TD 3 de mathématiques

1. Calculer $51 * 25 \mod 91$, $25^{71} \mod 91$.

2. Calculer $\phi(85)$, $\phi(1024)$, $\phi(759), \phi(105)$, $\phi(1155)$, $\phi(48)$.

3. Soit n le produit de deux entiers premiers et $\phi(n)$ la fonction indicatrice d'Euler de n. Connaissant n et $\phi(n)$, comment peut-on faire pour factoriser n (c'est à dire trouver p et q tel que $n = pq$)?

4. Soit p premier, on rappelle que a est un résidu quadratique modulo p (RQ) si $a < p$ et si $x^2 = a \mod p$ pour un certain x. Calculer tous les RQ modulo 7 puis modulo 23.

5. Calculer $8^{11} \mod 11$, $7^{11} \mod 11$, $5^8 \mod 7$, $14^{16} \mod 17$, $67^{258} \mod 68$, $3^{45} \mod 5$, $7^{31} \mod 11$, $4^{25} \mod 35$, $7^8 \mod 30$.

6. Soit $g < p$, p premier. 2 est-il un élément primitif modulo 11? 3 est-il un élément primitif modulo 11?
   Soit Z_5 l'ensemble des entiers modulo 5, $Z_5 = \{0, 1, 2, 3, 4\}$. Montrer que Z_5 peut s'écrire sous la forme $Z_5 = \{0\} \cup \{g^0, g^1, g^2, g^3\}$.

7. Calculer $\#\mathbb{Z}_{86}^*$. $\mathbb{Z}_{86}^*$ admet-il un élément primitif modulo 86 ?

8. Supposons que $\mathbb{Z}_n^*$ admette un élément primitif. Combien en admet-il ?

9. Alice souhaite chiffrer un message m à Bob en utilisant RSA. Expliquer comment Alice est Bob vont procéder et quels sont les propriétés arithmétiques utilisées. Donner un exemple numérique.

10. Attaque sur RSA : Théorème du reste chinois :
    Stephane doit envoyer le même message M à Alice, Claire et Corinne dont les clés publiques sont respectivement $(n_1 = 26, e = 7)$, $(n_2 = 35, e = 7)$, $(n_3 = 33, e = 7)$, (où n_i sont les modules RSA).
    Stephane envoie les valeurs $C_1 = 24$, $C_2 = 23$, $C_3 = 29$.
    Comment Estelle va-t-elle procéder pour retrouver M après avoir intercepté les trois valeurs et les clés publiques?