Lab 4: Attacking Classic Crypto Systems

Objectives:

- To attack classic crypto systems

Submission:

- Corresponding source files and a report explaining the approaches taken.

Instruction:

In this lab, we are going to break several classic crypto systems. The main idea is to demonstrate the weaknesses of these crypto systems. Use any programming language to code programs that could be used to break these systems by decrypting the corresponding cipher. Then submit the corresponding source files.

Also, prepare a report in which outline the approach you have taken to break each crypto system. You don't need to be concise. I would like to know your thought process of attacking the crypto system. Therefore, add as many details as possible.

Problem – 2 (Marks 15)

The following two ciphers have been created using a substitution cipher. Write a program to decipher them.

Which input was easier to break? Explain your answer.

For your convenience, a frequency distribution of English characters is given in the next page.

Cipher-1: *MIT EKTC EGFLOLML GY EGGHTK, MIT KGZGML MBKL BFR EBLT, BFR MIT LEOTFMOLML RK. BDTSOB ZKBFR (HKGYTLLGK ZKBFR'L RBWUIMTK), RK. KGDOSSA, BFR RK. RGAST. BYMTK MKBXTKLOFU MIT CGKDIGST, EGGHTK, RGAST BFR BDTSOB WLT B KBFUTK MG OFXTLMOUBMT DOSSTK'L HSBFTM, BF GETBF CGKSR. BYMTK SBFROFU OF QFTT-IOUI CBMTK BFR YOFROFU GFSA CKTEQBUT YKGD DOSSTK'L TVHTROMOGF, B UO*

Cipher-2: *RTEQBKR LGGF DTTML B LGXOTM HGSOET EGFMBEM CIG MWKFL GWM MG ZT GFT GY MIT FTVWL-LOV KTFTUBRTL OF ROLUWOLT. RTEQBKR KTMOKTL MIT BFRKGOR, MITF YSOTL GYY MG KTMOKT IOL FTVM MBKUTM: BF GHTKB LOFUTK BFRKGOR. IGCTXTK, IT OL LWRRTFSA BKKTLMTR BFR RTMBOFTR BM B HGSOET RTHBKMDTFM IT IBL FTXTK ITBKR GY ZA B HGSOET GYYOETK CIGD IT OL LWKHKOLTR FTXTK MG IBXT DTM. BM MIOL LMKBFUT LMBMOGF, RTEQBKR'L CGKSRXOTC OL LIBQTF CITF BF GYYOEOBS FBDTR UBKSBFR BEEWLTL RTEQBKR IODLTSY GY ZTOFU BF BFRKGOR. BYMTK B LTKOTL GY DALMTKOGWL KTXTSBMOGFL BM MIT LMBMOGF, RTEQBKR HGFRTKL MIT TMIOEBS BFR HIOSGLGHIOEBS JWTLMOGFL IOL SOFT GY CGKQ KBOLTL KTUBKROFU BFRKGOR OFMTSSOUTFET, TDHBMIA, BFR CIBM OM DTBFL MG ZT IWDBF. HIOS KTLEI, MIT LMBMOGF'L KTLORTFM ZGWFMA IWFMTK, KTMKOTXTL MTLMOFU TJWOHDTFM MG RTMTKDOFT OY IOL EGCGKQTKL--OFESWROFU RTEQBKR BFR KTLEI IODLTSY--BKT BFRKGORL GK IWDBFL. UBKSBFR LWZLTJWTFMSA KTXTBSL MIBM MIT TFMOKT LMBMOGF OL B LIBD, LMBYYTR TFMOKTSA ZA BFRKGORL, OFESWROFU UBKSBFR IODLTSY. KTLEI LIGGML UBKSBFR OF MIT ITBR, BSSGCOFU IOD BFR RTEQBKR MG TLEBHT; MGUTMITK, MITA YOFR MIT GHTKB LOFUTK, CIGD KTLEI ZKWMBSSA KTMOKTL OF EGSR ZSGGR. BSMIGWUI KTLEI BFR RTEQBKR BKT FGC EGSSBZGKBMGKL, TBEI LMOSS CGKKOTL MIBM IT (GK MIT GMITK) DOUIM ZT BF BFRKGOR. RTEQBKR BRDOFOLMTKL MIT TDHBMIA MTLM MG IODLTSY BFR MG KTLEI, CIOEI EGFYOKDL MIBM KTLEI OL B IWDBF ZTOFU--LODHSA B HBKMOEWSBKSA KWMISTLL GFT--BFR MIBM RTEQBKR OL BSLG IWDBF, ZWM COMI B LTFLT GY TDHBMIA YGK MIT BFRKGORL. GFSA MIKTT GY MIT FTVWL-LOV BFRKGOR YWUOMOXTL*

KTDBOF, BFR GFT, HKOL LMKBMMGF, DGXTL OFMG BF BHBKMDTFM ZWOSROFU CIGLT GFSA GMITK OFIBZOMBFM OL PGIF K. OLORGKT, B KBROGBEMOXTSA RBDBUTR, OFMTSSTEMWBSSA ZTSGC-BXTKBUT IWDBF ESBLLOYOTR BL B LHTEOBS. MIT SGFTSA OLORGKT BMMTDHML MG ZTYKOTFR ITK. KGA BFR OKDUBKR ZBMA