1. IV Randomness

In CBC IVs are selected at random. Your friend, after buying and reading a used crypto book, tries to implement a cipher and decides that random IVs are a bit excessive. They propose that instead IVs for different messages be chosen iteratively rather than randomly (i.e. the IV for message $m_2$ is simply one larger than the IV for message $m_1$). Build an Chosen Plaintext Attack (CPA) against your friend’s system demonstrating that this method of using CBC is not secure.

2. Transmission Errors

Pretend that one byte of a cipher text gets garbled during transmission, either through accident or malicious action. What is the impact of this one byte of garbled data on the decryption for CBC, OFB, and CTR modes? What is the impact of an entire block being dropped during transmission on CBC, OFB, and CTR modes?

3. Output Sizes

Say CBC mode encryption is used to encrypt a 1024 bit message with a block cipher having a 256 bit key, a 128 bit block length. What is the length of the resulting cipher text? Why?

4. Rotating AES

Let’s Define Rotating Mode AES as follows. An IV is generated, prepended to the front of the cipher text. The first block of the message is fed through the block cipher and then the output bits are right rotated a number of positions equal to the unsigned integer interpretation of the IV. This value becomes the first block of the cipher text. The next block of the message is fed into the block cipher, and then right rotated a number of positions equal to the unsigned integer interpretation of the first block of cipher text. This process continues with each block. In other words the ith block of the message is processed by feeding it into the block cipher and right rotating the result a number of positions equal to the integer interpretation of the (i-1)th block of cipher text. Assuming our block cipher is a strong pseudo-random function, prove or disprove that this mode is secure against a CPA adversary.
• Let’s define rotating IV mode AES as follows. An IV is generated, prepended to the front of the cipher text. The first block of the message is XORed with the IV and fed into the block cipher. The output becomes the first block of the cipher text. The IV is then right rotated one position, and used in a similar fashion for the second block, repeating until all blocks are encrypted. Assuming our block cipher is a strong pseudo-random function, prove or disprove that this mode is secure against a CPA adversary.

5. (Grad only) Double Cipher

Solve question 3.29 from the textbook.