Lab 2: Attacking Classic Crypto Systems

Objectives:

- To attack classic crypto systems

Submission:

- Checkpoints 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. Once a system is broken, show the result to your teacher.

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.

Checkpoint – 1 (Marks 5)

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

Cipher: zljbypafhukwypchjfptwvzljvuayhkpjavyfylxbpyltluazavmbsmps

Write a program to break it and display the result. Show it your teacher.

Checkpoint – 2 (Marks 8 + 7)

The following two ciphers have been created using a substitution cipher with different keys. Write a program to decipher each of 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: cz uczsdj qv lcf day vjqyq vdos ws kwz icwavgo ygsm sq zcm fqqy-lmd sq skd fgdzsz. jguqgjz qv zsjcafd dedasz kcy lm aqn zijdcy coo qedj skd vwdoy, lgs vjqyq nqgoy qaom zcm aq yqgls dedjmskwaf nwoo ld todcjdy gi wa skd uqjawaf. clqgs uwyawfks tcjjwcfdz tcud vqj skd wuiqjscas vqox. qad lm qad skdm jqoody cncm, vwoody nwsk vgoo lgs edjm gazcswzvwdy kqllwsz. fcjydadjz tcud lm cjjcafdudas, cay jduqedy wa nkddo-lcjjqnz skqzd skcs kcy wacyedjsdasom jducwady ldkway. awfks zoqnom

Cipher-2: cej amxziu, gobxm om zbz uij kiqhmj wfwqdx'a gwqubuh, zbz uij jobul ik bj gbjo wud hqmwj zmhqmm ik niunmujqwjbiu. oba kiqjbmjo cbqjozwd nwfm wuz gmuj--gbjo jom eaewx vadnoixihbnwx cxig. kiqjd! om gwa uij dieuh wud xiuhmq. xbkm ui xiuhmq ajqmjnomz cmkiqm obf wa w ywaj eunowqjmz kbmxz, bja oiqbpiu xiaj bu jom zbajwunm. om owz cmmu iu jqwujiq kiq mbhoj dmwqa wuz jom jbfm owz vwaamz tebnlxd. wuijomq mbhoj dmwqa wuz om giexz cm umwqxd kbkjd. ixz whm giexz cm xiifbuh. wuz om owz uij mymu fwzm w zmnmuj cmhbuubuh bu vadnoiobajiqd! dehi wfwqdx avilm cqbhojxd ik xwga wuz giqlmz iej oba mtewjbiua cd fwlbuh zwqbuh waaefvjbiua cwamz iu bujebjbiu. cej oig niexz ium viaabcxd jmaj

joiam waaefvjbiua? vadnoiobajiqd gwa uij dmj wu msvmqbfmujwx anbmunm. jom nifvxmjm ajezd ik vadnoiobajiqd giexz qmtebqm msvmqbfmuja jowj giexz buyixym giqxza ik vmivxm, nmujeqbma ik jbfm--wuz w jijwx xwnl ik mjobnwx qmaviuabcbxbjd. bj viamz wu bfviaabcxm vqicxmf wuz om qmamujmz owybuh ji avmuz wud jbfm gowjmymq iu zmvwqjfmujwx jwala, ai om gwxlmz oifm wj jom muz ik jom zwd bu w fiqiam fiiz. iqzbuwqbxd om niexz wxgwda nieuj iu w gwxl joqieho jom nwfvea ji qieam oba avbqbja. ajqmmxbuh eubymqabjd gwa obho-zifmz wuz jom nwfvea hwym jom kmmxbuh ik cmbuh iej bu jom ivmu gbjoiej jom umnmaabjd ik muzeqbuh jom lbuz ik gmwjomq om owz msvmqbmunmz iu oba ium (wuz iuxd) ybabj ji jom bfvmqbwx vwxwnm. jomqm gmqm jqmma, xwgua, gwxla, wxfiaj wa joieho om gmqm iu jom nwfvea ik oba ixz nixxmhm iu oba oifm giqxz ik omxbniu. jom bxxeabiu ik nxiezbumaa owz cmmu wqqwuhmz kiq jom zwd gbjo jom aeuxbhoj (ui aeu, ik nieqam, reaj aeuxbhoj) wvvmwqbuh wuz zbawvvmwqbuh wj izz bujmqywxa. wuz bj gwa w xbjjxm niix, reaj w xbjjxm. bj ammfmz ji amxziu jowj jom niix zwda nwfm w xbjjxm fiqm kqmtemujxd jowu jomd eamz ji. gwa jqwujiq awybuh mumqhd? gwa bj bunqmwabuh bumkkbnbmund? iq (wuz om anigxmz bugwqzxd wa om joiehoj bj) gwa om hmjjbuh ixz wuz gwa oba cxiiz hmjjbuh jobu? om vxwnmz oba owuza bu

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%				