King Fahd University of Petroleum and Minerals
College of Computer Sciences and Engineering
Department of Computer Engineering

COE 451 – Computer and Network Security (T151)

Programming Assignment (due date & time: Sunday 01/11/2015 during class period)

Description:

Using any programming language, implement both an **ECB** mode and a **CBC** mode of the **Tiny Encryption Algorithm (TEA)** with 32 rounds for encrypting each block. Use the following 128-bit key (represented in HEX): **`A56BABCD00000000FFFFFFFFAB3D7F31`**. **Leave the first 10 blocks unencrypted**. Test your implementation of both the ECB and the CBC modes by using the following linked image to show a diagram analogous to that in Figure 3.3.

Deliverables:

1. Submit a hard copy of your diagrams.
2. Submit a **well-documented** soft copy of your implementation to marwan@kfupm.edu.sa and g201307310@kfupm.edu.sa along with a **readme file** on how to execute your implementation.

As usual, the implementation should be based on your own genuine effort ☺