**National University of Sciences & Technology**

**Military College of Signals**

**IS-842 Applied Cryptography**

**MSIS-11 (Fall 2012)**

**Quizz #2**

Maximum Time: 15 Minutes

Maximum Marks: 10

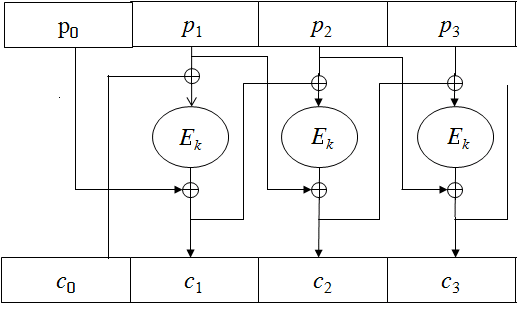
Instructor: Brig (R) Dr. Ashraf Masood

Note: Attempt ALL questions. For full credits, justify your answers with appropriate reasons wherever required.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Question #1**

Let EK(p) and DK(c) be a block cipher. We consider a new block cipher mode as depicted in the figure where IV={ p0, c0}



1. Write the equation representing Encryption and Decryption operation for this new mode.
2. Draw the diagram showing how to decrypt.
3. Suppose ciphertext block c3 is damaged in transit. Which plaintext blocks become undecipherable as a result? Explain. [5 Marks]

**Question #2**

An attacker intercepts the following ciphertext (hex encoded):

20814804c1767293b99f1d9cab3bc3e7ac1e37bfb15599e5f40eef805488281d   
  
He knows that the plaintext is the ASCII encoding of the message "Pay Bob 100$" (excluding the quotes). He also knows that the cipher used is CBC encryption with a random IV using AES as the underlying block cipher. Show that the attacker can change the ciphertext so that it will decrypt to "Pay Bob 500$". What is the resulting ciphertext (hex encoded)? This shows that CBC provides no integrity. [5 marks]

**Question #3 [Bonus Question]**

Consider the following proposal for block ciphers mode





This is not a useful mode; why? [2 Marks]

**ASCII Table**

