NOM : LAPOSTOLET

Prénom : Arsène

Groupe : 10

IUT de Paris – Dép. Informatique – Arithmétique – DST du 9 novembre 2017

Durée : 2 heures – Sans documents, sans calculatrice, sans portable.

Pour les exercices 1 et 3, vous répondrez directement sur le sujet. L'exercice 2 sera traité sur une copie séparée.

Sur la dernière feuille du sujet, vous trouverez des rappels sur la méthode RSA et son accélération, sur les commandes Scilab, ainsi que les tables de multiplication jusqu'à 30 pour vous faciliter éventuellement les calculs. Cette dernière feuille peut être détachée du reste du sujet.

15

Exercice 1 *(~ 8 points)*

Pour les questions à choix multiples, il peut y avoir une ou plusieurs bonne(s) réponse(s). Toute réponse juste apportera les points correspondants, et toute réponse fausse fera perdre la moitié des points correspondants.

1. Cocher les propositions toujours vraies. Si y est inverse de x modulo m, alors :

   ☐ $x + 2y \equiv 1\ [m]$ ☐ $x + y^2 \equiv 1\ [m]$ ☐ $(xy)^2 \equiv 1\ [m]$ ☐ $2xy \equiv 1\ [m]$ ☐ $xy + 2m \equiv 1\ [m]$

   ☒ aucune relation proposée n'est correcte

2. Si x est pair, alors il n'existe aucun m tel que x soit congru à 1 modulo m.

   ☐ Vrai ☒ Faux

   Si c'est vrai, justifiez. Sinon, donner un contre-exemple.

   $10 \equiv 1\ [3]$

   or 10 est pair.

3. Qu'affiche Scilab à l'appel de la commande suivante lorsque $n = 294$?

```
if pmodulo(n,2)==0 then t = 'vrai'; else t = 'faux'; end; t
if pmodulo(n,10)==5 then s = 'vrai'; else s = 'faux'; end; s
if pmodulo(n,2)==0 & pmodulo(n,5)==0 then r = 'vrai'; else r = 'faux'; end; r
```

   ☐ error ☒ t=vrai ☐ t=faux ☐ s=vrai ☒ s=faux ☐ r=vrai ☒ r=faux

4. Qu'affiche Scilab à l'appel de la même commande lorsque $n = 300$?

   ☐ error ☒ t=vrai ☐ t=faux ☐ s=vrai ☒ s=faux ☒ r=vrai ☐ r=faux

5. On donne la relation de Bezout suivante : $3 \times 11 - 2 \times 16 = 1$.
   Pour appliquer RSA, quel(s) couple(s) de clés publique/privée (e, d) et quelle(s) valeur(s) de $n = p \times q$ peut-on choisir ?

   ☐ $e = 3, d = 11, n = 32$ ☐ $e = 11, d = 3, n = 32$ ☐ $e = 3, d = 11, n = 51$
   ☐ $e = 11, d = 3, n = 51$ ☐ $e = -2, d = 16, n = 33$ ☐ $e = 16, d = -2, n = 48$
   ☐ aucun trio proposé ne convient

6. Combien y a -t-il d'éléments inversibles dans $\mathbb{Z}/19\mathbb{Z}$ (c'est-à-dire entre 0 et 19) ?

   ☐ 0 ☐ 1 ☐ 5 ☐ 8 ☐ 15 ☐ 18 ☐ 19 ☐ aucune valeur proposée ne convient

7. On appelle le code Scilab ci-dessous. Que vaut `i` à l'issue de son exécution ?

```
a=157; r=25; m=100; p=1; a=pmodulo(a,m); i=0;
while r>0
   if pmodulo(r,2)==1 then r=(r-1)/2; p=pmodulo(a*p,m);
      else r=r/2;
   end
   a=pmodulo(a^2,m); i=i+1;
end; i
```

☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☒ 5 ☐ 6 ☐ 7 ☐ aucune valeur proposée ne convient

Exercice 2 *(~ 8 points, à traiter sur une copie séparée)*

On considère deux personnes, Alicia et Bruno, qui souhaitent s'envoyer des messages cryptés par RSA. La clé publique d'Alicia est $(e_A, n_A) = (27, 55)$ et celle de Bruno est $(e_B, n_B) = (11, 77)$. Les textes sont transformés en suites de chiffres en faisant correspondre deux chiffres à chaque lettre (son rang dans l'alphabet).

1. Ils se sont mis d'accord pour chiffrer par RSA des groupes de deux chiffres (c'est-à-dire que pour un message à 4 chiffres, ils codent les deux premiers chiffres par RSA, puis les deux suivants par RSA).
   (a) Cette manière de chiffrer leurs messages est-elle sécurisée ? Justifier.
   (b) Déterminer la clé privée d_B de Bruno en appliquant l'algorithme d'Euclide *(on peut utiliser la factorisation $77 = 11 \times 7$)*.
   (c) Vérifier que la clé privée d'Alicia d_A vaut 3 *(on peut utiliser la factorisation $55 = 11 \times 5$)*.
2. Alicia envoie à Bruno le message 22 01 22 53 14.
   (a) Pour déchiffrer ce message, faudra-t-il utiliser la clé privée d'Alicia ou de Bruno ?
   (b) En appliquant l'algorithme des carrés, déchiffrer 22. *(On donne $6 \times 77 = 462$.)*
   (c) Déchiffrer 01.
3. Pour 53 et 14, on va utiliser la méthode d'accélération de RSA.
   (a) Déterminer une relation de Bezout entre $p = 11$ et $q = 7$.
   (b) Déterminer les valeurs (positives) d_p et d_q telles que $d_B \equiv d_p$ [10] et $d_B \equiv d_q$ [6].
   (c) Déchiffrer 53 en utilisant la méthode d'accélération de RSA. *(On donne $2 \times 77 = 154$.)*
   (d) Déchiffrer 14 en utilisant la méthode d'accélération de RSA.
   (e) En utilisant le tableau de correspondance ci-dessous, en déduire à quelle station de métro Alicia a donné rendez-vous à Bruno.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22

W	X	Y	Z
23	24	25	26

Exercice 3 *(~ 4 points)* On donne le code Scilab suivant, qui devrait calculer pour deux valeurs entières $a > b$ leur PGCD dans la variable `pgcd` et les coefficients `x` et `y` de la relation de Bezout (tels que $ax + by = a \wedge b$). Il est présenté ici avec pour a et b par exemple les valeurs 125 et 43.

```
a=125;b=43;
//on choisit d'indicer _p la ligne du dessous, _m celle du dessous
xy_p=[1 0]; xy_m=[0 1];
// on a stocké dans le vecteur ligne xy les valeurs de x et de y
r_p=a; r_m=b;
// on a stocké dans r les valeurs de la colonne 'ax+by' dans l'algorithme d'Euclide
while r_m<=0,
   q=pmodulo(r_p/r_m);
   // on a stocké dans q les valeurs des quotients successifs
   xy_tmp=xy_p-b*xy_m; r_tmp=floor(r_p,r_m);
   xy_p=xy_m; r_p=r_m;
   xy_m=xy_tmp; r_m=r_tmp;
end
pgcd=r_p, x=xy_p(1), y=xy_p(2)
```

APOSTOLET
Thème
109

Ce code contient deux erreurs. Quels éléments doivent être changés dans le code ci-dessus pour que les valeurs de pgcd, x et y soient correctement calculées?

```
a=125; b=63;
xy_p=[1 0]; xy_m=[0 1];
r_p=a; r_m=b;
while r_m(>=)0, // On change <= en >=
q=pmodulo(r_p/r_m);
xy_tmp=xy_p-(q*xy_m); r_tmp=gcd(r_p,r_m);
// on remplace b par q.
xy_p=xy_m; r_p=r_m;
xy_m=xy_tmp; r_m=r_tmp;
end
pgcd=r_p, x=xy_p(1), y=xy_p(2)
```

2