Janvier 2016

NOM :
Prénom :
Groupe :

Examen

Cryptologie

- *La calculatrice est autorisée.*
- *Documents et tout moyen de communication sont prohibés.*
- *Ce document est composé du sujet de l'examen ainsi que du support de réponse.*
- *Il ne s'agit en aucun cas d'une feuille de brouillon.*
- *Vous êtes autorisé à pleurer (en silence).*
- *Assurez-vous de ne pas laisser tomber vos larmes sur la copie.*
- *Position fœtale permise.*

Exercice 1

10 min

1. Cette égalité définie-t-elle une division euclidienne $10 = 2 \times 3 + 4$. Justifier (si c'est le cas, donner le dividende, le diviseur, le quotient et le reste). 0.5

2. Cette égalité définie-t-elle une division euclidienne $5 = 2 \times 2 + 1$. Justifier (si c'est le cas, donner le dividende, le diviseur, le quotient et le reste). 0.5

3. Donner la fonction de déchiffrement du cryptosystème de César par paquet de 2 de clef 1234. 0.5

Exercice 2

30 min

Donner le reste de la division euclidienne de A par B.

1. $A = 555$, $B = 12$ 0.5

2. $A = 3078$, $B = 487$ 0.5

3. $A = 123^{122}$, $B = 124$ 0.5

4. $A = 2^{1147}$, $B = 7$ 1

5. $A = 133^{39}$, $B = 10$ 1

Exercice 3

10 min

Déterminer $\mathrm{PGCD}(2016, 233)$. A cette fin, appliquer l'algorithme d'Euclide et remplissez le tableau suivant où chaque ligne (est une division euclidienne $a = bq + r$) représente une étape de l'algorithme. 1.5

a	b	r	q

$$\boxed{\mathrm{PGCD}(2016, 233) = \_\_\_\_\_}$$

Exercice 4

30 min

Cryptosystème affine.
Le but de cet exercice est de déchiffrer le message *NITOTK* obtenu en appliquant le cryptosystème affine par paquet de 1 de clef $(19, 13)$.

1. Appliquer l'algorithme d'Euclide et déterminer $\mathrm{PGCD}(26, 19)$. 1

a	b	r	q	u	v

$$\boxed{\mathrm{PGCD}(26, 19) = \_\_\_\_\_}$$

2. Expliquer pourquoi $(19, 13)$ est bien une clef du cryptosystème affine par paquet de 1. 0.5

3. Déterminer deux entiers relatifs u et v tels que $26u + 19v = 1$. On complètera le tableau précédent. 1.5

$$\boxed{26 \times \left(\_\_\_\_\right) + 19 \times \left(\_\_\_\_\right) = 1}$$

4. En déduire l'inverse de 19 modulo 26. 0.5

5. Donner la fonction de déchiffrement $D_{(19,13)}$. 1

6. Déchiffrer le message 1.5

Message crypté	N	I	T	O	T	K
Codage						
Message clair						

Message clair : _____

Exercice 5

30 min

1. Déterminer l'écriture de 17 en binaire. 0.5

2. En appliquant l'algorithme d'exponentiation modulaire rapide, calculer
   (a) 3285^{17} modulo 3840. 1

   (b) 1267^{17} modulo 3840. 1

   (c) 1519^{17} modulo 3840. 1

Exercice 6

30 min

Vous interceptez un message codé en RSA

$$768 - 3285 - 1267 - 1519$$

Vous savez que la clef publique utilisée pour chiffrer ce message est $(3977, 2033)$. Le but de l'exercice est de déchiffrer ce message.

1. Déterminer deux nombres premiers p et q tels que $p < q$ et $pq = 3977$. 0.5

2. En déduire la valeur de $\varphi = (p-1)(q-1)$. 0.5

3. Appliquer l'algorithme d'Euclide étendu pour déterminer l'inverse de 2033 modulo φ. 1

a	b	r	q	u	v

$$2033^{-1} \equiv_{\varphi} \_\_\_\_\_$$

4. Déchiffrer le message. 1

Exercice 7

30 min

Soit $A = \begin{pmatrix} -1 & 6 \\ 7 & 1 \end{pmatrix}$.

1. Calculer le déterminant de A.

2. La matrice A est-elle une matrice inversible de $\mathcal{M}_2(\mathbb{Z}/26\mathbb{Z})$? Justifier.

3. Chiffrer le message *SAURON*.

4. Déterminer la matrice A^{-1} la matrice inverse de A modulo 26.

5. Déchiffrer le message *VZSDRPAF*.