1 ♦◇◇ Mot de passe

Un système est protégé par un mot de passe, après un essai infructueux le système attend 1s avant de redemander. Combien de temps faudra-t-il pour s'identifier dans les cas suivants :

1. le mot de passe est un prénom [a] ;
2. c'est un mot du dictionnaire [b] ;
3. il est composé de 4 chiffres ;
4. il fait 8 caractères.

■

a. L'INSEE publie la liste des 20 000 prénoms donnés en France depuis 1946. En pratique, seul un millier de prénoms suffit à désigner plus de la moitié de la population française.

b. Le français compte environ 200 000 mots dont seulement 3000 sont utilisés couramment.

2 ♦◇◇ Dénombrements

Le nombre de clés disponibles dans un système de chiffrement donne une borne maximale de sa sécurité (mesure de la complexité d'une recherche exhaustive).

1. Quel est le nombre de clés possibles dans un chiffrement de César ?
2. Pour un chiffrement affine ? ($C(x) = ax + b \mod 26$ pour chaque caractère $x \in \mathbb{Z}_{26}$)
3. Pour un chiffrement par substitution (substitution arbitraire, caractère par caractère) ?
4. Pour un chiffrement de Vigénère (avec une clé de longueur `k`) ?

■

3 ♦◇◇ Vider l'océan 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 3800 m. Encadrer entre deux puissances de 2 consécutives le nombre de dés à coudre d'eau que contiennent les océans.

■

4 ♦◇◇ La force brute

Le *facteur de travail* d'un algorithme est le nombre d'instructions élémentaires nécessaire à son exécution. La puissance d'une machine est le nombre d'instructions qu'elle exécute par unité de temps. La puissance d'un PC actuel est d'environ 2000 Mips. (millions d'instructions par secondes). Le facteur de travail d'un algorithme optimisé pour tester une clé de 128 bits de l'algorithme AES est d'environ 1200 instructions élémentaires.

On dispose d'un couple clair/chiffré connu et on désire retrouver la clé utilisée par force brute, c'est- à-dire en testant toutes les clés les unes après les autres. Une clé est constituée d'un mot de 128 symboles binaires. On suppose que toutes les clés sont équiprobables.

On utilisera les approximations :

$10^3 = 1000 \approx 2^{10}$, 1 jour = 2^{16} secondes, 1 an = 2^9 jours = 2^{25} secondes, etc.

1. En combien de temps une machine de 2000 Mips teste-t-elle une clé ?
2. Combien y a-t-il de clés possibles ?
   Quel est le nombre moyen de clés à tester avant de trouver la bonne ?
3. Á quel temps moyen de calcul cela correspond-il si on suppose que le milliard de PC de l'internet sont mobilisés à cette tâche ?

5 ♦♦◇ La loi de Moore

Il est admis que, grâce aux progrès technologiques permanents, la puissance des machines double en moyenne tous les 18 mois (loi de Moore). On suppose maintenant que l'on change les machines tous les mois (30 jours) en commençant avec une machine d'une puissance de 1000 Mips. $\forall n$, on note W_n le nombre d'instructions exécutées par la machine du mois n.

1. Quel est le facteur d'amélioration a de la puissance des machines d'un mois à l'autre ?
2. Calculer W_0, puis W_n en fonction de W_0, de a et de n.
3. Quel est le temps moyen nécessaire pour trouver la clé (de l'exercice précédent) ?

6 ♦◇◇ César

1. Est-il plus facile de décrypter un texte long ou un texte court ?
2. Pouvez-vous décrypter le message suivant : `pwpnetzyacpdtopyetpwwp`

7 ♦◇◇ Chiffrement de Vigénère

1. Si l'attaquant obtient la connaissance d'un couple message clair / message chiffré, peut-il déchiffrer tous les messages chiffrés ensuite avec cette même clé ?
2. On suppose que seulement un message chiffré est à disposition de l'attaquant.
   Si un attaquant connaît la longueur de la clé, comment faire pour déchiffrer ?
3. D'une manière générale, ce système de chiffrement est-il difficile à casser ?
4. Chiffrer le texte suivant : `textesecretadecoder` en utilisant comme clé le mot `crypto`.
5. Pour le même texte clair, le chiffré est `brqksmzcspxiqxtcxzr`. Quelle est la clé ?
6. Même question si le chiffré est `aaabbbcccdddeeefffg`. Que remarque-t-on ?

8 ♦◇◇ Seulement des XOR

Alice veut envoyer à Bob le message $M \in \mathbb{F}_2^n$.

1. Alice et Bob partagent une clé secrète $K \in \mathbb{F}_2^n$. Ils effectuent le protocole suivant :
   - Alice envoie $C = M \oplus K$ à Bob.
   - Bob calcule $M = C \oplus K$.

   Montrer que $C \oplus K$ est bien le message M.
2. Alice possède une clé secrète $K \in \mathbb{F}_2^n$ et Bob une clé $L \in \mathbb{F}_2^n$.
   Ils effectuent le protocole suivant :
   - Alice envoie $C_1 = M \oplus K$ à Bob.
   - Bob envoie $C_2 = C_1 \oplus L$ à Alice.
   - Alice envoie $C_3 = C_2 \oplus K$ à Bob.

   Montrer que Bob peut retrouver le message, mais en interceptant tous les échanges, un interlocuteur Oscar peut également retrouver M.

9 ♦♦♢ Chiffrement de Polybe

On considère l'alphabet privé du W, soit 25 lettres. Polybe a proposé le mécanisme suivant : on range les lettres dans un tableau 5×5, en commençant par le mot clé (et en supprimant les doublons), puis on continue avec les lettres restantes de l'alphabet, dans l'ordre.

Par exemple, avec le mot-clé MYSTERE, on construit le tableau suivant :

	1	2	3	4	5
1	M	Y	S	T	E
2	R	A	B	C	D
3	F	G	H	I	J
4	K	L	N	O	P
5	Q	U	V	X	Z

Le chiffrement s'effectue alors en remplaçant chaque lettre par les deux chiffres : ligne colonne qui indiquent sa position dans la grille . Par exemple, F est chiffré 31.

1. Expliquer comment on peut cryptanalyser un tel système : par une attaque à clair connu, puis dans une attaque simple (seulement un chiffré).

   Raoul envoie un message à Anna pour lui fixer rendez-vous.

   Le cryptogramme est le suivant :

   123222 512215 424215 512242 242255 534352 111524 225254
   322252 512211 515222 532251 142251 154352 21

2. Décrypter ce message **(on ne connaît pas le mot-clé)**.

■