I. Taille des clefs

1.1 Combien de déchiffrement DES cette machine est-elle capable d'effectuer par seconde ? 16 cartes-support avec chacune 8 FPGAs capable d'exécuter 4 "cœurs" de chiffrement DES en parallèle. Cadencé à 140 MHz avec un chiffrement DES par cycle d'horloge.

1.2 En combien de temps une COPACOBANA peut-elle casser le DES (qui a des clefs de 56 bits) ?

1.3 En combien de temps une COPACOBANA peut-elle casser SkipJack (qui a des clefs de 80 bits), en admettant qu'un chiffrement skipjack prend le même temps qu'un chiffrement DES ?

1.4 Combien y a-t-il de mots de passe de 8 caractères, en autorisant minuscules, majuscules, chiffres et quelques signes de ponctuation ? Quelle est la taille de clef secrète correspondante ? (ceci est parfois nommé l'entropie du mot de passe).

1.5 Un cœur d'un CPU contemporain, est capable de faire 8 millions de chiffrements AES par seconde. Combien de cœurs faut-il pour casser un tel mot de passe en une semaine ?

1.6 Bremermann a démontré qu'un système matériel auto-suffisant ne peut pas réaliser plus de $1.36 \cdot 1050$ opérations par seconde et par kilo de matière (cette valeur est environ c^2/h, où c est la vitesse de la lumière et h est la constante de Planck). Sachant que la planète terre pèse $5.972 \cdot 1024$ kg, donner une borne inférieure sur le temps nécessaire pour casser une clef secrète de 512 bits par force brute.

1.9 Considérons l'algorithme suivant :

```
1: procedure ManyTrials(C, n, k)
2:     K ← Random bit string of size n
3:     P ← D(K, C)
4:     repeat
5:         if P ≠ ⊥ then
6:             Return (P, K)
7:         end if
8:     until k trials have failed
9:     Return ⊥
10: end procedure
```

Quelle est sa probabilité de succès, en fonction de n et k ?

- Probabilité de succès pour un essai ?
- Pour k essais, quelle probabilité de succès total ?
- Quelle probabilité pour que l'algorithme ne trouve pas la solution ?
- Avec quelle probabilité chaque essai échoue ?
- Quelle probabilité que l'attaque réussisse après k essais ?

1.10 Qu'est-ce qui est le plus probable : « ManyTrial casse une clef de 128 bits avec un million d'essais » ou « Je joue 4 fois à l'euro-millions et je gagne les 4 fois »
- D'après l'énoncé de 1.8: 139 838 160 combinaisons possibles pour l'Euromillions.

Exercice I. Modes opératoires et propriétés de sécurité

Considérons un système de chiffrement par bloc E qui chiffre des blocs de n bits (i.e. M = {0, 1} n). Montrer que le mode opératoire ECB n'assure pas la sécurité sémantique.

- Qu'est ce que la sécurité sémantique ?
- Qu'est ce que le mode opératoire ECB (Electronic Codebook) ?

a. Montrer que le mode opératoire ECB n'assure pas la sécurité sémantique. (Tester avec des messages choisis par l'attaquant, avec l'un des messages qui se répète.)

b. Supposons que E est utilisé en mode compteur CTR. Montrer que si le nombre de blocs de suite chiffrante est suffisamment grand, alors il est facile de distinguer la suite chiffrante d'une suite aléatoire. Donner la longueur de la suite chiffrante pour que le distingueur ait un avantage supérieur à 1/2 si le chiffrement par bloc E opère sur des blocs de 64 bits (comme le DES).

- Quel est l'un des moyens de s'assurer qu'un chiffrement est efficace ? A quoi doit-il être semblable ?

Étudions cette question sur un système de chiffrement par bloc en mode compteur (CTR)

- Soient S_A une suite aléatoire et S_{CTR} un chiffrement par CTR. Peut-on les différencier ?
- On s'aide du paradoxe des anniversaires pour la suite, quel est-il et quel résultat important fournit-il ?
- Les suites S_A et S_{CTR} contiennent-elles des répétitions ?

c. Montrer que le mode opératoire CBC n'assure pas la sécurité sémantique pour des messages suffisamment longs.