

Assessment 2

Assessment Number	2
Contribution to Overall Mark	10%
Submission Deadline	19 May, 2019, Sunday, Week 13

Assessment Objective

This assessment aims at evaluating students' understanding and problem solving skills involved in channel coding and cryptography, which are accumulated during lectures, tutorials and after-class study.

Submission Procedure

Please submit one electronic copy on **ICE** and one hardcopy to the submission box in front of office **EE320**.

Marking Scheme

The specific marks assigned are shown on the right column of each question and sub-question.

Question 1: Hamming Codes (25 points)

Consider the systematic (7, 4) Hamming code. The parity-bit generator matrix P is shown below.

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

- i) Give the corresponding generator matrix G and the parity check matrix H . (4 points)
- ii) Generate the code words for the following messages: 0100, 1010. (8 points)
- iii) Determine whether the received words 1010010, 0111100, 0011100 are valid code words using the syndrome decoding and correct if necessary. Decode the codewords to recover the original messages. (13 points)

Question 2: Cyclic Codes (24 points)

Consider a (n, k) cyclic redundancy check (CRC) code. Verify if the following generator polynomials are able to catch certain types of errors.

- i) Single-bit of error with error polynomial of $e(x) = x^i$:
 - $g(x) = x + 1$; (6 points)
 - $g(x) = x^5$; (6 points)
- ii) Two isolated single-bit errors with error polynomial of $e(x) = x^j + x^i$:
 - $g(x) = x^2 + 1$; (6 points)
 - $g(x) = x^{14} + x^{13} + 1$. (6 points)

Question 3: Convolutional Codes (26 points)

Design a rate $1/2$ convolutional encoder with a constraint length $v = 4$ and $d^* = 6$.

- i) Construct the State Diagram of this encoder. (6 points)
- ii) Construct the Trellis Diagram of this encoder. (6 points)
- iii) What is the d_{free} of this code. (4 points)
- iv) Determine the Generator Matrix G . (6 points)
- v) Is this code Non-Catastrophic? Why? (4 points)

Question 4: Cryptography (25 points)

Given two prime numbers 29 and 61, calculate

- i) Public key for the RSA algorithm. (10 points)
- ii) Private key for the RSA algorithm. (15 points)