Tutorial #1
Security in Computing COSC2356/2357

Q1 (a) Find the plaintext and the key from the ciphertext **ZLJBYPAF** given that the cipher is a simple substitution of the shift-by-*n* variety.

(b) [**Do It Yourself**] Find the plaintext and the key from the ciphertext **GSQIFEGO** given that the cipher is a simple substitution of the shift-by-*n* variety.

Q2: Suppose that we have a computer that can test 2^{41} keys each second.

a. What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2^{88}?
b. [**Do It Yourself**] What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2^{112}?
c. [**Do It Yourself**] What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2^{256}?

Q3: [**Do It Yourself**] Encrypt the message, "**WE ARE ALL TOGETHER**", using ***double transposition cipher*** with 4 rows and 4 columns, using the following permutations:
Row permutation: (2, 4, 1, 3) → (1, 2, 3, 4)
Column permutation: (3, 1, 2, 4) → (1, 2, 3, 4)

Q4. Decrypt the following ciphertext using the ***double transposition cipher*** using a matrix of **3 rows** and **4 columns**.

UROXTLAEELVF

Hint: The first two letters in the plaintext are "A" and "T".

Q5. Assume that the following ciphertext has been produced using a simple substitution cipher:

GFS WMY OG LGDVS MF SFNKYHOSU ESLLMRS, PC WS BFGW POL DMFRQMRS, PL OG CPFU M UPCCSKSFO HDMPFOSXO GC OIS LMES DMFRQMRS DGFR SFGQRI OG CPDD GFS LISSO GK LG, MFU OISF WS NGQFO OIS GNNQKKSFNSL GC SMNI DSOOSK. WS NMDD OIS EGLO CKSJQSFODY GNNQKKPFR DSOOSK OIS 'CPKLO', OIS FSXO EGLO GNNQKKPFR DSOOSK OIS 'LSNGFU' OIS CGDDGWPFR EGLO GNNQKKPFR DSOOSK OIS 'OIPKU', MFU LG GF, QFOPD WS MNNGQFO CGK MDD OIS UPCCSKSFO DSOOSKL PF OIS HDMPFOSXO LMEHDS. OISF WS DGGB MO OIS NPHISK OSXO WS WMFO OG LGDVS MFU WS MDLG NDMLLPCY POL LYEAGDL. WS CPFU OIS EGLO GNNQKKPFR LYEAGD MFU NIMFRS PO OG OIS CGKE GC OIS 'CPKLO' DSOOSK GC OIS HDMPFOSXO LMEHDS, OIS FSXO EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'LSNGFU' DSOOSK, MFU OIS CGDDGWPFR EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'OIPKU' DSOOSK, MFU LG GF, QFOPD WS MNNGQFO CGK MDD LYEAGDL GC OIS NKYHOGRKME WS WMFO OG LGDVS.

Find the plaintext by **frequency analysis technique.** Use the following frequency table of English letters:

E	**T**	**A**	**O**	**I**	**N**	**S**	**H**	**R**	**D**	**L**	**U**	**C**
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3	4.0	2.8	2.8
M	**W**	**F**	**Y**	**G**	**P**	**B**	**V**	**K**	**X**	**J**	**Q**	**Z**
2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.2	0.2	0.1	0.1

Q6. From a bank's perspective, which is usually more important, the integrity of its customer's data or the confidentiality of the data? From the perspective of the bank's customers, which is more important?