Introduction à la Cryptographie

TD1

1 Ordre de grandeur

On souhaite vider les océans avec un dé à coudre. On considère qu'un dé à coudre est un cylindre de 1.5 cm de hauteur pour 1.5 cm de diamètre. Selon l'Institut Français des Mers, les océans couvrent 360 millions de km^2 avec une profondeur moyenne de 3800m. Estimez le nombre de dés à coudre que contiennent les océans. Déduisez-en un encadrement entre deux puissances de 2¹.

2 One Time Pad

- 1 On donne un message de taille m , i.e. qui appartient à $\{0, 1\}^m$. Rappeler le fonctionnement du chiffrement OTP.
- 2 Montrer que l'OTP est un chiffrement parfait.

3 Générateurs pseudo-aléatoires

Soit $S = \{1, 0, 1, 1\}$ une séquence linéaire, dite le germe. Pour calculer le bit suivant, on va utiliser la formule de récurrence donnée par :

$$S_{n+1} = S_{n-1} \oplus S_{n-3}.$$

1. Trouver les 10 prochains bits de la séquence. Quelle est la suite obtenue ? Est-elle bien "aléatoire" ?
2. Montrer que tout générateur pseudo-aléatoire a un cycle et déterminer la longueur maximale de ce cycle pour un générateur avec un germe de 4 bits.
3. Même question pour le générateur donné par la récurrence suivante :

$$x_{n+1} = ax_n \pmod{7}.$$

4 Introduction au paradoxe des anniversaires

Supposons que des codes confidentiels de 4 chiffres sont distribués au hasard. Combien de personnes doit-on rassembler pour que la probabilité que deux personnes aient le même code soit de $\frac{1}{2}$?

1. Le volume d'un cylindre de rayon r et de hauteur h est égal à $\pi \times r^2 \times h$