SR 5 PPA - Cryptographie - Contrôle continu numéro 2

Nom : _____

Prénom : _____

- Durée : 1 heure 30. Documents interdits, calculatrices interdites.
- Ecrivez 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 Question de cours (3 points)

1. [1 point] Pourquoi n'est-il pas intelligent d'utiliser des nombres à virgule flottante pour faire des calculs cryptographiques ?

   **Solution:** Parce que la perte de précision engendrée par un dépassement de capacité de la mantisse fausserait les résultats.

2. [1 point] Rappelez les deux premières règles d'or du cryptographe.

   **Solution:** Le message doit pouvoir tomber entre les mains de l'ennemi sans pouvoir être lu. L'algorithme doit pouvoir être connu de tous sans que sa sécurité soit compromise.

3. [1 point] Quelles sont les limites de la cryptographie sans clé ?

   **Solution:** La secret de l'algorithme doit être bien tenu. Et il ne faut pas utiliser le même pour communiquer avec des personnes différentes.

# 2 Arithmétique (5 points)

1. [1 point] Décomposez 392 en produit de facteurs premiers.

   **Solution:** $392 = 2^3 \times 7^2 = (3, 0, 0, 2)$

2. [2 points] Donnez dans l'ordre croissant, la liste des diviseurs positifs de 392

| Diviseurs de 392 |
|---|
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |

**Solution:** Comme $392 = 2^3 \times 7^2$ la liste des diviseurs est

| Diviseurs de 392 | |
|---|---|
| $2^0 \times 7^0 =$ | 1 |
| $2^1 \times 7^0 =$ | 2 |
| $2^2 \times 7^0 =$ | 4 |
| $2^3 \times 7^0 =$ | 8 |
| $2^0 \times 7^1 =$ | 7 |
| $2^1 \times 7^1 =$ | 14 |
| $2^2 \times 7^1 =$ | 28 |
| $2^3 \times 7^1 =$ | 56 |
| $2^0 \times 7^2 =$ | 49 |
| $2^1 \times 7^2 =$ | 98 |
| $2^2 \times 7^2 =$ | 196 |
| $2^3 \times 7^2 =$ | 392 |

3. [2 points] Donner, dans l'ordre croissant, tous les nombres de $\{0, 1, \ldots, 35\}$ qui ne sont pas premiers avec 35.

| Nombres non premiers avec 35 |
|---|
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |

**Solution:**

| Nombres non premiers avec 35 |
|---|
| 0 |
| 5 |
| 7 |
| 10 |
| 14 |
| 15 |
| 20 |
| 21 |
| 25 |
| 28 |
| 30 |
| 35 |

# 3 Pgcd (6 points)

1. [1 point] Donnez la relation mathématique sur laquelle est construit l'algorithme d'Euclide.

   **Solution:** $pgcd(a, b) = pgcd(b, a \ mod \ b)$ si $b \neq 0$, et $pgcd(a, 0) = a$.

2. [2 points] Calculez $pgcd(38, 23)$ avec l'algorithme d'Euclide

   **Solution:** $pgcd(38, 23) = pgcd(23, 15) = pgcd(15, 8) = pgcd(8, 7) = pgcd(7, 1) = pgcd(1, 0) = 1$

3. [2 points] Calculez $pgcd(72, 53)$ avec l'algorithme d'Euclide

   **Solution:** $pgcd(72, 53) = pgcd(53, 19) = pgcd(19, 15) = pgcd(15, 4) = pgcd(4, 3) = pgcd(3, 1) = pgcd(1, 0) = 1$

4. [1 point] Soit $au + bv = 1$ une solution particulière d'une équation d'inconnues $u$ et $v$ dans l'ensemble des entiers relatifs. Donnez la solution générale de cette équation.

   **Solution:** Pour tout $k$, $a(u + kb) + b(v - ka) = 1$

# 4 Algorithme d'Euclide étendu (6 points)

Complétez les deux tableaux ci-dessous :

1. 3 points

| $a$ | $b$ | $q$ (quotient) | $r$ (reste) | $u$ | $v$ |
|---|---|---|---|---|---|
| 88 | 64 | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | 1 |

**Solution:**

| $a$ | $b$ | $q$ | $r$ | $u$ | $v$ |
|---|---|---|---|---|---|
| 88 | 64 | 1 | 24 | $-5$ | 7 |
| 64 | 24 | 2 | 16 | 2 | $-5$ |
| 24 | 16 | 1 | 8 | $-1$ | 2 |
| 16 | 8 | 2 | 0 | 1 | $-1$ |
| 8 | 0 | | | 1 | 1 |

2. 3 points

| $a$ | $b$ | $q$ (quotient) | $r$ (reste) | $u$ | $v$ |
|---|---|---|---|---|---|
| 70 | 27 | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | 0 |

**Solution:**

| $a$ | $b$ | $q$ | $r$ | $u$ | $v$ |
|---|---|---|---|---|---|
| 70 | 27 | 2 | 16 | $-5$ | 13 |
| 27 | 16 | 1 | 11 | 3 | $-5$ |
| 16 | 11 | 1 | 5 | $-2$ | 3 |
| 11 | 5 | 2 | 1 | 1 | $-2$ |
| 5 | 1 | 5 | 0 | 0 | 1 |
| 1 | 0 | | | 1 | 0 |