Lab 2: 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 systems. Therefore, add as many details as possible.

In addition, you will also need to write code for the Vignere crypto system.

Problem – 1 (Marks 3)

The following cipher has been created using the Caesar cipher. Write a program to decipher it.

Cipher: krclxrwrbxwnxocqnlxxunbcrwencrxwbrwanlnwccrvnb

Problem – 2 (Marks 12 (6 + 6))

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: *IT CNJ FGM ETKMNOF CITMITK MIT JWF JIGFT GK YGK MINM SNMMTK CITMITK OM CNJ ZNB GK FOUIM IT CNJ NJINSTZ MG NJQ NDD MIT HDNFTM JTTSTZ MG DOXT RTFTNMI STMND MIT STND GY CIOEI IT INZ PWJM HNKMNQTF INZ RTTF DNRTDTZ DWFEITGF RWM MITKT CTKT SNFB HDNFTMJ CIOEI DOXTZ N JMNFZNKZ MOSTJENDT MINM MGGQ FG NEEGWFM GY MIT HTKINHJ OFEGFXTFOTFM NDMTKFNMOGF GY ZNB NFZ FOUIM. MIT KNMT GY HDNFTMNKB MWKFOFUJ ZOYYTKTZ, NFZ IT ZOZ FGM QFGC MINM GY MKNFMGK*

Cipher-2: *VDUMU NEC E NEFF EDUEY SV ZUOEH DSOD SH VDU ESM EHY URVUHYUY BKNEMY LBV LI CSODV SV NEC MSYYFUY NSVD DLFUC VDEV NUMU VDU GLBVDC LI VBHHUFC OEEF'C VERS GLAUY VLNEMY LHU, VDUH KFBHOUY SHVL SV ILM E GLGUHV OEEF NLHYUMUY SYFP DLN DSC YMSAUM TLBFY KSTX LBV LHU EGLHO CL GEHP VDUMU NEC HLN LHFP ZFETXHUCC NSVD HLVDSHO ZBV VDU KECV-IFECDSHO LI E TLFLMUY CSOHEF FSODV VL MUFSUAU VDU OFLLG VDU ESM NEC IBFF LI E MBCDSHO CLBHY OEEF FUEHUY ILMNEMY EOESHCV YUTUFUMEVSLH VDUH EHY VDU VERS KLKKUY LBV LI VDU VBHHUF EHY YUCTUHYUY VL OMLBHY-FUAUF LHTU GLMU VDU FBRLM DLVUF CESY VDU YMSAUM BHHUTUCCEMSFP DU DUFKUY OEEF NSVD DSC ZEOOEOU ETTUKVUY E VUHVD-TMUYSV VSK NSVD E ZBCSHUCCFSXU ESM KSTXUY BK E NESVSHO KECCUHOUM EHY NEC MSCSHO EOESH*

SH EFF VDSC IMLG VDU GLGUHV LI YUZEMXEVSLH VDUMU DEY ZUUH HL OFSGKCU LI CXP VMEHVLM EV VDU ZUOSHHSHO LI VDU VDSMVUUHVD GSFFUHHSBG VDSC VUHYUHTP MUETDUY SVC TFSGER EC VDU TUHVUM LI VDU SGKUMSEF OLAUMHGUHV ILM BHZMLXUH DBHYMUYC LI OUHUMEVSLHC EHY FLTEVUY EC SV NEC VLNEMY VDU TUHVMEF MUOSLHC LI VDU OEFERP EGLHO VDU GLCV YUHCUFP KLKBFEVUY EHY SHYBCVMSEFFP EYAEHTUY NLMFYC LI VDU CPCVUG, SV TLBFY CTEMTUFP DUFK ZUSHO VDU YUHCUCV EHY MSTDUCV TFLV LI DBGEHSVP VDU METU DEY UAUM CUUH SVC BMZEHSQEVSLH, KMLOMUCCSHO CVUEYSFP DEY ISHEFFP MUETDUY VDU BFVSGEVU. EFF VDU FEHY CBMIETU LI VMEHVLM CJBEMU GSFUC SH URVUHV NEC E CSHOFU TSVP VDU KLKBFEVSLH EV SVC DUSODV NEC NUFF SH URTUCC LI ILMVP ZSFFSLHC VDSC UHLMGLBC KLKBFEVSLH NEC YUALVUY EFGLCV UHVSMUFP VL VDU EYGSHSCVMEVSAU HUTUCCSVSUC LI UGKSMU EHY ILBHY VDUGCUFAUC EFF VLL IUN ILM VDU TLGKFSTEVSLHC LI VDU VECX (SV SC VL ZU MUGUGZUMUY VDEV VDU SGKLCCSZSFSVP LI KMLKUM EYGSHSCVMEVSLH LI VDU OEFETVST UGKSMU BHYUM VDU BHSHCKSMUY FUEYUMCDSK LI VDU FEVUM UGKUMLMC NEC E TLHCSYUMEZFU IETVLM SH VDU IEFF) YESFP IFUUVC LI CDSKC SH VDU VUHC LI VDLBCEHYC ZMLBODV VDU KMLYBTU LI VNUHVP EOMSTBFVBMEF NLMFYC VL VDU YSHHUM VEZFUC LI VMEHVLM SVC YUKUHYUHTU BKLH VDU LBVUM NLMFYC ILM ILLY EHY SHYUUY ILM EFF HUTUCCSVSUC LI FSIU GEYU VMEHVLM SHTMUECSHOFP ABFHUMEZFU VL TLHJBUCV ZP CSUOU SH VDU FECV GSFFUHHSBG LI VDU UGKSMU VDU GLHLVLHLBCFP HBGUMLBC MUALFVC GEYU UGKUMLM EIVUM UGKUMLM TLHCTSLBC LI VDSC EHY SGKUMSEF KLFSTP ZUTEGU FSVVFU GLMU VDEH VDU KMLVUTVSLH LI VMEHVLM'C YUFSTEVU WBOBFEM AUSH

Frequency distribution English characters

a:	8.05%	b:	1.67%	c:	2.23%	d:	5.10%
e:	12.22%	f:	2.14%	g:	2.30%	h:	6.62%
i:	6.28%	j:	0.19%	k:	0.95%	l:	4.08%
m:	2.33%	n:	6.95%	o:	7.63%	p:	1.66%
q:	0.06%	r:	5.29%	s:	6.02%	t:	9.67%
u:	2.92%	v:	0.82%	w:	2.60%	x:	0.11%
y:	2.04%	z:	0.06%				

Problem – 3 (Marks 5)

Write a program to simulate the Vignere crypto system having the following properties and inputs. The program should have encryption as well as decryption facilities with the provision to ask the user the operation the user would like to perform.

Key: pinkfloyd

Sample Input/Output: Ethereum is an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract functionality

Sample Output/Input: tbuowpik lh ia yupb-qrjzpo, ufpjlr, jyyhvqfdxv-okxpr blhbesgfhcg rwzzzewlj etndkzfk dcl bzjcorlco fixesk itigewtbe vbied hzbrupkg pzyqrldvnvnem