Décembre 2016

NOM :
Prénom :
Groupe :

Examen

Cryptologie

- *La calculatrice est autorisée.*
- *Tous documents et tout moyen de communication sont prohibés a l'exception de l'antisèche légale, si elle ne comporte aucune note manuscrite.*
- *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.*
- *L'utilisation du 49.3 ne permet pas de résoudre les problèmes.*

Exercice 1

15 min

On a utilisé un chiffrement de César par paquet de 2 avec 2000 comme clef et on a obtenu *1094-2017-492*. Quel était le message non chiffré ? Détailler les étapes. 3

Exercice 2

15 min

Calculer les congruences suivantes. On détaillera les étapes de calcul.

1. 15^{2016} modulo 31 1

2. 7^{2017} modulo 50 1

3. 2018^{2020} modulo 2019 1

Exercice 3

30 min

1. Déterminer l'inverse de 979 modulo 2526, en appliquant l'algorithme d'Euclide étendue. 1

a	b	r	q	u	v

2. Expliquer pourquoi $(979, 119)$ est une clef valide du chiffrement affine par paquet de 2. 0.5

3. Déchiffrer le message suivant, crypté par la méthode de affine par paquet de 2 de clef $(979, 119)$:

$$1767 - 629 - 2026 - 1649$$

1

Exercice 4

45 min

1. (a) Montrer que l'écriture binaire de 19 est $(10011)_2$. 0.5

(b) Utiliser l'algorithme d'exponentiation modulaire rapide et calculer 303^{19} modulo 9797. 2

k	0	1	2	3	4
303^{2^k}					

2. (a) Donner la liste des nombres premiers inférieur à 10. 0.5

(b) Expliquer pourquoi 101 est un nombre premier. 0.5

(c) Montrer que 9797 est le produit de deux nombres premiers $p < q$. 0.5

(d) Appliquer l'algorithme d'Euclide étendu et déterminer l'inverse de 7579 modulo 9600. 1

a	b	r	q	u	v

(e) Vérifier que (9797, 7579) est un clef de chiffrement valide du cryptosystème RSA. 1

(f) Déterminer la clef privée associé à la clef publique (9797, 7579). 0.5

3. On a chiffré un nombre par la méthode RSA de clef publique (9797, 7579) et on a obtenu le cryptogramme 303. Quel est le nombre claire ? 0.5

Exercice 5

15 min

Pour chacune des matrices suivantes, calculer son déterminant et <u>entourer</u> celle qui sont inversibles modulo 26. Aucune justification n'est demandée.

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \qquad C = \begin{pmatrix} -2 & 11 \\ 1 & 1 \end{pmatrix} \qquad D = \begin{pmatrix} 4048 & 2 \\ -73 & 1 \end{pmatrix}$$

$\det(A) =$ _____ $\det(B) =$ _____ $\det(C) =$ _____ $\det(D) =$ _____

Exercice 6

20 min

1. Calculer l'inverse modulaire de 21 modulo 26. 1

2. Calculer le déterminant de la matrice $A = \begin{pmatrix} 3 & 23 \\ 19 & 14 \end{pmatrix}$ 0.5

3. Expliquer pourquoi la matrice A est inversible modulo 26. 0.5

4. Déterminer l'inverse de la matrice A ; on simplifiera le résultat. 1.5

5. Déchiffrer le message suivant, crypté par la méthode de Hill par paquet de 1 de clef A :

$$5 - 12 - 22 - 10 - 25 - 24$$

1.5

Exercice 7

10 min

Voici le carré de Polybe :

A	B	C	D	E
F	G	H	I, J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Déchiffrer le message suivant : 1

311514111214153511453135342211