Tutorial #1 Solution
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.

Ans:
Using backward shift, try all possible shift from 1 to 25 unless a meaningful word is found.

n = 1, YKIAXOZE
n = 2, XJHZWNYD
n = 3, WIGYVMXC
n = 4, VHFXULWB
n = 5, UGEWTKVA
n = 6, TFDVSJUZ
n = 7, SECURITY

Therefore, the plaintext = **SECURITY** and key n = **7**.

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

Ans:
Using backward shift, try all possible shift from 1 to 25 unless a meaningful word is found.

n = 1, FRPHEDFN	*n* = 15, RDBTQPRZ
n = 2, EQOGDCEM	*n* = 16, QCASPOQY
n = 3, DPNFCBDL	*n* = 17, PBZRONPX
***n* = 4, COMEBACK (found meaningful)**	*n* = 18, OAYQNMOW
n = 5, BNLDAZBJ	*n* = 19, NZXPMLNV
n = 6, AMKCZYAI	*n* = 20, MYWOLKMU
n = 7, ZLJBYXZH	*n* = 21, LXVNKJLT
n = 8, YKIAXWYG	*n* = 22, KWUMJIKS
n = 9, XJHZWVXF	*n* = 23, JVTLIHJR
n = 10, WIGYVUWE	*n* = 24, IUSKHGIQ
n = 11, VHFXUTVD	*n* = 25, HTRJGFHP
n = 12, UGEWTSUC	
n = 13, TFDVSRTB	
n = 14, SECURQSA	

Therefore, the plaintext = **COMEBACK** and key n = **4**.

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. What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2^{112}?
c. What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2^{256}?

Ans:

a. The required time = $\frac{2^{88}}{2^{41}}\ seconds = 2^{47} seconds = \frac{2^{47}}{60\times60\times24\times365}\ years = 4.462 \times 10^{6}\ years$
b. The required time = $2^{71}\ seconds \approx 7.487 \times 10^{13}\ years$
c. The required time = $2^{215}\ seconds \approx 1.67 \times 10^{57}\ years$

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

Ans:
We have to perform a double transposition cipher with 4 rows and 4 columns matrix. The rules of permutations are given as follows:
Row permutation: (1, 2, 3, 4) → (2, 4, 1, 3)
Column permutation: (1, 2, 3, 4) → (3, 1, 2, 4)

Step-1: Convert the given plaintext into a 4 X 4 matrix.

	1	2	3	4
1	W	E	A	R
2	E	A	L	L
3	T	O	G	E
4	T	H	E	R

Step-2: Perform row permutations.

	1	2	3	4
2	E	A	L	L
4	T	H	E	R
1	W	E	A	R
3	T	O	G	E

Step-3: Perform column Permutations.

	3	1	2	4
2	L	E	A	L
4	E	T	H	R
1	A	W	E	R
3	G	T	O	E

The ciphertext is: **LEALETHRAWERGTOE**

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".***

Ans:

According to the question, we have only two information for decryption. First, the matrix dimension is **3 X 4** (i.e. **3 rows** and **4 columns**). Second, the first two letters in the plaintext are "**A**" and "**T**". Row and column permutations are not given. Therefore, we will have to find the *plaintext* by **cryptanalysis technique** using given information.

Step-1: Represent the given ciphertext by a **3 X 4** matrix:

	1	2	3	4
1	U	R	O	X
2	T	L	A	E
3	E	L	V	F

Step-2: In order to bring 'A' in column position '1', swap Column-3 and Column-1 of the previous step:

	3	2	1	4
1	O	R	U	X
2	A	L	T	E
3	V	L	E	F

Step-3: In order to bring ‘T’ in column position ‘2’, swap Column-1 and Column-2 of the previous step:

	3	1	2	4
1	O	U	R	X
2	A	T	L	E
3	V	E	L	F

Step-4: Swap *Row-2* and *Row-1* of the previous step to make ‘A’ and ‘T’ as the first and second letters, respectively:

	3	1	2	4
2	A	T	L	E
1	O	U	R	X
3	V	E	L	F

Step-5: Check, which rows and columns should be swapped to get some meaningful words from the beginning of the matrix. From the previous step, the letter ‘X’ does not make any meaningful word. Hence, it might have been used as a letter to fill up the empty space during encryption process. The location of letter ‘X’ might be in the 4^{th} column of 3^{rd} row.

Therefore, swap *Row-3* and *Row-1* of the previous step at to keep ‘X’ in the 4^{th} column of 3^{rd} row:

	3	1	2	4
2	A	T	L	E
3	V	E	L	F
1	O	U	R	X

Step-6: We get three meaningful words, AT, LEVEL and FOUR, with an ‘X’ at the end. The ‘X’ can be considered as filler during encryption process and can be removed.

Therefore, the plaintext becomes: **AT LEVEL FOUR**

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

Ans:

The first step is to find the frequency of all the letters appearing in the intercept. Use any online tool to find the frequency of letters. We are using the following:
https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html

For this intercept we get the values given in the table below.

Ciphertext Letter	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
Frequency	5	2	26	42	23	51	67	8	33	1	35	39	35	29	85	30	14	17	88	0	17	3	16	6	10	0

The above frequencies ordered from most common to least to make comparisons easier.

Ciphertext Letter	S	O	G	F	D	L	K	M	I	P	N	C	E	R	U	W	Q	Y	H	X	A	V	B	J	T	Z
Frequency	88	85	67	51	42	39	35	35	33	30	29	26	23	17	17	16	14	10	8	6	5	3	2	1	0	0

Now that we have all the frequencies of ciphertext letters, we can start to make some substitutions. Substitutions can be done using the following online tool (same as above):
https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html

We see that the most common ciphertext letter is "S", closely followed by "O". From the chart and table above, we can guess that these two letters represent "e" and "t" respectively, and after making these substitutions we get:

GFe WMY tG LGDVe MF eFNKYHteU EeLLMRe, PC We BFGW PtL DMFRQMRe, PL tG CPFU M UPCCeKeFt HDMPFteXt GC tIe LMEe DMFRQMRe DGFR eFGQRI tG CPDD GFe LIeet GK LG, MFU tIeF We NGQFt tIe GNNQKKeFNeL GC eMNI DetteK. We NMDD tIe EGLt CKeJQeFtDY GNNQKKPFR DetteK tIe 'CPKLt', tIe FeXt EGLt GNNQKKPFR DetteK tIe 'LeNGFU' tIe CGDDGWPFR EGLt GNNQKKPFR DetteK tIe 'tIPKU', MFU LG GF, QFtPD We MNNGQFt CGK MDD tIe UPCCeKeFt DetteKL PF tIe HDMPFteXt LMEHDe. tIeF We DGGB Mt tIe NPHIeK teXt We WMFt tG LGDVe MFU We MDLG NDMLLPCY PtL LYEAGDL. We CPFU tIe EGLt GNNQKKPFR LYEAGD MFU NIMFRe Pt tG tIe CGKE GC tIe 'CPKLt' DetteK GC tIe HDMPFteXt LMEHDe, tIe FeXt EGLt NGEEGF LYEAGD PL NIMFReU tG tIe CGKE GC tIe 'LeNGFU' DetteK, MFU tIe CGDDGWPFR EGLt NGEEGF LYEAGD PL NIMFReU tG tIe CGKE GC tIe 'tIPKU' DetteK, MFU LG GF, QFtPD We MNNGQFt CGK MDD LYEAGDL GC tIe NKYHtGRKME We WMFt tG LGDVe.

We now notice that the word "tIe" is appearing frequently in the passage. In English, the most common 3 letter word is "the" and this fits with what we have already done, which suggests that "I" should be decrypted to "h".
Also, by looking at the frequencies again, we see the next most common letter is "G", which is probably one of "a", "i" or "o". We see that the third word is "tG", and the only one of these options that makes sense is "to", so we guess "G" is "o".

oFe WMY to LoDVe MF eFNKYHteU EeLLMRe, PC We BFoW PtL DMFRQMRe, PL to CPFU M UPCCeKeFt HDMPFteXt oC the LMEe DMFRQMRe DoFR eFoQRh to CPDD oFe Lheet oK Lo, MFU theF We NoQFt the oNNQKKeFNeL oC eMNh DetteK. We NMDD the EoLt CKeJQeFtDY oNNQKKPFR DetteK the 'CPKLt', the FeXt EoLt oNNQKKPFR DetteK the 'LeNoFU' the CoDDoWPFR EoLt oNNQKKPFR DetteK the 'thPKU', MFU Lo oF, QFtPD We MNNoQFt CoK MDD the UPCCeKeFt DetteKL PF the HDMPFteXt LMEHDe. theF We DooB Mt the NPHheK teXt We WMFt to LoDVe MFU We MDLo NDMLLPCY PtL LYEAoDL. We CPFU the EoLt oNNQKKPFR LYEAoD MFU NhMFRe Pt to the CoKE oC the 'CPKLt' DetteK oC the HDMPFteXt LMEHDe, the FeXt EoLt NoEEoF LYEAoD PL NhMFReU to the CoKE oC the 'LeNoFU' DetteK, MFU the CoDDoWPFR EoLt NoEEoF LYEAoD PL NhMFReU to the CoKE oC the 'thPKU' DetteK, MFU Lo oF, QFtPD We MNNoQFt CoK MDD LYEAoDL oC the NKYHtoRKME We WMFt to LoDVe.

The first word is now "oFe", which when considered with the appearance of "theF", leads us to the conclusion that "F" is "n". This also fits in with the frequencies of both letters in the tables.

In the third line we see the word "Lheet", which is most likely to be "sheet", and so we replace "L" with "s". Again, the frequencies of these two letters are about right.

one WMY to soDVe Mn enNKYHteU EessMRe, PC We BnoW Pts DMnRQMRe, Ps to CPnU M UPCCeKent HDMPnteXt oC the sMEe DMnRQMRe DonR enoQRh to CPDD one sheet oK so, MnU then We NoQnt the oNNQKKenNes oC eMNh DetteK. We NMDD the Eost CKeJQentDY oNNQKKPnR DetteK the 'CPKst', the neXt Eost oNNQKKPnR DetteK the 'seNonU' th CoDDoWPnR Eost oNNQKKPnR DetteK the 'thPKU', MnU so on, QntPD We MNNoQnt CoK MDD the UPCCeKent DetteKs Pn the HDMPnteXt sMEHDe. then We DooB Mt the NPHheK text We WMnt to soDVe MnU We MDso NDMssPCY Pts sYEAoDs. We CPnU the Eost oNNQKKPnR sYEAoD MnU NhMnRe Pt to the CoKE oC the 'CPKst' DetteK oC the HDMPnteXt sMEHDe, the neXt Eost NoEEon sYEAoD Ps NhMnReU to the CoKE oC the

'seNonU' DetteK, MnU the CoDDoWPnR Eost NoEEon sYEAoD Ps NhMnReU to the CoKE oC the 'thPKU' DetteK, MnU so on, QntPD We MNNoQnt CoK MDD sYEAoDs oC the NKYHtoRKME We WMnt to soDVe.

We see the world "soDVe", which could be "solve", implying the transformations of "D" and "V" to "l" and "v" respectively.
In the second line we now have the phrase "one sheet oK so", which suggests that "K" is "r".

one WMY to solve Mn enNrYHteU EessMRe, PC We BnoW Pts lMnRQMRe, Ps to CPnU M UPCCerent HlMPnteXt oC the sMEe lMnRQMRe lonR enoQRh to CPll one sheet or so, MnU then We NoQnt the oNNQrrenNes oC eMNh letter. We NMll the Eost CreJQentlY oNNQrrPnR letter the 'CPrst', the neXt Eost oNNQrrPnR letter the 'seNonU' the ColloWPnR Eost oNNQrrPnR letter the 'thPrU', MnU so on, QntPl We MNNoQnt Cor Mll the UPCCerent letters Pn the HlMPnteXt sMEHle. then We looB Mt the NPHher teXt We WMnt to solve MnU We Mlso NlMssPCY Pts sYEAols. We CPnU the Eost oNNQrrPnR sYEAol MnU NhMnRe Pt to the CorE oC the 'CPrst' letter oC the HlMPnteXt sMEHle, the neXt Eost NoEEon sYEAol Ps NhMnReU to the CorE oC the 'seNonU' letter, MnU the ColloWPnR Eost NoEEon sYEAol Ps NhMnReU to the CorE oC the 'thPrU' letter, MnU so on, QntPl We MNNoQnt Cor Mll sYEAols oC the NrYHtoRrME We WMnt to solve.

In the middle of the second line we have the word "enoQRh", which is likely to be "enough", and so we have the transformations "Q" and "R" to "u" and "g" respectively.

one WMY to solve Mn enNrYHteU EessMge, PC We BnoW Pts lMnguMge, Ps to CPnU M UPCCerent HlMPnteXt oC the sMEe lMnguMge long enough to CPll one sheet or so, MnU then We Nount the oNNurrenNes oC eMNh letter. We NMll the Eost CreJuentlY oNNurrPng letter the 'CPrst', the neXt Eost oNNurrPng letter the 'seNonU' the ColloWPng Eost oNNurrPng letter the 'thPrU', MnU so on, untPl We MNNount Cor Mll the UPCCerent letters Pn the HlMPnteXt sMEHle. then We looB Mt the NPHher teXt We WMnt to solve MnU We Mlso NlMssPCY Pts sYEAols. We CPnU the Eost oNNurrPng sYEAol MnU NhMnge Pt to the CorE oC the 'CPrst' letter oC the HlMPnteXt sMEHle, the neXt Eost NoEEon sYEAol Ps NhMngeU to the CorE oC the 'seNonU' letter, MnU the ColloWPng Eost NoEEon sYEAol Ps NhMngeU to the CorE oC the 'thPrU' letter, MnU so on, untPl We MNNount Cor Mll sYEAols oC the NrYHtogrME We WMnt to solve.

We have the word "Nount" which is could be "count" and "EessMge" which is likely to be "message", giving us that "N", "E" and "M" and "c", "m" and "a".

one WaY to solve an encrYHteU message, PC We BnoW Pts language, Ps to CPnU a UPCCerent HlaPnteXt oC the same language long enough to CPll one sheet or so, anU then We count the occurrences oC each letter. We call the most CreJuentlY occurrPng letter the 'CPrst', the neXt most occurrPng letter the 'seconU' the ColloWPng most occurrPng letter the 'thPrU', anU so on, untPl We account Cor all the UPCCerent letters Pn the HlaPnteXt samHle. then We looB at the cPHher teXt We Want to solve anU We also classPCY Pts sYmAols. We CPnU the most occurrPng sYmAol anU change Pt to the Corm oC the 'CPrst' letter oC the HlaPnteXt samHle, the neXt most common sYmAol Ps changeU to the Corm oC the 'seconU' letter, anU the ColloWPng most common sYmAol Ps changeU to the Corm oC the 'thPrU' letter, anU so on, untPl We account Cor all sYmAols oC the crYHtogram We Want to solve.

It is likely that "W"->"w", "X"->"x", "Y"->"y" and "Z"->"z".

The word "occurrPng" is clearly meant to read "occurring", and it is likely that "sYmAol" is "symbol".

one way to solve an encryHteU message, iC we Bnow its language, is to CinU a UiCCerent Hlaintext oC the same language long enough to Cill one sheet or so, anU then we count the occurrences oC each letter. we call the most CreJuently occurring letter the 'Cirst', the next most occurring letter the 'seconU' the Collowing most occurring letter the 'thirU', anU so on, until we account Cor all the UiCCerent letters in the Hlaintext samHle. then we looB at the ciHher text we want to solve anU we also classiCy its symbols. we CinU the most occurring symbol anU change it to the Corm oC the 'Cirst' letter oC the Hlaintext samHle, the next most common symbol is changeU to the Corm oC the 'seconU' letter, anU the Collowing most common symbol is changeU to the Corm oC the 'thirU' letter, anU so on, until we account Cor all symbols oC the cryHtogram we want to solve.

We can now see that "C" is "f", "B" is "k", "U" is "d", "J" is "q" and "H" is "p".

one way to solve an encrypted message, if we know its language, is to find a different plaintext of the same language long enough to fill one sheet or so, and then we count the occurrences of each letter. we call the most frequently occurring letter the 'first', the next most occurring letter the 'second' the following most occurring letter the 'third', and so on, until we account for all the different letters in the plaintext sample. then we look at the cipher text we want to solve and we also classify its symbols. we find the most occurring symbol and change it to the form of the 'first' letter of the plaintext sample, the next most common symbol is changed to the form of the 'second' letter, and the following most common symbol is changed to the form of the 'third' letter, and so on, until we account for all symbols of the cryptogram we want to solve.

The final list of substitutions is given below:

S	O	G	F	D	L	K	M	I	P	N	C	E	R	U	W	Q	Y	H	X	A	V	B	J	T	Z
E	T	O	N	L	S	R	A	H	I	C	F	M	G	D	W	U	Y	P	X	B	V	K	Q	-	-

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?

Ans:
The bank's primary concern is with the integrity of transactions, while its customers probably have roughly equal concern with both.