Shahjalal University of Science and Technology
Institute of Information and Communication Technology
Software Engineering
Final Examination, 3rd Year 2nd Semester (Session: 2017-18)
Course Code: SWE 337 Credits: 2 Course Title: Computer, Data and Network Security
Total Marks: 30

Group A
[Answer all the questions]

1.		**2x2.5=5**
a)	Suppose we are using ASCII encoding. Now each English alphabet is estimated to carry 1.25 bits of information. Calculate the probability that a randomly selected sequence of 32 bits is a meaningful text message.	
b)	How can we detect whether CBC can hide patterns or not? Describe the process.	
2.		**2x5=10**
a)	Between CFB and OFB which one has a better encryption architecture? Why?	
b)	The English language has an information content of about 1.25 bits per character. Thus, when using the standard 8-bit ASCII encoding, about 6.75 bits per character are redundant. Compute the probability that a random array of t bytes corresponds to English text.	

Group B
[Answer all the questions]

3.		**2x2.5=5**
a)	With respect to the C.I.A. and A.A.A. concepts, what risks are posed by Trojan horses?	
b)	Describe a process through which a system can fulfill the Complete Mediation security principal.	
4.		**2x5=10**
a)	Encrypt the text “BBC ABC BCA A” using Block Cipher with padding where m = 3; $k = \begin{bmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \\ 9 & 10 & 11 \end{bmatrix}$; For the first block $\vec{x} = \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix}$ And for the last block $\vec{x} = \begin{bmatrix} 0 \\ 3 \\ 3 \end{bmatrix}$ Hints: The last block will become A22 after padding. And you may assume that there are at most 4 characters in the entire character set	
b)	What do you understand by Complete Mediation? Can you give example of a real life system that should incorporate this principle in their system?	