ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

UNIVERSITY OF PIRAEUS
DEPARTMENT OF DIGITAL SYSTEMS

Κρυπτογραφια

Εργασια 2

Γεωργιάδης Άγγελος E12029

1. Caesar Decryption

Ciphertext : S DGFy LAEw syG, AF s ysDsPQ xsJ, xsJ sOsQ ....
aL AK s HwJAGv Gx uANAD OsJ. jwtwD KHsuwKzAHK, KLJACAFy xJGE s zAvvwF tsKw, zsNw OGF LzwAJ xAJKL NAuLGJQ sysAFKL Lzw
wNAD YsDsuLAu WEHAJw.
VMJAFy Lzw tsLLDw, JwtwD KHAwK EsFsywv LG KLwsD KwuJwL HDsFK LG Lzw WEHAJw'K MDLAEsLw OwsHGF, Lzw VWSlZ klSj, sF
sJEGJwv KHsuw KLsLAGF OALz wFGMyz HGOwJ LG vwKLJGQ sF wFLAJw HDsFwL.
hMJKMwv tQ Lzw WEHAJw'K KAFAKLwJ sywFLK, hJAFuwKK dwAs JsuwK zGEw stGsJv zwJ KLsJKzAH, uMKLGvAsF Gx Lzw KLGDwF
HDsFK LzsL usF KsNw zwJ HwGHDw sFv JwKLGJw xJwwvGE LG Lzw ysDsPQ ....

Κλειδί : 18

Plaintext : A LONg TIMe agO, IN a gaLaXY faR, faR aWaY iT IS a PeRIOd Of cIVIL WaR rebeL SPaceShIPS, STRIKINg fROM a hIddeN baSe haVe WON TheIR fIRST VIcTORY agaINST The eVIL GaLacTIc EMPIRe DURINg The baTTLe, RebeL SPIeS MaNaged TO STeaL SecReT PLaNS TO The EMPIRe S ULTIMaTe WeaPON The DEAtH stAr aN aRMORed SPace STaTION WITh eNOUgh POWeR TO deSTROY aN eNTIRe PLaNeT pURSUed bY The EMPIRe S SINISTeR ageNTS pRINceSS leIa RaceS hOMe abOaRd heR STaRShIP cUSTOdIaN Of The STOLeN PLaNS ThaT caN SaVe heR PeOPLe aNd ReSTORe fReedOM TO The galaxy

Επεξήγηση : Για να βρω το κλειδι χρησιμοποιησα το προγραμμα CaesarCipherTest.py στο οποιο βαζοντας ένα δειγμα από το κειμενο (π.χ. “S DGFy”)εμφανιζει ολες τις δυνατες αποκρυπτογραφησεις μαζι με το αντιστοιχο κλειδι για κάθε αποκρυπτογραφηση.Βαζοντας λοιπον μια φραση από το ciphertext παρατηρουμε ότι για κλειδι 18 η εξοδος είναι φραση της αγγλικης γλωσσας.Τελος εκτελωντας το CaesarDecryption.py εχουμε το plaintext.

2. Affine Decryption

Ciphertext : Hflyy Lqtuw jel hfy Yxdyt-mqtuw stnyl hfy wmk,
Wydyt jel hfy Noglj-xelnw qt hfyql fgxxw ej whety,
Tqty jel Ielhgx Iyt neeiyn he nqy,
Ety jel hfy Nglm Xeln et fqw nglm hflety
Qt hfy Xgtn ej Ielnel ofyly hfy Wfgneow xqy.
Ety Lqtu he lsxy hfyi gxx, Ety Lqtu he jqtn hfyi,
Ety Lqtu he rlqtu hfyi gxx gtn qt hfy nglmtyww rqtn hfyi
Qt hfy Xgtn ej Ielnel ofyly hfy Wfgneow xqy.

Κλειδιά : α=11 , β=6

Plaintext : THREE RINGS FOR THE ELVEN-KINGS UNDER THE SKY, SEVEN FOR THE DWARF-LORDS IN THEIR HALLS OF STONE, NINE FOR MORTAL MEN DOOMED TO DIE, ONE FOR THE DARK LORD ON HIS DARK THRONE IN THE LAND OF MORDOR WHERE THE SHADOWS LIE. ONE RING TO RULE THEM ALL, ONE RING TO FIND THEM, ONE RING TO BRING THEM ALL AND IN THE DARKNESS BIND THEM IN THE LAND OF MORDOR WHERE THE SHADOWS LIE.

Επεξήγηση : Ομοια με το CaesarCipherTest.py ,το AffineCipherTest.py εμφανιζει για κάθε κλειδι β(το οποιο παιρνει τιμες από 1 εως 26) και για κάθε κλειδι α(το οποιο είναι περιττος,δηλαδη παιρνει τιμες 1,3,5,…,23,25) τις πιθανες αποκρυπτογραφησεις.Ετσι αμα βαλουμε την λεξη “HFLYY” πηγαινοντας για β=6 και α=11 ή α=13 εχουμε την λεξη “THREE”.Ομως επειδη gcd(13,26)=13 ≠ 1 συμπεραινουμε ότι το κλειδι α θα είναι 11.Εκτελουμε λοιπον το AffineDecryption.py με α=11 και β=6 και παιρνουμε το plaintext.

3. Vigenere Decryption

Ciphertext : Qwtguhexcymwlhtzltjiwyuxethizyetcowqbpgzcwb

Κλειδι : xppuuf

Plaintext : THEMACHINESROSEFROMTHEASHESOFTHENUCLEARFIRE

Επεξήγηση : Με τη Μέθοδο Kasiski παρατηρούμε ότι το ζευγάρι γραμμάτων "**et"** επαναλαμβάνεται με απόσταση 6 χαρακτήρων **"ethizyet"**.
Άρα το κλειδί πιθανότατα είχε μήκος 6,3,2 ή 1.
Χρησιμοποίησα το site http://www.dcode.fr/vigenere-cipher , για τη διευκόλυνση της εύρεσης κλειδιού, εφόσον ήξερα το πιθανό μήκος του κλειδιού. Μετα από πολλες προσπαθειες και δοκιμες παρατηρησα ότι το κλειδι **"XPPGUF"** εβγαζε αποτελεσμα το plaintext **"THEAACHINSSROSETROMTHSASHESCFTHENICLEARTIRE"** το οποιο είναι μια καλη προσεγγιση του κανονικου plaintext και εμφανιζει μερικες λεξεις από το plaintext όπως πχ **"ASHES","THE","ROSE"**.Δοκιμαζοντας στο ιδιο site διαφορετικες παραλαγες του κλειδιου αυτου(αλλαζοντας ένα γραμμα κάθε φορα) βρηκα το κλειδι και δοκιμαζοντας το στο προγραμμα αποκρυπτογραφησης VigenereDecryption.py βγηκε το αποτελεσμα.Δυστηχως όμως δεν καταφερα να φτιαξω μονος μου ένα προγραμμα ελεγχου κλειδιου.