AL 5 ppa - Cryptographie et algorithmique - DST

Nom : _____

Prénom : _____

- Durée : 1 heure 30. Documents interdits, calculatrices interdites.
- Écrivez 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 Congruences (7 points)

1. [1 point] Rappelez la définition de $a \equiv b \pmod{n}$

   Solution: $a \equiv b \pmod{n} \iff n|a-b$.

2. [2 points] Calculez 2^{1324} *mod* 7

   Solution: Comme $2^3 \equiv 1 \pmod{7}$, calculons 1324 *mod* 3. On a $1324 \equiv 1000 + 300 + 24 \equiv 1 \pmod{3}$, donc $2^{1324} \equiv 2^1 \equiv 2 \pmod{7}$.

3. [2 points] Calculez 2^{1324} *mod* 15

   Solution: On remarque que $\phi(15) = \phi(3 \times 5) = 2 \times 4 = 8$. Comme $2^{\phi(15)} \equiv 2^8 \equiv 1 \pmod{1}5$, calculons 1324 *mod* 8. On a $1324 \equiv 1000+300+20+4 \equiv 0+(240+60)+4+4 \equiv 4 \pmod{8}$. D'où $2^{1324} \equiv 2^4 \equiv 16 \equiv 1 \pmod{15}$

4. [2 points] Calculez $17^{1327^{143}}$ *mod* 11

   Solution: On a $17^{1324^{143}} \equiv 6^{1327^{143}} \pmod{11}$. On constate que $6^{10} \equiv 1 \pmod{11}$. Calculons 1327^{143} *mod* 10. On constate que $1327^4 \equiv 7^4 \equiv 1 \pmod{10}$, calculons donc 143 *mod* 4. On a $143 \equiv 3 \pmod{4}$. Donc $1327^{143} \equiv 7^3 \equiv 3 \pmod{10}$ et $17^{1327^{143}} \equiv 6^3 \equiv 7 \pmod{11}$

2 RSA (9 points)

Vous (B) décidez de communiquer avec A et C. La clé publique RSA de C est $(7, 55)$.

1. [1 point] Chiffrez le message 4 pour l'envoyer à C.

   Solution: $4^7 \equiv (4^3)^2.4 \equiv 9^2.4 \equiv 26.4 \equiv 49 \pmod{55}$

2. [1 point] Soit (k, n) votre clé publique. On pose $n = 65$. Factorisez n

   Solution: $n = 5 \times 13$

3. [1 point] Déterminez $\phi(65)$

   Solution: $\phi(65) = \phi(5 \times 13) = \phi(5) \times \phi(13) = (5-1)(13-1) = 4 \times 12 = 48$.

4. [1 point] Pourquoi ne peut-on pas prendre $k = 8$?

   Solution: k et $\phi(n)$ doivent être premiers entre eux.

5. [1 point] On pose $k = 5$. Calculer $pgcd(48, 5)$ en utilisant l'algorithme d'Euclide.

   Solution: $pgcd(48, 5) = pgcd(5, 3) = pgcd(3, 2) = pgcd(2, 1) = pgcd(1, 0) = 1$.

6. [1 point] Calculez $\phi(48)$.

   Solution: Les éléments de $\{1, \ldots, 48\}$ premiers avec 48 ($= 3*2^4$) sont $\{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47\}$, comme il y en a 16, alors $\phi(48) = 16$

7. [1 point] Determiner l'inverse de 5 dans $Z/48Z$ en utilisant l'algorithme d'Euclide étendu.

   Solution:

a	b	q	r	u	v
48	5	9	3	2	-19
5	3	1	2	-1	2
3	2	1	1	1	-1
2	1	2	0	0	1
1	0			1	0

L'inverse de 5 est -19, à savoir 29 dans $Z/48Z$.

8. [1 point] Quelle est votre clé privée ?

Solution: $(29, 65)$.

9. [1 point] A vous a envoyé le message chiffré 41. Donnez la formule permettant de le déchiffrer.

Solution: 41^{29} *mod* 65

3 Programmation (4 points)

1. [4 points] Ecrire en C l'algorithme d'Euclide étendu. Vous utiliserez le protype `long euclideEtendu(long a, long b, long* u, long* v) ;`

Solution:

```
long euclideEtendu(long a, long b, long* u, long* v)
{
  long uR, vR, p;
  if (b == 0)
    {
      *u = 1;
      *v = 0;
      return a;
    }
  p = euclideEtendu(b, a%b, &uR, &vR);
  *u = vR;
  *v = uR - a/b*vR;
```

```
  return p;
}
```