TD de cryptographie

1. L'algorithme de chiffrement d'ElGamal est-il déterministe ? pourquoi ? pourquoi le chiffrement d'ElGamal est-il composé de deux parties ?
2. Quels sont les avantages et inconvénients du chiffrement asymétrique par rapport au chiffrement symétrique ?
3. Alice souhaite envoyer des messages chiffrés à Bob. Chacun dispose d'une biclé (clé publique/ clé privé), d'un système de chiffrement symétrique et d'un système de chiffrement asymétrique. On note m le message à envoyer, l'algorithme de chiffrement est E, l'algorithme de déchiffrement est D, la biclé d'Alice est A_p/A_s et celle de Bob est B_p/B_s.
   (a) Le message à envoyer ne dépasse pas 300 bits. Comment Alice va-t-elle procéder ?
   (b) Le message est le dernier film qu'elle vient de tourner. Comment Alice va-t-elle procéder ?
4. Calculer $PGCD(79, 23)$
5. Calculer $18^{-1} \mod 23$, $25/8 \mod 11$, $7/4 \mod 10$, $8/3 \mod 10$.
6. Résoudre $5x \equiv 20 \mod 25$ et $4x \equiv 3 \mod 29$
7. Calculer x tel que $\begin{cases} x = & 13 \mod 19 \\ x = & 6 \mod 23 \end{cases}$
8. Donner la définition de $\mathbb{Z}_n$ et celle de $\mathbb{Z}_n^*$.
9. Calculer $\#\mathbb{Z}_{24}^*$, $\#\mathbb{Z}_{11}^*$, $\#\mathbb{Z}_{1024}^*$, $\#\mathbb{Z}_{35}^*$ (où la notation # signifie le nombre d'éléments).
10. Déterminer tous les entiers premiers inférieurs à 30 qui sont congrus à $3 \mod 4$.
11. Calculer l'inverse de $65 \mod 101$.
12. Calculer $8 * 29 \mod 33$, $5 * (-28) \mod 30$.
13. Calculer l'inverse de 13 mod 29.
14. Calculer $51 * 25 \mod 91$.
15. Soit $a, b, n, n' \in Z$ avec $n > 0$ et $n'|n$, Montrer que si $a \equiv b \mod n$, alors $a \equiv b \mod n'$.
16. Soit $d = PGCD(a, b) \neq 0$, Calculer $PGCD(a/d, b/d)$.
17. Déterminer x et y tel que $5x + 17y = 1$.
18. Résoudre dans Z : $5x + 4 \equiv 7 \mod 19$
19. Résoudre dans Z : $5x + 4 \equiv 7 \mod 15$
20. Résoudre dans Z_{18} : $16x + 4 = 7$
21. Résoudre dans Z_{18} : $16x + 5 = 7$
22. Quels sont les ordres possibles des éléments de Z_{14}^*?
23. Quel est le dernier chiffre de (257!) ?
24. $(Z_3 \times Z_2, +, (0, 0))$ est-il un groupe cyclique?

25. Déterminer un générateur de Z_9^*, et de Z_{11}^*.

26. Soit $G = (Z_6, +)$, déterminez un sous groupe propre de G (sous groupe différent de G).

27. Déterminer les diviseurs de zéro de Z_{30} (les non inversibles).

28. Montrez qu'un groupe où tous les éléments sont involutifs (cad $a^2 = e$) est abélien.

29. Cherchez le groupe des inversibles de R^2 muni de la loi

$$(a, b)(c, d) = (ac, bc + d).$$