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.

0000000000

……

Cipher-2: *EGFLORTK B KGGD. MIT SGEBMOGF GY MIT KGGD OL FGM OF JWTLMOGF BM MIT DGDTFM. OM OL DTKTSA LWYYOEOTFM MG LBA MIBM OF MIBM KGGD, DGKT MIBF BFACITKT, MIT LTEGFR YGWFRBMOGF TVOLMTR. OM CBL B KGGD CIOEI, MIKGWUI MIT ETFMWKOTL, IBR ZTTF MIT BZGRT GY HWKT LEOTFET ATM OM IBR FGFT GY MIT UBRUTML COMI CIOEI, MIKGWUI DOSSTFFOB GY BLLGEOBMOGF, LEOTFET IBL EGDT MG ZT EGFLORTKTR TJWOXBSTFM. OM CBL B LEOTFET, OFLMTBR, CIOEI RTBSM COMI DBMITDBMOEBS EGFETHML GFSA, OF B DBFFTK LODOSBK MG MIT LHTEWSBMOGF GY BFEOTFM, BFEOTFM KBETL OF MIT HKODOMOXT, HKTIOLMGKOE RBAL ZTYGKT MTEIFGSGUA IBR EGDT MG ZT; ZTYGKT DBF IBR LHKTBR ZTAGFR B LOFUST, FGC-WFQFGCF CGKSR. YGK GFT MIOFU, MITKT CBL OF MIBM KGGD - HKGMTEMTR ZA B DTFMBS LEOTFET BL ATM WFBLLBOSBZST ZA MIT EGDZOFTR HIALOEBS DOUIM GY MIT KTLM GY MIT UBSBVA - MIT HKODT KBROBFM, CIOEI ITSR OF OML XOMBSL MIT LTSRGF HSBF - EGDHSTMT. YGK BFGMITK, MITKT CBL B DBF, MGG, OF MIBM KGGD - MIT YOKLM LHTBQTK. IT CBL MIT MCTSYMI OF MIT SOFT GY EIOTY UWBKROBFL GY MIT HSBF, BFR IOL MOMST ZGKT FG RTTHTK LOUFOYOEBFET MIBF MIT YBEM MIBM BM MIT UBMITKOFUL GY MIT STBRTKL GY MIT LTEGFR YGWFRBMOGF, IT LHGQT YOKLM. IOL HKTRTETLLGK IBR ZTBMTF MIT DWST, ZWM MIT CKTEQBUT GY MIBM UOUBFMOE LMKWUUST LMOSS SOMMTKTR MIT HBMI GY MIT HSBF- YGK MCTFMA-YOXT ATBKL, IT, BFR IOL BRDOFOLMKBMOGF, IBR ZTTF MKAOFU MG YGKET B UBSBVA GY LMWZZGKF BFR LMWHOR IWDBF ZTOFUL ZBEQ MG MIT HBMI- OM CBL B MTKKOZST MBLQ. MIT YOKLM LHTBQTK SGGQTR WH BM MIT GHTFOFU RGGK. TXTF CIOST, OF MIT SGFTSOFTLL GY MIT KGGD, IT EGFLORTKTR IOL JWBKMTK ETFMWKA GY TYYGKM, CIOEI FGC LG LSGCSA BFR OFTXOMBZSA BHHKGBEITR OML ESODBV; TXTF CIOST IT IBR ZTTF LG TFUBUTR, IOL DOFR*

IBR ZTTF EGFLORTKOFU MIT FTCEGDTK COMI B UTFMST TVHTEMBMOGF. B AGWMI, B LMWRTFM, GFT GY MIGLT CIG DOUIM MBQT GXTK, TXTFMWBSSA.