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: *KTFRTNXGWL COMI KBDB ZA BKMIWK E. ESBKQT KTEGWFML MIT DOLLOGF GY MIT LHBETLIOH TFRTBXGWK BFR OML LMBYY BL OM EGDHSTMTL BF TVHSGKBMGKA DOLLOGF GF BF BSOTF LHBET XTLLTS MKBXTSOFU MIGWUI MIT LGSBK LALMTD. MIT FGXTS WFRTKSOFTL MIT ROYYOEWSMOTL TFEGWFMTKTR ZA MIT TVHSGKTKL BL MITA MKA MG BRBHM MG BF TFXOKGFDTFM MIBM GZTAL MIT KWSTL GY HIALOEL OF B HSBET MIBM*

Cipher-2: *RWKOFU MIT SBLM JWBKMTK GY MIT MCTFMA LTEGFR ETFMWKA, DBFQOFR LHGMMTR BF WFQFGCF BFR WFTVHTEMTR LHBET GZPTEM MKBXTSOFU BEKGLL MIT HBMI GY MIT HSBFTML MGCBKR MIT LWF. MIT GZPTEM OL FBDTR KBDB BFR LEOTFMOLML LTFR B HKGZT FTBK MIT GZPTEM. MIT HKGZT ORTFMOYOTL KBDB BL BF BKMOYOEOBS, DTMBSSOE GZPTEM MIT LONT GY B LDBSS DTMTGKOMT, HTKYTEMSA EASOFRKOEBS BFR BHHBKTFMSA OFBEMOXT. B MTBD GY TVHSGKTKL OL MITF LTFM GF B DOLLOGF MG SBFR GF MIT GZPTEM BFR TVHSGKT OML EGFMTFM. MIT MTBD BZGBKR LHBETLIOH TFRTBXGWK ROLEGXTKL B CGKSR CIGLT HIALOEBS EIBKBEMTKOLMOEL BKT XTKA ROYYTKTFM YKGD MIBM CIOEI HKTXBOSL TSLTCITKT OF MIT WFOXTKLT BFR CITKT MIT SBCL GY HIALOEL BHHSA MG B LTSY-TFESGLTR, LTSY-LWYYOEOTFM EASOFRKOEBS CGKSR. BM YOKLM, MIT CGKSR GY KBDB LTTDL MG IBXT ZTTF TOMITK BLSTTH GK RTBR YGK B DOSSOGF ATBKL BL OM RKOYMTR MIKGWUI LHBET. MITF BL OM UTML FTBKTK MG MIT LWF, MIT EGSR BFR RBKQ BSOTF LIOH BCBQTFL COMIGWM B CBKFOFU BFR SOUIML WH. SOYT TDTKUTL YKGD MIT RTHMI GY MIT EASOFRKOEBS LTB MIBM EWML MIT KBDB CGKSR OF IBSY. TXGSWMOGF MBQTL HSBET BM B IOUISA BEETSTKBMTR HBET BL LHTEOTL GY BSOTFL BKT EGFLMBFMSA ZGKF BFR SBMTK KTEAESTR ZA MITOK TFXOKGFDTFM. MIT TVHSGKTKL TFEGWFMTK ROYYTKTFM, FGF-MIKTBMTFOFU LHTEOTL GY BSOTFL. MITLT BSOTF EKTBMWKTL, HBKMA ZOGSGUOEBS BFR HBKMSA KGZGMOE, BKT ZTOFU KTHTBMTRSA KTHSBETR ZA DGKT EGDHSTV ZTOFUL GXTK EAESTL SBLMOFU B YTC RBAL. MIT BRXTFMWKTKL YBET ROYYTKTFM MTEIFGSGUOEBS EIBSSTFUTL BFR IBXT MG KTSA GF*

ZGMI MITOK GCF QFGCSTRUT BFR MIT BRXOET GY B EGDDOMMTT GY LEOTFMOLML SGEBMTR GF B ROYYTKTFM HSBFTM MG EGFJWTK MIT LTEKTML GY KBDB. MIT HBMI GY MIT BSOTF LIOH YGKETL MIT TVHSGKTK'L XTLLTS MG TFR OML DOLLOGF BFR STBXT PWLM BL MIT CGKSR GY KBDB LTTDL MG KTXTKM MG OML GKOUOFBS RBKQ, LOSTFM BFR BHHBKTFMSA LSTTHA LMBMT. KBDB MITF KTBSOUFL