BITS PILANI – DUBAI
International Academic City, Dubai
First Semester 2011 – 2012
Information Theory and Coding ECE C393 (III year)
Comprehensive Exam (Closed Book)

Duration: 3 Hours **Weightage: 40%**
9 January 2012 **MAX: 40 Marks**

Note: Show all working to get full credit.

Question 1 (Total Marks: 5)
Consider a Binary Symmetric Channel (BSC) with **p(x,y)** given in the following table. X is the input to the BSC and Y the output.

Y	X	
	0	1
0	0	3/4
1	1/8	1/8

1) Calculate H(X).
2) Calculate H(X|Y).
3) Calculate I(X; Y).
4) Determine the smallest probability of error using Fano's indequality given below.

$$H(P_e) + P_e \log(|\mathcal{X}| - 1) \geq H(X \mid Y)$$

(0.5 + 1 + 0.5 + 3)

Question 2 (Total Marks: 6 Marks)
Obtain Shannon code for a system where 6 source symbols have to be encoded. These 6 symbols have the following probability of occurrence: {0.25, 0.2, 0.15, 0.1, 0.1, 0.2}. For this code book, answer the following questions:

1) Is the code book obtained unique? Justify your answer.
2) Are all codebooks obtained instantaneous? Justify your answer.
3) Can it be guaranteed that we always will have one instantaneous codebook? Justify your answer.

(3 + 1 + 1 + 1)

Question 3 (Total Marks: 5)
Let the message be D = 1010001101. Assume CRC-16 is used for which $P(x) = x^{16} + x^{15} + x^2 + 1$.

1) Obtain the FCS. Show all calculations.
2) We know that for P = 110101, FCS = 01110. When would you use CRC-16 and when would you use P = 110101? Justify your answer.

(4 + 1)

Question 4 (Total Marks: 4)
Using the following two prime numbers: 29 and 59, obtain the encrypted value of the message M = 7 (this could be the letter 'G') using RSA. Make appropriate assumptions but state your assumptions.

Question 5 (Total marks: 6)

Design an encryption system that meets the following specifications.

1) two levels of authentication.
2) two levels of confidentiality.
3) two levels of signature.

Draw a schematic of the system. Demonstrate and prove that your system meets the specification.

Question 6 (Total Marks: 8x0.5 = 4)

Write brief justification in answering whether following statements are true or false.

1) LZW is the best data compression technique for English Language.
2) In Arithmetic coding technique, decoding is accomplished with ease.
3) For low SNR, a high channel bit rate can be obtained.
4) DES is a stream cipher.
5) Hash function is the same as encryption.
6) Diffie-Hellman is an encryption algorithm.
7) When generating a (k,n) code using the following generator matrix, k = 2, n = 3.

$$G = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

8) The minimum distance of a code book that can detect and correct a maximum of 4 errors is at least 8.

Question 7 (Total Marks: 5x2 = 10)

The following information is given for a communication system.

1) Voice is source encoded ~~with 4 bits~~ using Huffman coding. The source values have the following probabilities: {A, B, C, D} = {0.25, 0.25, 0.375, 0.125}
2) The communication channel is bandlimited to 4 KHz. The SNR in the channel = 31.
3) Convolution encoding is used.

Answer the following questions:

1) Obtain the Huffman code for the specifications given.
2) Which of the following design values can meet the above specifications? Justify your answer.
    a. 2000 samples per second and (1,3) convolution coding.
    b. 8000 samples per second and (1, 2) convolution coding.
3) For the chosen (k,n) convolution coding (2a or 2b), which shift register size would given that there is a constraint in available memory: Shift register of length 2 or shift register of length 3?
4) Draw the convolution encoder with parameter values chosen in (2) and (3). Obtain the complete state transition diagram and corresponding outputs.
5) For the following analog value sequence: DABCCA, write the binary value sequence that is to be transmitted on the channel after source coding and channel coding.

BITS PILANI – DUBAI
International Academic City, Dubai
First Semester 2011 – 2012
Information Theory and Coding ECE C393 (III year)
Test 2 (Open Book)

Duration : 50 minutes **Weightage : 20%**
11 November 2011 **MAX : 20 Marks**

Note: Show all working to get full credit.

Question 1 (Total Marks: 5): Assume a source has four symbols (M = 4) (Symbols are A, B, C, D). The probabilities and distribution of the symbols are p = [0.25 0.375 0.25 0.125]. Assume that the sequence to be transmitted is **DBAC**.

1. Choose ***one*** of the following coding techniques: Shannon codes, SFE codes, Arithmetic codes. Justify your choice.
2. Encode the sequence to be transmitted with the technique you have chosen in part (1).

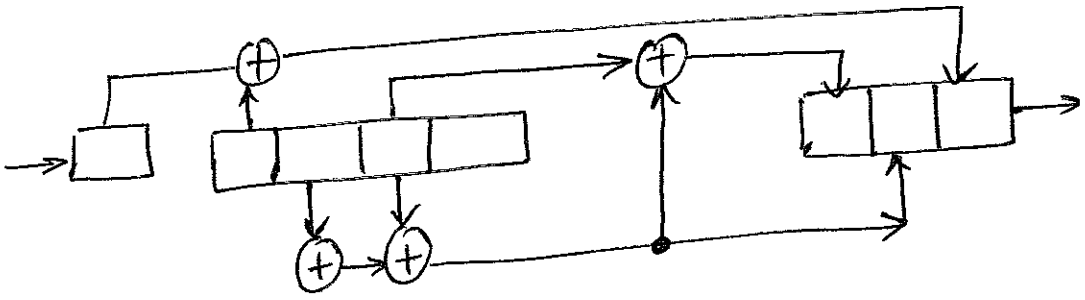
(1 + 4 Marks)

Question 2 (Total Marks: 5): The CRC algorithm specified in CCITT is uses the following Pattern Polynomial:

$P(x) = x^{16} + x^{12} + x^5 + 1$

What would be the transmitted data given that the message is given by 1010001101?

Question 3 (Total Marks: 5): For the convolution encoder shown below, create the table in the format shown. The table must be complete for **all** combinations of *current input* and *current state*.



Current Input	Current State	Next State	Output
0	0000		
1	0000		
0	0001		
1	0001		
0	0010		
1	0010		
0	0011		
1	0011		
0	0100		
1	0100		

Question 4 (Total Marks: 2): In the following expression for minimum information rate

$$R_g(D) = \begin{cases} \frac{1}{2}\log_2(\sigma_x^2 / D) & 0 \le D \le \sigma_x^2 \\ 0 & D > \sigma_x^2 \end{cases}$$

Answer the following questions:

1) What does a large and small value of (D/σ_x^2) mean practically?
2) What does a large or small value of $R_g(D)$ mean practically?

Question 5 (Total Marks: 3): State and show in **6 ways** how *diffusion* and *confusion* is used in DES to encrypt data.

BITS PILANI – DUBAI
International Academic City, Dubai
First Semester 2011 – 2012
Information Theory and Coding ECE C393 (III year)
Test 1 (Closed Book)

Duration : 50 minutes **Weightage : 25%**
16 October 2011 **MAX : 25 Marks**

Note: Show all working to get full credit.

Question 1 (Total Marks: 16): Let (X, Y) have the following joint distribution p(x, y):

	X = 0	**X = 1**
Y = 0	1/2	1/8
Y = 1	1/8	1/4

1. Compute H(X).
2. Compute H(X|Y).
3. Compute I(X; Y).
4. Compute I(X; X).
5. Draw a Venn Diagram to show the relationship between entropy and mutual information with numerical values wherever possible.
6. Obtain the Probability of Error (P_e) using Fano's Inequality. Can you obtain more than one value of Pe that satisfies Fano's Inequality? If yes, how would you choose between the values?
7. Now given that p(x, y) is estimated by q(x, y) given below. Obtain the Kullback Leibler distance D(p||q). Would you expect D(p||q) and D(q||p) to have the same value (without calculating D(q||p))?

	X = 0	**X = 1**
Y = 0	1/4	1/4
Y = 1	1/4	1/4

(2 + 2 + 2 + 1 + 1 + 2 + 4 + 2 Marks)

Question 2 (Total Marks: 9): Assume a source has four symbols (M = 4). The probabilities and distribution of the symbols are p = [0.25 0.375 0.25 0.125].

1. Determine the Huffman code for each of the four symbols.
2. Consider the following code books for the above probability distribution: Huffman code book (obtained in part (1)), {00, 01, 100, 110}, {10, 11, 101, 110} {0, 10, 110, 100}, {0, 1, 11, 1}. Which code book(s) would you select based on the following criterion? Justify your answers.
   a. Non-singular codes only
   b. Uniquely decodable codes only.
   c. Instantaneous codes only.
   d. Instantaneous and optimal codes.

(4 + 1 + 1 + 1 + 2 Marks)

BITS PILANI – DUBAI
International Academic City, Dubai
First Semester 2011 – 2012
Information Theory and Coding ECE C393 (III year)
Quiz 2 Set A (Closed Book)

Duration: 20 minutes **Weightage: 7%**
30 November 2011 **MAX: 7 Marks**

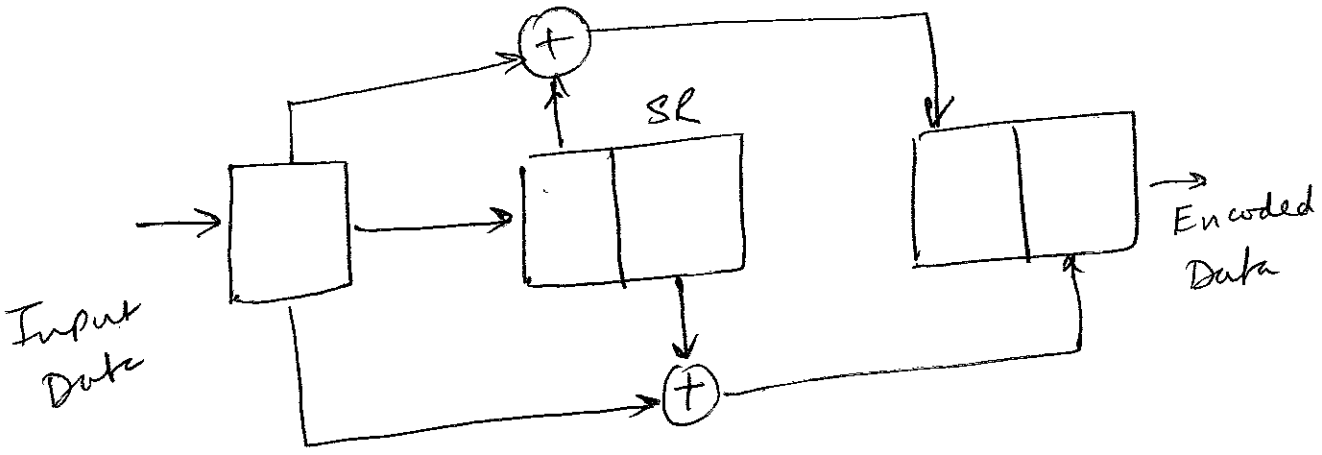
Note: Show all working to get full credit.

1) Assume that Music is band limited to 20 KHz. **(0.5 + 0.5 + 1 Marks)**
   a. What is a good sampling rate for this signal? Why?
   b. If 20 bits per sample are used in source coding, what is the required transmission rate?
   c. What should be the SNR of a channel that is band limited to 200 KHz in order for this signal to be transmitted?

2) For a (15, 11) linear block code (**0.5 + 1 + 0.5 + 1 Marks**)
   a. What is the code rate? Justify your answer.
   b. Can d* have the values 2, 5, 7? Justify your answer.
   c. For what value of d* is it a Maximum Distance Separable (MDS) code?
   d. How many bit errors can be corrected for this code?

3) Given the following pattern P = 1100000001111, answer the following questions: **(0.5 + 1 Marks)**
   a. What is the size of FCS bits?
   b. What is the length of the longest burst error that can be detected with 100% accuracy?

4) Write down the Generator Polynomial Matrix, G, for the shift register convolution encoder given below. **(0.5 Mark)**



BITS PILANI – DUBAI
International Academic City, Dubai
First Semester 2011 – 2012
Information Theory and Coding ECE C393 (III year)
Quiz 1 Set A (Closed Book)

Duration: 20 minutes **Weightage: 8%**
2 November 2011 **MAX: 8 Marks**

Note: Show all working to get full credit.

1) Is it possible for an instantaneous code to have the following alphabet size (D) and codeword lengths? Justify your answers. **(1 Mark)**
   a. D = 4; $l_1 = 1, l_2 = 1, l_3 = 1, l_4 = 1$
   b. D = 2; $l_1 = 1, l_2 = 1, l_3 = 1, l_4 = 1$

2) Given the following probabilities and codeword lengths,
   a. Are the codeword lengths for a Shannon code or Shannon-Fano-Elias code? Justify your answer.
   b. Is the codebook likely to be optimal? Justify your answer.

X	p(x)	l(x)
1	0.25	3
2	0.25	3
3	0.5	2

(1 + 2 Marks)

3) What are ***one*** reason why the following codebook ***cannot*** be Huffman code:

(1 Mark)

X	p(x)	Codeword
1	0.25	01
2	0.25	100
3	0.2	11
4	0.15	000
5	0.15	001

4) Given that $b_5 = 0.3426$ and $l_5 = 0.00001$ when encoding a sequence of length 5 with Arithmetic code, what is the minimum number of bits required for this code? Show all working. **(1 Mark)**

5) In Lempel Ziv Welch (LZW) *encoding*, if the Extended Dictionary value reaches 64 for an initial Dictionary that contains 52 characters, what is the size of the *next* output character? Justify your answer. **(1 Mark)**

6) What is the channel capacity of Binary Symmetric Channel for which the probability of error is 0.0001? Show all working. **(1 Mark)**