Aurélien DUVAL

TP1 : Cryptographie et sécurité informatique

Exercice 1 : Briser Vigenère

On cherche à déchiffrer le texte suivant :

YHKMV MSXVV XTMGV WMRCJ KSQRE JYCBE JYIVOD EFDSC TIRTPE SMPVP ITSYEG BYTNZ SXWLC TLSSXB VTBOG YJWYF GIEZOR XCEKY RHCEE BYMHW SBMEN ZSXCEF CINPPU ZRDEB NZRDO YHZRD EPFZKS BPYKIH TGUCP ODGCG LORXY OXNEG LPTDIS HZWD HILVZO RWYZR YTLYIA YRHMD SFIRAW VYMXB VYXIR NVPVIK CSPOC MJYIBT IRKFKC ONFTV AMHKI HTEWZ TREVC JEZAM LFJKLKI IMDHQ MKLKT GLVEDE XBVIXC VSGXS ORUEH DHILVZ ORWCE KNEGLP TDISHK LODINR MVEHIG IBAXCF RYFEW ZTREVC JGYNXL FPVEHV FXRBCN YIKLKIIM DHQUE HSNIUT LSNWN RRMEFS ROOYXB ZWSSE MVGBEX CUIKLPS BRYWRI EPITSNY IMOQGL RSCEHK WESYU CPIAWB FVDSXL ZRQOJ WYEBA GNVVC WLCTLS SRYVHO DXIUIM RCJKX REGCG LORXY OXKCV SGXYS CMKIWI WNYIY RHYIIN LMMKS PEPYDI XTWIW JSNMN VTYSW CSPOP PUZRD EBNJJS NMNVT YSWCS POCCJ YIBTIRK WPIRCK IZOWM ZFVEOY PWKNH NYIONG LPTDIS HRRNDI WICZT MIEEVG SLZXRM WQYMM HGIIVOS TIEHDO IUTLUE CEVCCA VYZQZO VNRRDA WWZTR EVMNM DHSOKZ KRMUSP OKISJGK NFYKVS VMUCPI BVIBIXW MNYSXL CNYIUN SQCINGI IWXREG CGLORY MVHKN HUIIDHIL VJYRIOJI VEWMFV OVIHTSE NXYITBO HOTXSV IZFVWO WNGYBP SMVWRI WNFVSC EFCCMIT BVVCWI LVSPTIH LWODHC IIMTPSW SBERWI CZTMIE SBDIWIC ZTMIEA STLILXK DHCKM YNEFG VYCIXL VOSWO TLKSEO KLONX CTEDISH FVSNXY XVSTCW YIMKW

On sait que le texte est chiffré en anglais. De plus on sait que l'indice de coïncidende de la langue anglaise est : 0,066. Nous savons aussi que la clef est de taille inférieure ou égale à 8.

Nous allons donc utiliser le test de Friedman pour rettrouver la clef.

1)

Le test de Friedman nous donne le résultat suivant :
Soit m la taille de la clef testée.

m	Ic(x)							
1	0,045							
2	0,047	0,050						
3	0,061	0,052	0,051					
4	0,045	0,047	0,048	0,054				
5	0,042	0,047	0,042	0,046	0,047			
6	0,063	0,068	0,065	0,064	0,068	0,065		
7	0,046	0,044	0,046	0,042	0,051	0,052	0,040	
8	0,043	0,045	0,050	0,048	0,047	0,048	0,046	0,059

On remarque qu'avec une clef supposée de taille 6 les indices de coïncidence obtenus se rapprochent le plus de la langue anglaise. On pose donc que la taille de la clef est 6.

2)

Nous cherchons maintenant à déterminer la clef qui a chiffré le message ! Pour cela nous allons utiliser l'indice de coïncidence mutuel dans le but de trouver le décalage des colonnes par rapport à la colonne 0.

Les lettres les plus fréquentes dans la colote 0 du texte sont :

I>W>M>X>G>E>S>H

Trouvons le décalage de chaque colonne par rapport à la colonne 0 :

Pour la colonne 1 avec K = 16 on a : IC(x,y-k) = 0.06684
Pour la colonne 2 avec K = 13 on a : IC(x,y-k) = 0.06277
Pour la colonne 3 avec K = 0 on a : IC(x,y-k) = 0.05977
Pour la colonne 4 avec K = 6 on a : IC(x,y-k) = 0.06621
Pour la colonne 5 avec K = 22 on a : IC(x,y-k) = 0.06505

On a donc :
k1 = k0 +16
k2 = k0 +13
k3 = k0
k4 = k0 +6
k5 = k0 +22

Faisons un premier essai :
On sait que la lettre la plus utilisée dans la langue anglaise est E.
On pose donc :

$E_{k_0}(E) = I$ D'où $4 + k_0 = 8$ => $k_0 = 4$ (E)
On a donc : $k_1 = k0 + 16 = 20$ (U)
De même : $k_2 = 17$ (R)
$k_3 = 4$ (E)
$k_4 = 10$ (K)
$k_5 = 26$ (A)

La clef supposée est donc : k=EUREKA

Essayons de déchiffrer le texte →

Until modern times cryptography referred almost exclusively to encryption which is the process of converting ordinary information called plain text into un intelligible text called cipher text. Decryption is there verse in other words moving from the unintelligible cipher text back to plain text. A cipher is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a key this is a secret ideally known only to the communicants usually

a short string of characters which is needed to decrypt the cipher text. A cryptosystem is the ordered list of elements of finite possible plain texts finite possible cypher texts finite possible keys and the encryption and decryption algorithms which correspond to each key. Keys are important as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless or even counter productive. For most purposes historically ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks.

La clef trouvée est donc la clef qui a été utilisée pour chiffrer le text original.

K = EUREKA