Mod.?ZEFZLEFule Sécurité TD N°1

1. Donnez et expliquer les objectifs et qualités attendus d’un bon crypto-système

***Réponse :*** *Les objectifs et qualités d’un bon crypto-système sont de pouvoir crypter et décrypter de manière sécurisée offrant un niveau de confidentialité et d’intégrité satisfaisant et de plus satisfaire les propriétés suivantes à savoir : 1. L’authentification : les participants à une session de communications confidentielles sur un canal non sécurisé sont bien les véritables entités du dialogue. 2. La non-répudiation : les participants ne peuvent nier avoir émis, transmis ou reçu de messages et avec preuve à l’appui si tels sont les cas (On peut le prouver).*

1. Définir ce qu’est une Attaque de force brute ou Puissance Calculatoire et donnez un exemple simple

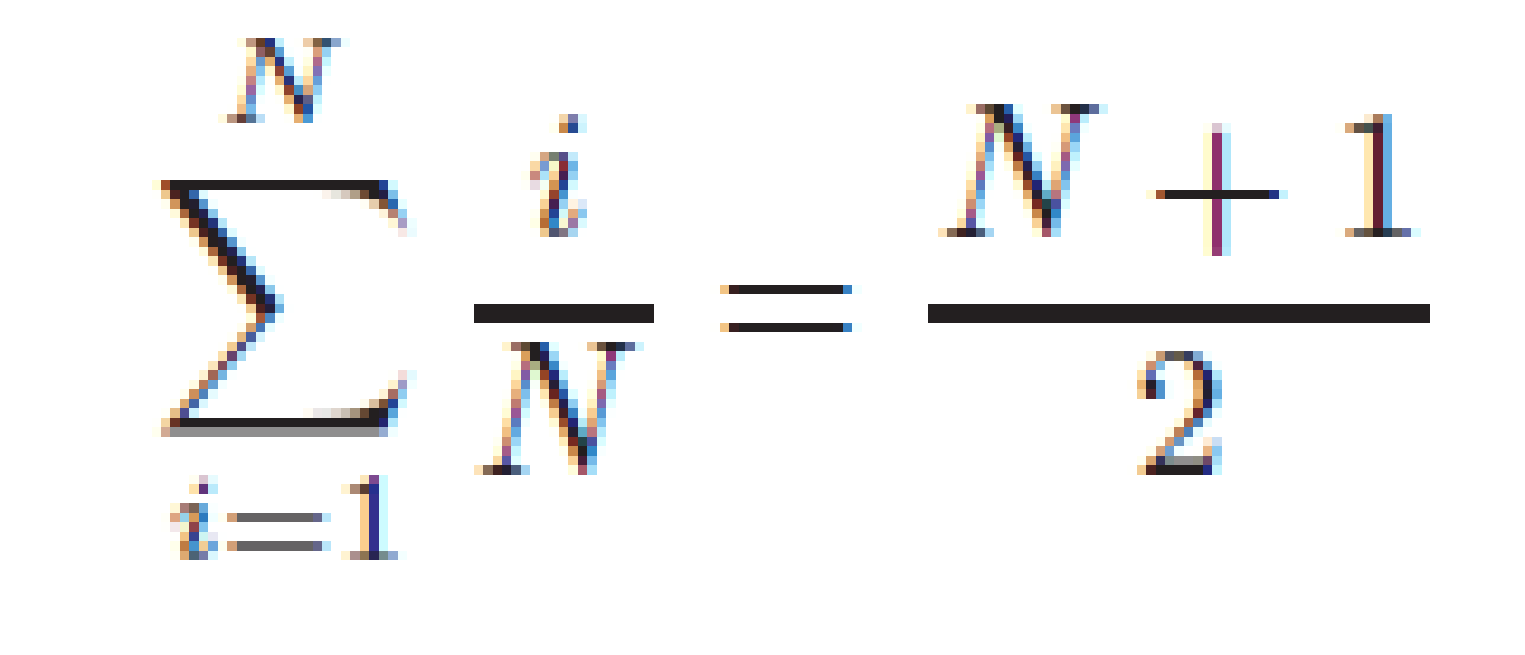
**Cette attaque consiste à essayer systématiquement toutes les clefs possibles jusqu’`a ce que l’on tombe sur la bonne clef.** On peut simplifier le modèle de cette attaque en supposant que l’on a un oracle (un dispositif) qui répond par oui ou par non à la question: Cette clé est-elle correcte?

On peut définir la complexité par le nombre d’appels à l’oracle qui seront nécessaire pour obtenir la bonne clef. On aura une notion de complexité dans le pire des cas (worst case complexity ), une notion de complexité en moyenne (average complexity), etc...

Dans le cas d’un espace de clefs contenant N clefs qui sont générées uniformément on peut montrer que la meilleure attaque a une complexité dans le pire des cas de N essais et une complexité en moyenne de ∼ N/2 essais.

En effet, la meilleure attaque consiste à ordonner sans répétition les clefs de l’espace des clefs suivant un ordre aléatoire et commencer les essais. Si on se place dans le pire des cas, la bonne clé est la dernière et il a donc fallu effectuer N essais.

Si la bonne clé est la ième dans la liste, il a fallu i fois essais. Comme la liste a été établie au hasard et la probabilité que la bonne clé soit la ième est 1/N. Par conséquent, la complexité en moyenne, c’est `a dire le nombre d’essais qu’il a fallu faire en moyenne, est :



**Exemple simple :** Soit une valise protégée par une combinaison numérique (cadenas) à 3 chiffres.

L’espace des clés = 103 clés 0

0

0 

1 9

. 9

.

9

Si la clé est 000, on la trouvera du premier coup mais si elle est 999 alors on aura essayé 1000 clés donc en moyenne (1+1000)/2 essais, soit (N+1)/2

1. **Exercice**

Le facteur de travail d'un algorithme représente le nombre d'instructions élémentaires nécessaires à son exécution. La puissance d'une machine correspond au nombre d'instructions qu'elle peut exécuter par unité de temps. On suppose que la puissance actuelle d'un PC est d’environ 2000 Mips (millions d'instructions par seconde).

Le facteur de travail d'un algorithme optimisé pour tester une clé de 128 bits d’un algorithme de cryptographie (par exemple AES) est d'environ 1200 instructions élémentaires.

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

**Questions**

1. Quel est le temps t mis par une machine de 2000 Mips pour tester une clé ?

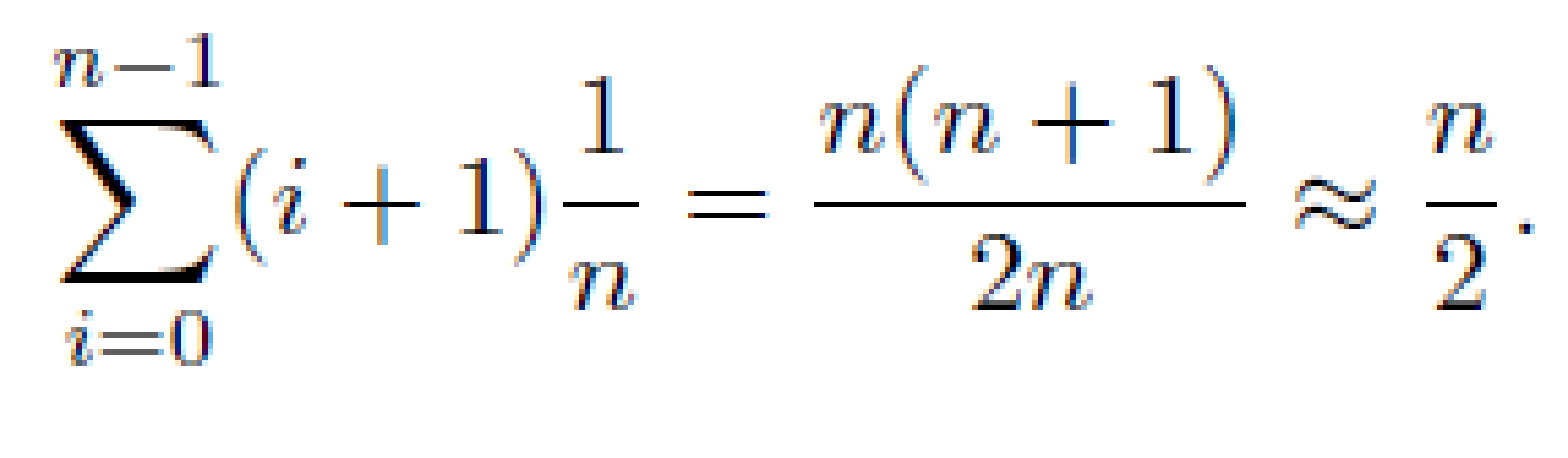
2. Combien de clés contient l’espace des clés (Nombre de clés possibles) ? Quel est le nombre moyen de clés à tester avant de trouver la bonne ?

3. Déterminer le temps moyen de calcul nécessaire à un PC pour effectuer la recherche de la clé. Quel serait ce temps si un milliard de PC de l'Internet sont mobilisés à cette tâche ?

**Réponses**

1. t = facteur de travail / puissance = 1200/ 2000\*106 = 12\*102/2\*109= (12/2)\*10-7 = 0,6 μs
2. Nombre de clés possibles = 2128 . On considère les clés possibles comme étant les entiers de 0 à 2128 – 1, et la clé secrète est notée k. Pour l'attaque par force brute avec n = 2128,

On essaie tous les entiers les uns après les autres. La probabilité, pour un entier i donné, d’être la clé, c’est-à-dire d'avoir k = i (et donc d'avoir exactement i+1 tirages à effectuer si on part de 0), est égale à 1/n. L'espérance du nombre d'essais est donc :



1. En utilisant un seul PC pour la recherche de la clé, on obtient :

Un PC exécute 2103\*2106 = 2109 instructions par seconde ≈ 2\*230 = 231 i/s

Nombre d’instructions à exécuter pour trouver la clé : 2128/2 clés \*1200= 2128\*29=2137

D’où t=2137/231 = 2106 s ou bien 2106/225 années = 281 années ≈ 2\* (210)8 ≈ **2\*1024**années

En utilisant un milliard de PCs soit 230 d’où 2137/231+30 ≈ 266s

Plus simple : 2\*1024/109 = **2\*1015** années