UNIVERSITÉ LAVAL

Chapitre I : exercices

MOHAMED MEJRI

Groupe LSFM

Département d'Informatique et de Génie Logiciel

Université LAVAL

Québec, Canada

Chiffrement affine

➪ Question : Trouver m tel que : $e_k(m) = WNIIR\ PRAIK$ avec $k = (3, 1)$.

Chiffrement par substitution

➪ Question : Trouver m tel que : $e_\pi(m) = QSNQRFRSRFLK$ avec π est celle donnée dans l'acétate 20.

Carré de Polybe

➪ Question : La plus fameuse victime de la cryptanalyse est :

44211 21324 15522 11215

Trouver son nom sachant qu'il a été crypté avec le carré de Polybe en utilisant "CRYPTANALYSE" comme clé.

Chiffrement par permutation

➪ Question : En probabilité, pour critiquer la notion de "moyenne", on dit : lecqiu aiutal etenad nusuof tersel eipdsd snafnu gireso nesnet yomnne rtebse nei

Retrouver le message en clair correspondant sachant qu'il a été crypté avec le chiffrement par permutation en utilisant 3 2 1 comme clé.

Chiffrement de Hill

➪ Question : Le plus petit entier x tel que les trois nombres x, x^2 et x^3 épuisent tous les chiffres $(0, 1, ..., 9)$ est : $YUNCNAQBEVTE$
Retrouver cet entier sachant qu'il a été écrit en toutes lettres et crypté avec le chiffrement de Hill en utilisant la matrice

$$K = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$