CSE 462

Introduction To Computer Security and Forensics Lab

Assignment 01

Objective:

The goal of this assignment is to apply the knowledge of several transposition ciphers and have hands-on experiences on them.

Task - 01:

a) Implement the Decryption part of Caesar Cipher which will take a key and a ciphertext as inputs and give a plaintext as output.

b) Use the above code to crack the following Caesar ciphertext, to identify the text encrypted:

XNZ XVMIDQVG VO DDXO WPDGYDIB NPNO DN BJDIB OJ WZ BMZVO VBVDI.

Also describe in detail (with code) how you have identified the plaintext.

c) Use the above code to decode these messages, which were encoded using the same Caesar cipher (among these 03 cipher blocks) and fill up the boxes.

Z	K	D	W		G	R		B	R	X		J	H	W		Z	K	H	Q		B	R	X

F	U	R	V	V		D		V	Q	R	Z	P	D	Q		Z	L	W	K		D

							?										
Y	D	P	S	L	U	H	?		I	U	R	V	W	E	L	W	H

Also describe in detail (with code) how you have identified the plaintext.

Task - 02:

The following ciphers have been created using a substitution cipher. While decrypting them, describe in detail (step by step) how you have identified the plaintext.

You may add necessary programs like frequency analysis, checking by trial-and-error etc. you have used while deciphering them.

For your convenience, a frequency distribution of English characters and list of hints are given.

a. gtd bsvgl vf fgedsugt dffml dkcymvsf gtmg gtd chjde ha aevdsxftvc tdycf bf gh id fgehsu aehz tmexftvcf. aevdsxf qms uvod bf gtd fgedsugt jd sddx jtds yvad udgf ghbut. vs mxxvgvhs, cdhcyd dkcedff bsvgl gtehbut yhod,amzvyl, aevdsxf, msx hgtdef ftmed fghevdf ha avsxvsu qhzzhs uehbsx jvgt fhzdhsd.gtded med zmsl idsdavgf ha fgmlvsu bsvgdx vs ghbut gvzdf, mf vg tdycf gh amqd qtmyydsuvsu fvgbmgvhsf jvgt qhbemud. gtd vzchegmsqd ha fgmlvsu bsvgdx tmf fgebqp m qthex mzhsu zmsl cdhcyd gtehbuthbg tvfghel.pddcvsu zdzhevdf ha jtmg jd tmod mqqhzcyvftdx gtehbuthbg tvfghel qms tdyc bf fdd thj vsxvovxbmyf msx qhzzbsvgvdf tmod cdefdodedx gtehbut ghbut gvzdf msx vsgh m ievutgde abgbed.

b. exupziu kxwqxagxom, upm gxsm zs l amtwzo exgg rmqzfm kigg lok xolquxjm.lgwz, l kxwqxagxomk amtwzo qlo qzoutzg lok plokgm upm wxuiluxzo zs gxjxoh xo l wzapxwuxqlumk elc uplo upzwm epz kz ozu.fztmzjmt, xs czi pljm l aglo lok czi elou
uz xfagmfmou xu xo czit gxsm upmo czi ommk kxwqxagxom.
xu flnmw upxohw mlwc szt czi uz plokgm lok iguxflumgc
rtxoh wiqqmww uz czit gxsm.xs ulgn lrziu upm ucamw zs kxwqxagxom, upmo upmc ltm hmomtlggc zs uez ucamw. sxtwu zom xw xokiqmk kxwqxagxom lok upm wmqzok zom xw wmgs-kxwqxagxom.xokiqmk kxwqxagxom
xw wzfmupxoh uplu zupmtw ulihpu iw zt em gmlto rc wmmxoh zupmtw. epxgm wmgs-kxwqxagxom qzfmw stzf exupxo lok em gmlto xu zo zit zeo wmgs. wmgs-kxwqxagxom tmyixtmw l gzu zs fzuxjluxzo lok wiaaztu stzf zupmtw.lrzjm lgg, szggzexoh czit klxgc wqpmkigm exupziu loc fxwulnm xw lgwz altu zs rmxoh kxwqxagxomk.

c. AUHC MVKFC V BYZUGC V IZMC CJ GUMBZYAZD UKUVM.
VC HZZGZB CJ GZ, V HCJJB PD CFZ VYJM KUCZ AZUBVMK CJ CFZ BYVWZ UMB OJY U IFVAZ, V TJNAB MJC ZMCZY.
OJY CFZ IUD, VC IUH PUYYZB CJ GZ.

d. JGRMQOYGHMVBJ WRWQFPW HGF FDQGFPFZR KBEEBJIZQ QO CIBZK. LFAFGQVFZFWW, EOG WOPF GFHWOL PHLR LOLFDMFGQW BLWBWQ OL KFWBYLBLY LFS FLJGRMQBOL WJVFPFW QVHQ WFFP QO QVFP QO CF POGF WFJIGF QVHL HLR OQVFG WJVFPF OL FHGQV. QVF ILEOGQILHQF QGIQV VOSFAFG BW QVHQ WIJV WJVFPFW HGF IWIHZZR QGBABHZ QO CGFHX.

Letter	Frequency	Letter	Frequency
e	12.7020%	m	2.4060%
t	9.0560%	w	2.3600%
a	8.1670%	f	2.2280%
o	7.5070%	g	2.0150%
i	6.9660%	y	1.9740%
n	6.7490%	p	1.9290%
s	6.3270%	b	1.4920%
h	6.0940%	v	0.9780%
r	5.9870%	k	0.7720%
d	4.2530%	j	0.1530%
l	4.0250%	x	0.1500%
c	2.7820%	q	0.0950%
u	2.7580%	z	0.0740%

Order Of Frequency Of Single Letters	E T A O I N S H R D L U
Order Of Frequency Of Digraphs	th er on an re he in ed nd ha at en es of or nt ea ti to it st io le is ou ar as de rt ve
Order Of Frequency Of Trigraphs	the and tha ent ion tio for nde has nce edt tis oft sth men
Order Of Frequency Of Most Common Doubles	ss ee tt ff ll mm oo
Order Of Frequency Of Initial Letters	T O A W B C D S F M R H I Y E G L N P U J K
Order Of Frequency Of Final Letters	E S T D N R Y F L O G H A K M P U W
One-Letter Words	a, I.
Most Frequent Two-Letter Words	of, to, in, it, is, be, as, at, so, we, he, by, or, on, do, if, me, my, up, an, go, no, us, am
Most Frequent Three-Letter Words	the, and, for, are, but, not, you, all, any, can, had, her, was, one, our, out, day, get, has, him, his, how, man, new, now, old, see, two, way, who, boy, did, its, let, put, say, she, too, use
Most Frequent Four-Letter Words	that, with, have, this, will, your, from, they, know, want, been, good, much, some, time

Task - 03:

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: SUSTCSE

Sample Input/Output:

CSE FINAL YEAR THEORY COURSE INTRODUCTION TO COMPUER SECURITY AND FORENSICS

Sample Output/Input:

UMW YKFED SWTT LLWIJR EGYJMW BPLVGXMVVASF NG VQETMYJ LGUYJCLR CFH XIJXPKMUM

Task - 04:

Write a program to simulate the Hill Cipher crypto system having the following properties and inputs. The program should have encryption facilities (decryption facilities: optional. You can get bonus if you do so) with the provision to ask the user the operation the user would like to perform.

Key:

AWESOME INTRODUCTION TO COMPUTER SECURITY AND FORENSICS

Sample Input/Output: SUST CSE

Sample Output/Input: WJCT KZU

Submission Guidelines:

- You need to submit corresponding source files (py, c, cpp, java etc as there is no restriction over choosing a programming language) and ***a report*** mentioning the approaches taken for problems you have solved.
- Explain as much as you can. The more convincing your report is, the more marks you can get.
- Report can contain codes you have written.
- A sample report format only for Task 02 is added with the credit of *2019331053 (M. M. Kabid Hasan)*. Obviously, you can use your own format for explaining.
- You can use library for some data manipulations. But not the whole algorithm itself.
- You can easily find the implementation of cipher algorithms on the Internet. **Do not copy from any web source or friend or seniors. The persons involved in such activities will be penalized by -100% of the total marks and will be marked **RED* for future assignments.**

Mark Distribution:

Task	Marks	Total
1	05+ 06 + 09	20
2	07 + 07 + 08 + 08	30
3	10	10
4	10 + (05 as bonus)	10

Deadline:

09th of February 2024. Friday 11.59 pm. (HARD & STRICT).