

## Programming Assignment 2

### Known plaintext attacks with short keys:

In this assignment, we work with the AES-128 algorithm, which we will use from a library. For Python, I recommend the library `cryptography` [Link here](#). For C/C++, I suggest `libgcrypt`: [Link here](#) or `openssl`: [Link here](#). Sample programs for each are included in the files. You may also use any publicly available AES-128 implementation instead.

1. In the first part, the goal is to find a 20-bit key by a brute-force attack. Since AES uses a 128-bit key, a 24-bit key is fed into an expansion subroutine that produces a 128-bit long key. The subroutine ignores the last 4-bits of the short key so that the effective key length is 20. The key expansion subroutine is given to you as C and Python files.

A set of four plaintexts and five ciphertexts are given to you as two text files, with the ciphertexts corresponding to the four given plaintexts and one secret plaintext. Use one of the plaintext, ciphertext pairs to find the key and hence find the secret plaintext as well.

2. In the second part, we do a meet-in-the-middle attack. Here the encryption is done using two 16-bit keys. Firstly, each key is expanded via a key expansion routine (given to you) to obtain two long (128-bit) keys. Then the message is encrypted with the first long key, and then again with the second long key, to obtain the ciphertext.

A set of four plaintexts and five ciphertexts is given as input and the goal is the same as in part 1.