Information Security and Management

Homework 1
Fall 2025

1 Cryptographic Primitives for C++/.NET/Java/Python

The followings are some popular packages for Cryptography:

- C++
  1. **Crypto++:** Crypto++ Library is a free C++ class library of cryptographic schemes. https://www.cryptopp.com/
  2. **Botan - Crypto and TLS for Modern C++:** Botan (Japanese for peony flower) is a C++ cryptography library released under the permissive Simplified BSD license. https://botan.randombit.net/
- .NET
  1. **Security in .NET:** The common language runtime and the .NET provide many useful classes and services that enable developers to easily write secure code and enable system administrators to customize the permissions granted to code so that it can access protected resources.
     https://docs.microsoft.com/en-us/dotnet/standard/security/
     Note: Cryptography Model
- Java
  1. **Java Cryptography (JCA/JCE)** The Java platform strongly emphasizes security, including language safety, cryptography, public key infrastructure, authentication, secure communication, and access control.
     Java Cryptography Architecture (JCA) Reference Guide:
     https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html
- Python
  1. **pyca/cryptography**: It includes both high level recipes and low level interfaces to common cryptographic algorithms such as symmetric ciphers, message digests, and key derivation functions.
     https://cryptography.io/en/latest/
  2. **Python Cryptography Toolkit (pycrypto)**: This is a collection of both secure hash functions (such as SHA256 and RIPEMD160), and various encryption algorithms (AES, DES, RSA, ElGamal, etc.).
     https://pypi.org/project/pycrypto/
  3. **PyCryptodome:** PyCryptodome is a self-contained Python package of low-level cryptographic primitives.
     https://www.pycryptodome.org/

2 Problems

- Please apply one of the above packages for the following block cipher modes to implement the *encryption/decryption*: **AES-CBC** and **AES-OFB**. You should encrypt *plaintext files* into ciphertext files, and then decrypt them. **Observe and analyze your output results** by adopting *different IVs* in enciphering phase, and *modifying IV, ciphertext and decryption key* in deciphering phase to observe the decryption results.

- Calculate the output of the MixColumns transformation in AES for the column vector input:

$$\begin{bmatrix} B3 \\ C9 \\ E2 \\ A5 \end{bmatrix}$$

  by referring to the textbook pp.180-183. Apply the InvMixColumns transformation to the obtained result to verify your calculation.

3 Schedule

- **Problem due date:** Friday, 31 Oct. 2025