1$ ou $x \equiv 3$ ou $x \equiv 5$ ou $x \equiv 7$ d'après la table

$\mathcal{S} = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$

1

(e) $x^2-2x+1 \equiv 4$

$x^2-2x+1 \equiv 4 \iff (x-1)^2 \equiv 4$

$\iff x-1 \equiv 2$ ou $x-1 \equiv 6$ d'après la table

$\iff x \equiv 3$ ou $x \equiv 7$

$\mathcal{S} = \{\overline{3}, \overline{7}\}$.

1