Jacobs University Bremen Due: Dec 18, 2022
Dr. Amr Alanwar
Tewodros Adane(Teaching Assistant) Assignment 3

MCSSE-CYB-01 Cryptography

In this project you will implement two decryption systems, one using AES in CBC mode and another using AES in counter mode (CTR). In both cases the 16-byte encryption IV is chosen at random and is *prepended* to the ciphertext.

For CBC encryption we use the PKCS5 padding scheme. In the following questions you are given an AES key and a ciphertext (both are hex encoded) and your goal is to recover the plaintext.

For an implementation of AES you may use an existing crypto library such as Pycryptodome (Python), cryptography(Python), Crypto++ (C++), or any other. While it is fine to use the built-in AES functions, you must implement CBC and CTR modes yourself.

Submission: Put the source code and a pdf file containing the plaintexts in a zip file and upload to moodle.

CBC mode:

1. **Key:**
   140b41b22a29beb4061bda66b6747e14
   Ciphertext:
   4ca00ff4c898d61e1edbf1800618fb2828a226d160dad07883d04e008a7897ee2e4b7465d5290d0c0e6c6822236e1daafb94ffe0c5da05d9476be028ad7c1d81

2. **Key:**
   140b41b22a29beb4061bda66b6747e14
   Ciphertext:
   5b68629feb8606f9a6667670b75b38a5b4832d0f26e1ab7da33249de7d4afc48e713ac646ace36e872ad5fb8a512428a6e21364b0c374df45503473c5242a253

CTR mode

1. **Key:**
   36f18357be4dbd77f050515c73fcf9f2
   Ciphertext:
   69dda8455c7dd4254bf353b773304eec0ec7702330098ce7f7520d1cbbb20fc388d1b0adb5054dbd7370849dbf0b88d393f252e764f1f5f7ad97ef79d59ce29f5f51eeca32eabedd9afa9329

2. **Key:**
   140b41b22a29beb4061bda66b6747e14
   Ciphertext:
   770b80259ec33beb2561358a9f2dc617e46218c0a53cbeca695ae45faa8952aa0e311bde9d4e01726d3184c34451