UNIVERSITÉ LAVAL

Chapitre II : exercices

MOHAMED MEJRI

Groupe LSFM

Département d'Informatique et de Génie Logiciel

Université LAVAL

Québec, Canada

Cryptanayse du chiffrement de Hill

- Question : Trouver la clé K qui permet de transformer le message $CRYPTO$ en $VKLCAV$ en utilisant le chiffrement de Hill.

Cryptanayse du chiffrement affine

↦ Questions : Soit m un message en français tel que :

$$e_k(m) = \begin{array}{l} MRLAD\ UUERP\ RSKFU\ UDSRU\ FDKYF\ EKDOR\ MFLEZ \\ YKVXE\ FYADR\ LMFHH\ DBNRP\ VSVFM\ YAFIR\ KDBNR \end{array}$$

- Le système cryptograpphique utilisé pour crypter m peut être le chiffrement de Vigenere ou un chiffrement affine. Trouver ce système sachant que $Ic(m) \approx 0.0575$.
- Trouver le message m.

Cryptanayse du chiffrement de Veginere

↦ Question : Décrypter le message suivant

KCCPK BGUFD PHQTY AVINR RTMVG RKDNB VFDET DGILT XRGUD DKOTF MBPVG EGLTG CKQRA CQCWD NAWCR XIZAK FTLEW

RPTYC QKYVX CHKFT PONCQ QRHJV AJUWE TMCMS PKQDY HJVDA HCTRL SVSKC GCZQQ DZXGS FRLSW CWSJT BHAFS IASPR

JAHKJ RJUMV GKMIT ZHFPD ISPZL VLGWT FPLKK EBDPG CEBSH CTJRW XBAFS PEZQN RWXCV YCGAO NWDDK ACKAW BBIKF

TIOVK CGGHJ VLNHI FFSQE SVYCL ACNVR WBBIR EPBBV FEXOS CDYGZ WPFDT KFQIY CWHJV LNHIQ IBTKH JVNPI ST

Sachant que le message original été encrypté avec un chiffrement de Vigenère en utilisant une clé de taille 6. Par ailleurs, les lettres les plus fréquentes dans Y^0 sont "q> g=j> v> c", et les $IC(Y^0, Y^i - k)$ $(1 \leq i \leq 5, 0 \leq k \leq 25)$ sont donnés par le tableau suivant :

i	$IC(Y^0, Y^i - k), 0 \leq k \leq 25$												
1	.0393	.0452	.0430	.0366	.0421	.0341	.0277	.0243	.0507	.0384	.0372	.0350	.0473
	.0326	.0344	.0747	.0246	.0320	.0323	.0307	.0360	.0477	.0464	.0332	.0369	.0363
2	.0332	.0369	.0430	.0440	.0273	.0375	.0320	.0384	.0409	.0473	.0381	.0409	.0329
	.0338	.0289	.0440	.0477	.0280	.0381	.0344	.0372	.0458	.0624	.0393	.0344	.0323
3	.0480	.0326	.0357	.0446	.0329	.0249	.0473	.0440	.0338	.0390	.0504	.0317	.0317
	.0729	.0347	.0283	.0397	.0344	.0255	.0427	.0433	.0301	.0341	.0483	.0372	.0310
4	.0360	.0412	.0421	.0317	.0449	.0430	.0446	.0341	.0378	.0283	.0366	.0427	.0326
	.0363	.0378	.0381	.0289	.0575	.0433	.0338	.0437	.0409	.0277	.0369	.0412	.0372
5	.0366	.0387	.0437	.0246	.0212	.0449	.0424	.0317	.0363	.0412	.0249	.0400	.0741
	.0347	.0323	.0320	.0326	.0366	.0517	.0452	.0341	.0387	.0400	.0421	.0357	.0430

Cryptanayse du chiffrement de Veigenere : Test de Kasiski

- Q1 : Encrypter m= "THE CHILD IS FATHER OF THE MAN" avec la clé k="POETRY" en utilisant le chiffrement de Vigenere.
- Q2 : Appliquer le test de Kasiski sur le texte chiffré obtenu en (Q1) pour déduire la taille de la clé k.