# Internet Infrastructure Security (COMP444)
# A2

Due at 11:55pm on 12 February 2015
Submission site: `https://submit.comp.polyu.edu.hk/`

Rocky K. C. Chang

February 5, 2015

1. `[6 marks]` (CBC without padding) Figure 1 shows a method for CBC-DES encryption and decryption without padding the plaintext to an integral number of blocks. This diagram, though drawn differently with different terms, is the same as ours in the slides. The thick-lined boxes are for DES encryption, while the thin-lined for DES decryption. The key is given by $CW$, and Whitener1 is the IV. As shown, the plaintext's length is between two blocks and three blocks. We again use $m_1$ and $m_2$ to denote the first two plaintext blocks, and $m_3$ to denote the remaining data.

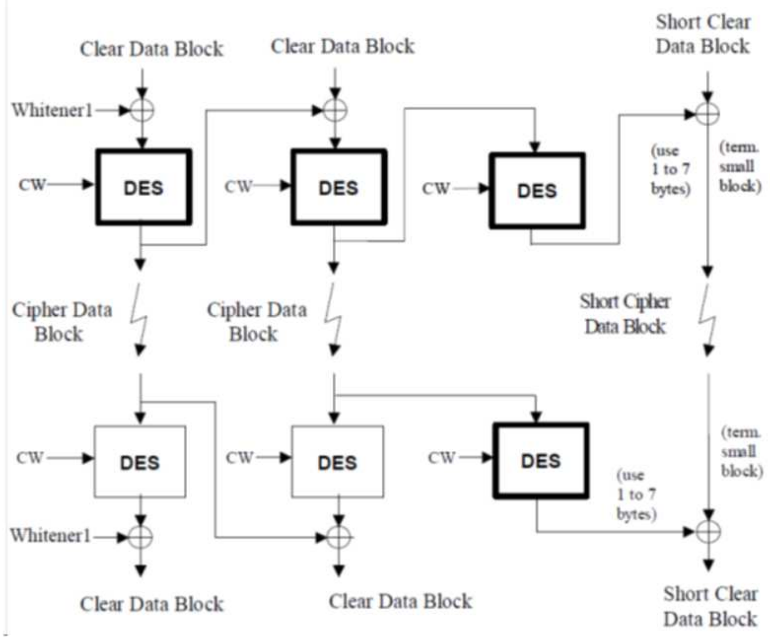

Figure 1: CBC-DES with special processing for the last "block" of data.

   (a) `[3 marks]` Write down the expression for encrypting $m_3$. You could use $c_i$ for the $i$th ciphertext block, $E()$ for encryption, and $D()$ for decryption.

   (b) `[3 marks]` Show how $m_3$ is recovered from the CBC-DES decryption.

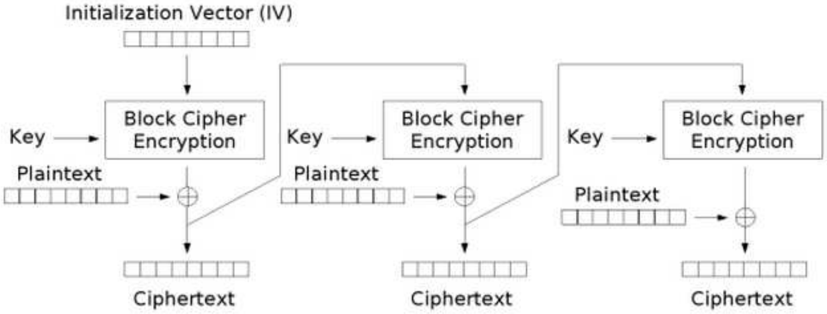

Figure 2: Encryption using a slightly different CBC.

2. `[6 marks]` (A different CBC) Consider a slightly different CBC encryption in Figure 2.

   (a) `[3 marks]` Based on Figure 2, write down the encryption and decryption functions using our usual notations $m_i$ and $c_i$ for the $i$th plaintext block and $i$th ciphertext block, respectively.

   (b) `[3 marks]` If bit 3 of $c_i$ is modified, what kind of changes will be made to the plaintext after decryption? (Hint: slide 37 of Introduction to Block Ciphers)