COMP3355 Cyber Security

Assignment 1

(Due on 23 Sep 2019, 23:59)

Q1. (15%) A sentence is encrypted using substitution cipher. Following is the encrypted sentence (spaces between words are suppressed):

```
ftqdq uezae gotft uzsme msdqm ffmxq zfiuf tagfs dqmfi uxxba iqd
```

Analyze the encryption to answer the following questions:

(a) What is the substitution being used in the above cipher?

(b) Recover the cipher text into plain text.

Q2. (15%) Suppose that the cipher text "ssthiihttrefissaensigmtncuoforbyueerscirrotycues" is encrypted using transposition cipher. The encryption key (permutation) is $\pi = (6\ 4\ 1\ 2\ 3\ 5\ 8\ 7)$.

(a) What is the inverse permutation (decryption key)?

(b) Decrypt the cipher text into plain text.

Q3. (40%) Referring to the lecture notes on DES, there are one Expansion Permutation (Table1), eight Substitution S-Boxes and one Permutation P-Box (Table 2) in the function $f(K_i, R_i)$ for round i in DES encryption. Given that the input plain text is `A7E2BC3FD4C896D2` and the encryption key is `1A5D6D895B4B66DB` in hexadecimal representation. Implement round 1 encryption manually and list L_1 and R_1. The initial permutation for input is shown in table 3.

Table 1: Expansion Permutation

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	01

Table 2: Permutation P-Box

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Table 3: Input Permutation

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Q4. (30%) An English prose quotation is encrypted with an unknown method. Below is the encrypted quotation (where spaces between words are suppressed).

```
fjwvs yfvbl hfwdu skevm wiodm bmiff wmhhu vzsxj iqjvs zfvhv
bvvjp hepqe dfrjs swtif zolmp hzzhz xiyxe wliem wrhww ubufi
ylubh rbryt jdths revbr rwwjl hkcvi wyofd jimuw zcfwi csjka
xiuvz osren kvdsg jzltd svucf lzsvm swyfg yhbdj ssrbh gkvwt
bwlww umtfd erkjp lxdhz vfybv ojwba rrikx suozo kidou vrsrj
hdlum vbfvv oleun kvssw uuvzo kyngl ktgpm izzby mumdt qwwtc
rehgx iywis sxzii raaxz uquqg sqyur hasou xjhje mcdzg sqfge
vfgju bhtce qphzv odxii ieolm phvzb oljwk kvwgp gpfbo ibfwy
vweem rwugz flqds fxnyh kwfkt jufja hfnkv asmoz riiej plffc
hisuw zcfev mwiod mbbdj sfisa hkwue mfbgi jwvyg kvwgb ovvcx
monhi bsxji qrzlv bxhcw tisuo zgsxj iqrik xsuoz odien kvtgv
nuwzc fsgnk vqsms hvxfg yququ okmbj dtwxm dyffb gqjwf fchis
uwzcf mucvr awqcy uftll fiuxo fmtuw zcfjp lhtcf sncft cgtfl
dkwgr bhgus nimis dsfxb hgkvw aplou hjeey riusr jtdkw grubh
issvf mhmsj emgda cjfjf dksje mzuvs lvbxh rujif ghehk evmwi
odmbb djdmv tohua gwulh tsfxm swyss ytnur zaevh lksvw uuwvg
xvfyw iovib auvse ionde ruppm hisus oipzq jimuw zcfwx cwybw
aaydc ofhbz rlbvm oapva tiswr lblvz iikvw yocwv rfeuc regsy
tnurz aebfv fasmo ndzbk eocqk sjrbn lfbsp bcggf gksup lbvis
qkzqz wpghj wpxzw rlblv jyvis uijph rgkmt ndeqw xiyel ryiuj
ufjah fmrms jxxid erslb fiswd pjiqw cjhfp hcchq fhwrg kmtnd
eqwet usvfu iondx sgjhx skvaw diqkf afvnl fbawm yvjhz eonkr
hgjub hlbem mfheb aynxh msdsq ghehy sbfv
```

Analyze the encryption to answer the following questions:

(a) What type of cipher is it? (Monoalphabetic / Polyalphabetic)

(b) Give the permutation(s) (if any) or the substitution(s) used in the cipher.

(c) Recover the cipher text into plain text.

In your answers, you should show the detailed steps of your solution instead of listing the plain text only.