CS 463/563: Cryptography for Cybersecurity
Spring 2024
Homework #5
Points: 20

Consider a simple system with **8-bit block size**. Assume the encryption (and decryption) to be as follows:

If plaintext is LT||RT and the key is **LK||RK**, where **LC, RC, LT,** and **RT** are each 4 bits, then ciphertext = LC||RC where **LC=LK XOR RT**; and **RC = RK XOR LT**; Plaintext and ciphertext are each 8 bits.

Similarly, to decrypt ciphertext, we perform exactly the reverse operation where,
LT=RC XOR RK and RT = LC XOR LK.

You are given the following 16-bit input **A8B9** (in Hexa).

You are provided IV as: **A9** (Hexa).

For **CTR** assume the stream of bits to be used for counter to be starting from **0001** and incremented by 1 every time; so, the stream would be 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111 …

The **8-bit key** to be used (where appropriate) is **C5** (Hexa).

Compute the encrypted output with

- **(i) ECB**
- **(ii) CBC**
- **(iii) OFB**
- **(iv) CFB**
- **(v) CTR (with IV = 0101)**

Express the output as **4 Hexa** characters so it is easy to read.

What to submit? Submit a pdf file with your answers via Canvas. Show your work