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: ftqzqjfwuxxqdmbbiuxxoaynuzqoxagpymotuzqxqmdzuzsuafmzpnxaowotmuz

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: tqmrajq ya gowopxyoap, fxog vcasqffac ycqmxtpql, tka kxg fqxyqg kqcfqms op x topiqg xcjrkxoc op scapy as ykq socq. jl pxjq of vcasqffac ycqmxtpql. lae jxl pay kxwq fqqp jq zqsacq. o sopg ykxy gqfrqpgopi yaa asyqp opya ykq kefymq xpg zefymq as ykq jxop frkaam rmaegf jl oppqc qlq. pazagl fxog xplykopi ya ykof qbycxacgopxcl vcapaeprqjqpy. vcasqffac ycqmxtpql gqmorxyqml cqxccxpiqg kqc fkxtm xpg rapyopeqg, fa lae kxwq rkafqp ya fyegl gowopxyoap, ykq jafy gossoremy as xmm jxiorxm xcyf. o jefy

Cipher-2: przu ekttkyzh hamapva ksp ke prz mxag tksgbz agpk prz kdczvjxpakg czipakg, xgh ckkg yzvz cappagb xp x pxdtz sghzv x ham tabrp yxpiragb prz mkjagb fxgkvxmx ke prz cpxvc. cfxiz cpxpakg kgz vzjktjzh kgiz x magspz, xgh prz izgpvaesbxt ekviz bzgzvxpzh du prac ctky cfag fvkhsizh xg xvpaeaiaxt bvxjapu znsxt pk prz mkkg'c. prac, ap rxh dzzg hacikjzvzh, yxc x bkkh ikmfvkmacz dzpyzzg zxvpr bvxjapu xgh gk bvxjapu xp xtt; mkvzkjzv, ap bxjz mkkg-dksgh fxcczgbzvc x irxgiz pk dzikmz xiitamxpaozh. kspcahz prz xtmkcp agjacadtz yaghkyc, zxvpr xgh cpxvc mxvirzh ag x catzgp fvkizccakg. xp prz mkmzgp, prac cahz ke prz cpxpakg yxc patpzh xyxu evkm prz csg; kprzvyacz, ap yksth rxjz dzzg amfkccadtz pk tkkw ksp, ekv prz tksgbz yksth

rxjz dzzg dtxcpzh yapr tabrp. zjzg xc ap yxc, prz btxvz ke prz zxvpr, eattagb rxte prz cwu, hvkygzh xtt dsp prz dvabrpzv cpxvc. dsp zxvpr yxc yxgagb, xc prz cpxpakg kvdapzh pkyxvh prz gabrp cahz ke prz ftxgzp; ag x ezy magspzc ap yksth dz x rsbz dtxiw hacw, cfxgbtzh yapr prz tabrpc ke iapazc. xgh przg prz cwu yksth dztkgb pk prz cpxvc. gky, cxah hamapva, xepzv rz rxh cyaeptu hkygzh rac eavcp hvagw xgh yxc pkuagb yapr prz czikgh, yrxp'c xtt prac xdksp xg zfahzmai ag prz s.c. czipkv? a yxgpzh pk bk przvz kg prac pvaf. 'gk, fvkezcckv,' przu pkth mz. 'yz'vz jzvu ckvvu, dsp przvz'c x cpvaip nsxvxgpagz sgpat esvprzv gkpaiz.' a fsttzh xtt prz cpvagbc a iksth; ap yxc gk scz. gky uks pztt mz yrxp'c rxffzgagb. ekvpu-eajz magspzc txpzv, prz xvazc-td tsgxv ixvvazv fsttzh xyxu evkm prz cpxpakg. przvz yxc gkgz ke prz fkyzv xgh esvu ke x pxwzkee evkm zxvpr - kgtu xg xtmkcp agxshadtz, exv-kee yracptagb xc prz tky-prvscp ftxcmx lzpc dtxcpzh przav ztzipvaeazh cpvzxmc agpk cfxiz. prz bzgptz fscr txcpzh ekv mkvz prxg eaepzzg magspzc, xgh prz math xiiztzvxpakg yksth gkp rxjz fvzjzgpzh xgukgz evkm mkjagb xvksgh prz ixdag. dsp yrzg ap yxc kjzv, prz craf yxc gk tkgbzv dksgh pk zxvpr, xc ap rxh dzzg yratz ap cpatt xiikmfxgazh

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%				