Février 2018

NOM :
Prénom :
Groupe :

Examen

Cryptologie

- *La calculatrice est autorisée.*
- *Tous documents, téléphones portables, 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.*
- *L'utilisation du 49.3 ne permet pas de résoudre les problèmes.*

Exercice 1

10 min

Considérons le programme suivant :

```
1   def Secret(Mot) :
2      res=""
3      for c in Mot :
4         if(c=="A") :
5            res+="S"
6         if(c=="B") :
7            res+="T"
8         if(c=="J") :
9            res+="L"
10        if(c=="N") :
11           res+="U"
12        if(c=="O") :
13           res+="A"
14        if(c=="P") :
15           res+="E"
16        if(c=="R") :
17           res+="D"
18        if(c=="U") :
19           res+="R"
20     return res
21
22  print(Secret(input("Mot : ")))
```

Le programme affiche `TAULARD`.
Quel est le `Mot` de départ ? 1

Exercice 2

15 min

Calcul les congruences suivantes. Justifier

1. $2019 \times 2020 \times 2021 \times 2022 \times 2023$ modulo 2018 1

2. 10^{2018} modulo 99 1

3. 99^{2018} modulo 42 1

Exercice 3

15 min

Appliquer l'algorithme d'Euclide étendu et calculer l'inverse de 5704 modulo 983.

a	b	r	q	u	v

$5704^{-1} \equiv_{983} \_\_\_\_\_$

2.5

Exercice 4

15 min

Le message suivant a été obtenu par un chiffrement de Cesar par paquet de 2 :

$$2119 - 597 - 199$$

On ignore la clef mais on sait que les deux premières lettres du texte claire sont `HA`. Déterminer la clef ainsi que le message claire dans son intégralité. Justifiez précisément.

2.5

Exercice 5

30 min

1. Calculer 19×11 modulo 26.

0.5

2. En déduire l'inverse de 19 modulo 26.

0.5

3. Calculer le déterminant de la matrice $A = \begin{pmatrix} 7 & 19 \\ 6 & 19 \end{pmatrix}$

1

4. Expliquez pourquoi la matrice A est inversible. 0.5

5. Déterminer A^{-1}. 1

6. Déterminer le message suivant obtenu par un chiffrement de Hill de clef A : `WEVBHT` 1.5

Exercice 6 45 min

1. (a) Déterminer l'écriture binaire de 99. 0.5

   (b) En utilisant l'algorithme d'exponentiation modulaire rapide, déterminer la valeur de 439^{99} modulo 2773. 2

2. (a) Expliquer pourquoi $(2773, 539)$ est une clef valide du cryptosystème RSA. 1

(b) Déterminer la clef privée associée à la clef publique $(2773, 539)$. 1

(c) En utilisant la clef publique $(2773, 539)$ on a obtenu le message 439. Quel est le nombre en claire ? 0.5

Exercice 7

15 min

Dans le cryptosystème de RSA on connait la clef publique $(229\,159\,043, 11\,111)$ et on sait que "$\varphi = 229\,128\,768$". Déterminez deux entiers premiers p et q tel que $pq = 229\,159\,043$. Justifier très précisément. 2

Exercice 8

10 min

Décrypter le message suivant : 1

I	S	S	S	F	L	D	Y	R	M
L	T	T	D	I	E	E	P	C	O
N	P	R	I	C	D	C	T	E	T
E	A	E	F	I	E	R	E	S	S