



ITT 402 - Cryptography and Network Security

Assignment # 1: Code Breakers

Assignment Start Date: 13-04-2023
Last Date of Submission: 24-04-2023

SHABANA KM

IDK19IT044

Problem Statement:

Decrypt the following cipher text using different crypto analytical techniques. Serial numbers corresponds to roll number of student for ciphertext decryption:

1. Fvby aptl pz sptpalk, zv kvu'a dhzal pa spcpun zvtlvul lszl'z spml. Kvu'a il ayhwwlk if kvnth
2. Vs lbh ybbx ng jung lbh unir va yvsr, lbh'yy nyjnlf unir zber. Vs lbh ybbx ng jung lbh qba'g unir va yvsr, lbh'yy arire unir rabhtu.
3. Ax qgm kwl qgmj ygsdk javaumdgmkdq zayz sfv al'k s xsadmjw, qgm oadd xsad stgnw wnwjqgfw wdkw'k kmuuwkk.
4. lhaved ozjz izzvpudlvv cmi au. zpx gb cbr izzv tqaq xh mmi qebavin epevdtv nhpexmv.
5. Mnomaq xkgkgfkx jpmj asc mxk mfsncjkna czieck. Bcjq niuk kvkxaszknkq.
6. hf cmiljwpq; jzzvpmbri pdw ma slcvedb rtkor
7. Lgc lfmvye ixk mvrvmvmlk: lfk svmzkkex ivd fsoiv elsjmdmlu; ivd M'o vcl esxk ipcsl lfk svmzkkex.
8. Rhn dghp rhn'kx bg ehox paxg rhn vtg'm ytee tlexxi uxvtnlx kxtebmr bl ybgteer uxmmxk matg rhnk wkxtfl.
9. yf xal gjhntk xaht rmi qeaz ah gwi mv gal akfco.
10. lv gayvi akfuv a kcn fmg gj tzzvprapvt o'dz ppererh dbpin etnj: mb zusw gb.
11. on dmi nxpw eal xklna, fmi xrb'g ahvz xh fvqqqnfvrnlrapvt
12. Yr stgd th ycd qnqdhy yctal ta ycd xrqsm. Jrhy idrisd dothy, ycnv th nss.
13. btdz es an dmi qavv xh rlm xhaafik. hpere ns an dmi qavv xh ztdz jtfvzzv
14. Ks oqqsdh hvs zcjs ks hwwby ks rsgsfjs
15. pb ba tfxmxv kh pf lhtxh itf ndht rmi urv xahn gh pf pzjzh itf ndht rmi urv rbh.
16. Vg qbrf abg qb gb qjryy ba qernzf naq sbetrg gb yvir
17. hucr iwzmrqv, yucr epcyc, snq d sdipitn aqbukmrpg: xapa aa lal mlhel wtnj
18. ftvj ma odht ahpetrf lh im odptp aa erv qmksvt uhalv galnf
19. cb ba frzzv khc zltx xh pf adht rmi guona ahvz ffr
20. btf vzzvp kuvhnx cmi urv entxp wmi fzgw wafqr qwgqbqv gt mhpxvrwk.
21. pn dmi ibyj pved wal fpcyc laht xzzvpmbri pdw ma jvedlvt, emi wcn bbyj rapvx gdht xzzvpmbri pdw ma lapvxsvt.
22. ma hrb'g lwi xapvty ss lalc yrv, aa wwi xalq ms oa erv
23. Fbzrgvzrf gur dhrfgvbafr ner pbzcyvpngrq naq gur nafjref ner fvzcyr
24. btnj maf'g tbpin ynvqlvt emiljwpq. qtnj ma sbpin vtvetbvt emiljwpq
25. Yaep zwqc wu lwqwzcx, ua xav'z oiuzc wz lwjwvm uaqcavc cluc'u lwhc. Xav'z nc zpiffcx ny xamqi
26. Un oiw biiq kl sjkl oiw jkhc ux bunc, oiw'bb kbskoa jkhc mipc. Un oiw biiq kl sjkl oiw rix'l jkhc ux bunc, oiw'bb xchcp jkhc cxiwyj.
27. cmil kbuq ma dtuubxh, vg rrb'g pwslx mb etddvt ygaqsbr ipdw'w dtvj. hrb'g uf xkrpeth ez brusm

28. ya ecegti mal pzjz aa xapvx ga hhwvwmz
29. Ah gmy usj gmyf wmktu fadaoytmyutg lawl kxd aj'u k hkatyfs, gmy catt hkat kzmns snsfgmxs stus'u uyoosuu.
30. Ojvikp lqti itivymnivi yqa uq. Lih xq qxi itiv wqei hq yqa mghnqah liktgxu nkjjgiv.
31. Khjwsv dgnw wnwjqozwjw qgm yg. Dwl fg gfw wnwj ugew lg qgm oalzgml dwsnafy zshhawj.
32. Ajm zqzmt hdipoz tjp vmz vibmt tjp gjnz ndsot nrxjiyn ja cvkkdiznn
33. tn dmi fzcj kt pdht rmi bhvz mv ytnj, cmi'fw llhwyq zhvz qafv. mn dmi fzcj kt pdht rmi xrb'g ahvz mv ytnj, cmi'fw yrzzv yhvz irbian.
34. llhwyq jvqqqnfv kaht rmi urv ebtgzfnxpj shvyky. ndml etso izzvpmbri ipdw.
35. Sdosqk jwewetwj lzsl qgm sjw stkgdmlwdq mfaimw. Bmkl dacw wnwjqgfw wdkw.
36. Bg woytmgjz; grgtwovg gjmg em ijtginw fiqgv
37. qn dmi mwz rmi xuold jzllkwfzimdj fpon hnq lb'l s ffitlv, cmi qetw qfit lbpjz izzvpmbri ipdw'w kmwegwk.
38. Qt ndjghtau; tktgndct taht xh pagtpsn ipztc.
39. ypk hapvty srj mvsnvbx: xal yhvzvjw enq kbgmn flnjxllbr; ynq l'u zbh lmlv ebpin mal yhvzvjw.
40. Knf kyzexj riv zewzekv: kyv lezmviyv reu yldre jklgzuzkp; reu Z'd efk jliv rsflk kyv lezmviyv.
41. imi exbk umi'lv mv yzjz adlr lmi wcn'g yflw lsdpit qfgcumw vveltbr ga xnvnlwj zfxmxv kahn lmi uuveme.
42. At kmt pmlyxt kmlk hnz dbvm kn vtt by kmt dngue.
43. Xa pda ydwjca pdwp ukq seod pk oaa ej pda sknhz.
44. Di ocmzz rjmy D xvi nph pk zqzmtocdib D'qz gzvmizy vwjpo gdaz: do bjzn ji.
45. Fc vlr qbii qeb qorqe, vlr alk'q exsb ql objbjybo xkvqefkd
46. Ucs avcg ucs'xk mv hczk gfkv ucs wiv'l rihh iehkkj pkwisek xkihmlu me rmvihhu pklkx lfiv ucsx dxkioe.
47. Weet vhyudti, weet reeai, qdt q ibuufo sedisyudsu: jxyi yi jxu ytuqb byvu.
48. dh ztdz ma lal vrrvwl mapvt ov gal akfco. pagl itsdap ibfal, maht ba slw.
49. Bylu qi yv oek muhu je tyu jecehem. Buqhd qi yv oek muhu je bylu vehuluh
50. Sd sc loddob dy lo rkdon pyb grkd iye kbo drkx dy lo vyfon pyb grkd iye kbo xyd.
51. Lg danw ak lzw jsjwkl lzafy af lzw ogjdv. Egkl hwghdw wpakl, lzsl ak sdd.
52. sb wrsw fbh wr hh rzapw zb quveme snq itfxkx mh ztdz
53. Cn cm hypyl nii funy ni vy qbun sio gcabn bupy vyyh
54. Daxw ak ozsl zshhwfk lg mk ozadw ow sjw escafy glzwj hdsfk
55. en dmi ddxjk ttsdap, cmi bhvz rb hbuq xh zzjz xalq
56. Ax qgm bmvwy hwghdw, qgm zsnw fg laew lg dgnw lzwe
57. Yv oek edbo huqt jxu reeai jxqj uluhoedu ubiu yi huqtydw, oek sqd edbo jxyda mxqj uluhoedu ubiu yi jxydaydw.
58. Lt sdc'i htt iwxcvh ph iwtb pgt, Lt htt iwtb ph Lt pgt
59. jgaqxubqw lal ukywlbwbf srj gqabatckctxh dnq wal enfoavj srj waubap
60. btnj maf'g tbpin ynvqlvt emiljwpq. qtnj ma sbpin vtvetbvt emiljwpq
61. on dmi nxpw eal xklna, fmi xrb'g ahvz xh fvqqqnfv rnlrapvt
62. imi exbk umi'lv mv yzjz adlr lmi wcn'g yflw lsdpit qfgcumw vveltbr ga xnvnlwj zfxmxv kahn lmi uuveme.
63. Wtqp tdy'e lmzfe qtyoty jzfcdpwq. Wtqp td lmzfe ncpletyr jzfcdpwq

-
64. Fbzrgvzrf gur dhrfgvbaf ner pbzcyvpngrq naq gur nafjref ner fvzcyr
65. lhgved ozjz izzvpudlvv cmi au. zpx gb cbr izzv tqaq xh mmi qebavin epevdt
nhpexmv.
66. btdz es an dmi qavv xh rlm xhaafik. hpere ns an dmi qavv xh ztdz jtfvzzv
67. Uron rbw'c jkxdc orwmrwp hxdabnuo. Uron rb jkxdc lanjcrwp hxdabnuo

Code Breaker's Journal:

Ciphertext:

imi exbk umi'lv mv yzjz adlr lmi wcn'g yflw lsdpit qfgcumw vveltbr ga xvnlnwj zfxmxv
kahn lmi uuveme.

General Observations:

Through observation, I understand that it is not a monoalphabetic Substitution assumed it is a polyalphabetic substitution, and worked on the cipher text.

Plan of Attack:

Vignertext: ^{9 12 8 4 23 1 10 20 12 8 11 21 12 21 24 25 12 5 0 8 11 17 11 12 8 22 2 13 6 24 5 11 22 11 18 3 15 8 19 16 5 22 20 12 22}
imi exbk umi'lv mv yzjz adlr lmi wcn'g yflw lsdpit qfgcumw

key: ^{10 24 16 20 10 13 14 22 24 14 20 17 4 8 13 11 14 21 4 22 7 4 13 24 14 20 20 13 19 5 0 11 0 18 11 4 4 15 1 4 20 20 18 4}
kjouknöwyo'ur ei nlov ewhe nyo ucan't far iaslee pbezaus

plain text: you know you're in love when you can't fall asleep because

Vignertext: ^{21 21 4 11 17 17 6 0 23 13 21 13 11 22 7 25 5 23 12 23 21 10 7 13 11 18 11 10 20 21 4 12 4}
vvelthbr ga xvnlnwj zfxmxv kahn lmi uuveme

key: ^{17 4 0 11 8 19 24 8 18 5 8 13 0 11 24 1 4 14 14 19 17 0 13 24 14 20 13 3 17 4 0 12 18}
e'reality is finally better than your dreams.

plain text: reality is finally better than your dreams.

$$p_i = (c_i - k_i) \bmod 26$$
 Eg:- $p^{(8)} - k^{(10)} = -8 \bmod 26 = 24 \rightarrow y$

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Shot on Y91
Vivo AI camera

<Trials 1>

Autokey cipher starts with a relatively-short keyword, the primer, and appends the message to it. So that I tried to brute force method to find out the initial key by applying different random alphabets as keys and most of them didn't turn out as meaningful plain text.

<Trials 2>

After several attempts to find the initial key, I finally tried the alphabet 'K' and it worked. I identified it as the enciphered with 'Autokey Cipher'.

Results:

Plaintext obtained- you know you're in love when you can't fall asleep because reality is finally better than your dreams.

The key obtained is K -10
