`CS3C03/SE4C03` `Test 3` `Winter 2012`

Name ________________________ Student No. ________________________

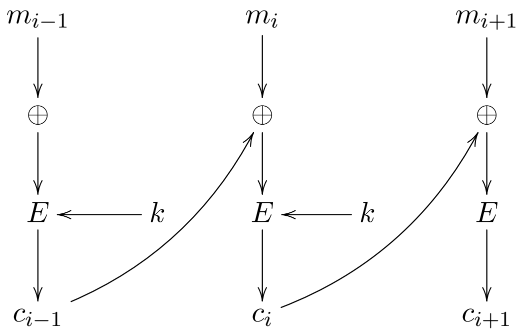
No aids allowed. Answer all questions on test paper. Use backs of sheets if necessary.

Total Marks: **30**

[10] 1. This question is based on the article *Cloud Computing*, by Brian Hayes, who says that even though the future of cloud computing is not perfectly clear, a few examples of present practice suggest likely directions. Give two such examples and provide brief descriptions.

Solution: The author gives four different examples (you were asked to provide two): Wordstar for the Web; Enterprise computing in the cloud; Cloudy infrastructure; The cloud OS. See the article for descriptions.

[10] 2. Consider a portion of cipher block chaining (CBC), depicted in the figure below.



(a) Suppose that an adversary intercepts the message, and wants to flip the 9-th bit of message block m_i, that is, he wants to change the ciphertext in such a way that the 9-th bit of message block m_i is flipped. How would he go about it? Justify your answer.

Solution: All he needs to do is to flip the 9-th of c_{i-1}. The reason is that c_i is xor'ed with the result of decrypting c_i with key k; call the result of this decryption d_i. Then, $m_i = d_i \oplus c_{i-1}$, and if $x \oplus y = y$, then $\bar{x} \oplus y = \bar{z}$.

(b) How could the legitimate recipient of the message detect the tampering?

Solution: By changing one bit of c_{i-1}, the attacker is forced to change m_{i-1}. Further, if the encryption/decryption algorithm has a good "mixing property," by changing one bit of c_{i-1} the attacker is likely to change many bits of m_{i-1} in a way that he has no control over. This could be detected by the recipient, especially if a CRC is used.

[10] 3. Explain the “Bucket Brigade / Man-in-the-Middle” attack against Diffie-Hellman. What is a possible defense against this attack?

Solution: See pp. 168 and 169 in KPS.