Devoir à rendre avant le prochain cours, soit au début du cours, soit par mail à quentin.deschamps@univ-lyon1.fr.

1 Substitution mono-alphabétique

Un chiffrement par substitution mono-alphabétique est un chiffrement dans lequel chaque caractère du message est remplacé par un autre caractère.

1. Quelle méthode permet d'attaquer ce type de chiffrement ?
2. Sur un alphabet de 26 lettres, combien y a t-il de permutations de l'alphabet possible.
3. En supposant qu'un ordinateur teste 10^9 permutations par seconde, combien de temps faudrait-il pour tester toutes les permutations (attaque par force brute) ?

2 Diffie-Hellman dans $\mathbb{Z}/n\mathbb{Z}$

On considère le groupe $\mathbb{Z}/n\mathbb{Z}$ avec $n = 13$ et un générateur $g = 6$

1. Calculer les puissances successives de 9. Vérifier ainsi qu'il s'agit bien d'un générateur du groupe.
2. Dans un échange de clef Diffie-Hellman, Alice choisi $a = 5$ et Bob $b = 8$. Calculer la clef commune K.
3. Eve voit passer les valeurs $A = 7$ et $B = 2$. Déterminer la clef K.