# Partie B

## Question 1 – Codage

1. **Expliciter les alphabets , et qui sont respectivement les alphabets pour la sortie de la source, du codeur et du bloc de chiffrement**

L’alphabet de la sortie de la source est les chiffres de [0-9].

L’alphabet de la sortie du codeur est le bit, donc il prend la valeur [0-1].

L’alphabet de sortie du bloc de chiffrement donne aussi le bit comme alphabet puisqu’il ne fait que permuter les bits.

1. **Identifiez** **les langages provenant des alphabets , et** .

Le langage provenant de la source est une suite de quatre chiffres.

Le langage provenant de la sortie du codeur est deux séquences de 32 bits.

Le langage provenant de la sortie du bloc de chiffrement donne une plage de 64 bits.

1. **Identifiez les attaques auxquelles le système est vulnérable.**

Un tel système est vulnérable aux attaques de forces brutes. Malgré la longueur de la sortie du bloc de 64 bits, il y en en fait que 10000 combinaisons, soit les quatre chiffres. Une seconde attaque est d’enregistrer un message intercepté et de le réexécuter plusieurs fois.

1. **Montrez à l’aide de traces d’exécution comment vous les effectueriez.**

Le script nommé « BruteForce.py », dans le dossier scripts, permet de générer un dictionnaire avec les 10000 combinaisons possibles. Ainsi, lorsqu’on intercept un message il suffit de faire une recherche dans le dictionnaire et de compter le numéro de ligne associé.

1. **Pour chacun des trois codages, dites quelles attaques du c) ils permettent de bloquer et démontrez-le à l’aide de trace d’exécution.**

|  |  |
| --- | --- |
| **Codage** | **Avantage** |
| Codage 1 | Rend beaucoup plus difficile l’attaque de force brute parce qu’il y a une longue chaine de caractère aléatoire à la fin des messages. |
| Codage 2 | Rend plus difficile l’attaque de force brute et empêche la réexécution de la requête grâce au « Timestamp ». |
| Codage 3 | Empêche la réexécution de la requête. |

1. **Selon vous quel est le meilleur codage ? Pourquoi ?**

Le codage 2 est le meilleur codage car il rend difficile l’attaque brute et empêche la réexécution de la requête. Il s’agit du seul des trois codages qui agit sur les deux attaques simultanément.

## Question 2 – Exploitation d’une vulnérabilité critique

## Question 3 – Certificats à clé publique, HTTPS et SSL

e) le codage 1 rend beaucoup plus difficile l’attaque de force brute.

Le codage 2 rend plus difficile l’attaque de force brute et empêche et empêche la réexécution de la requête.

Le codage 3 n’empêche pas l’attaque de force brute car les combinaisons sont de 10M mais empêche à réexécution du code.

f)Le codage 2 est le meilleur des 3 car il empêche la force brute et la réexécution de la requête.