

## 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 attack two classic crypto systems. The main objective 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:** odroboewscdrolocdcwkbdkmyxdbkmdzvkdpybwyeddrobo

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:** af p xpkcaqvnkp pfg, af ipqe qpri, gauuikifc tpw, ceiri udvk tiki afgarxifrphni cd eao-wvmd popkwn, hiqpvri du ear jvaql vfgikrcpfgafm du cei xkafqaxnir du xrwqedearcdkw pfg du ear aopmafpcasi xkdhafmr afcd fit pkipt. ac tpr qdoudkcafz cd lfdt cepc au pfwceafm epxxifig cd ringdf eaorinu hiudki cei opceiopcaqr du cei uaing qdvng hi qdoxniciw tdklig dvc-pfg edt rndtnw ac xkdqiigig, pfg edt odvfcapfdvr cei dhrcpqnr--ceiki tdvng pc niprc kiopaf dfi mddg oafg cepc tdvng qdfcafvi cei kiripkqe

**Cipher-2:** aceah toz puvq vcdl omj puvq yudqecov, omj loj aum klu thmjuv hs klu zlcvu shv zcbkg guovz, upuv zcndu lcz vuwovroaeu jczyyuvomdu omj qmubyudkuj vukqvm. klu vcdluz lu loj avhqnlk aodr svhw lcz kvopuez loj mht audhvu o ehdoe eunumj, omj ck toz yhyqeoveg auocupuj, tlakupuv klu hej sher wcnlk zog, klok klu lcee ok aon umj toz sqee hs kqmmuez zkqssuj tckl kvuozquv. omj cs klok toz mhk umhqnl shv sowu, kluvu toz oezh lcz yvhehmnuj pcnhqv kh wovpue ok. kcwu thvu hm, aqk ck zuuwuj kh lopu eckkeu ussduk hm wv. aonncmz. ok mcmukg lu toz wqdl klu zowu oz ok scskg. ok mcmukg-mcmu klug aunom kh doee lcw tuee-yvuzuvpuj; aqk qmdlomnuj thqej lopu aum muovuv klu wovr. kluvu tuvu zhwu klok zlhhr klucv luojz omj klhqnlk klcz toz khh wqdl hs o nhhj klcmn; ck zuuwuj qmsocv klok

omghmu zlhqej yhzuz (oyyovumkeg) yuvyukqoe ghqkl oz tuee oz (vuyqkujeg) cmubloqzkcaeu tuoekl. ck tcee lopu kh au yocj shv, klug zocj. ck czm'k mokqvoe, omj kvhqaueu tcee dhwu hs ck! aqk zh sov kvhqaueu loj mhk dhwu; omj oz wv. aonncmz toz numuvhqz tckl lcz whmug, whzk yuhyeu tuvu tceecmn kh shvncpu lcw lcz hjckcu omj lcz nhjh shvkqmu. lu vuwocmuj hm pczckcmn kuvwz tckl lcz vueokcpuz (ubduyk, hs dhqvzu, klu zodrpceeu-aonncmzuz), omj lu loj womg juphkuj ojwcvuvz owhmn klu lhaackz hs yhhv omj qmcwyhvkomp sowcecu. aqk lu loj mh dehzu svcumjz, qmkce zhwu hs lcz ghqmnuv dhqzcmz aunom kh nvht qy. klu uejuzk hs kluzu, omj aceah'z sophqvcku, toz ghqm svjh aonncmz. tlum aceah toz mcmukg-mcmu lu ojhykuj svjh oz lcz lucv, omj avhqnlk lcu kh ecpu ok aon umj; omj klu lhyuz hs klu zodrpceeu- aonncmzuz tuvu scmoeeeg jozluj. aceah omj svjh loyyumuj kh lopu klu zowu acvkljog, zuykuwauv 22mj. ghq loj aukku dhwu omj ecpu luvu, svjh wg eoj, zocj aceah hmu jog; omj klum tu dom dueuavoku hqv acvkljog-yovkcuz dhwshvkoaeg khnuklu. ok klok kcwu svjh toz zkcee cm lcz ktuumz, oz klu lhaackz doeeuj klu cvvzyhmzcaeu ktumkcuz auktuum dlcejllhj omj dhwcmm hs onu ok klcvkg-klvuu

### 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% |          |          |