Information Systems Security Laboratory

Spring 2021

Assignment – 3 Date: April 01, 2021

1. Implement the Auto-key Cipher.

2. Implement the following classic polyalphabetic ciphers (Generate the keys pseudo-randomly, check validity of the key, and store it into a key-file):
   a. Vigenere Cipher
   b. Keyed Transposition Cipher (Assume the block size to be 5.)

3. Modify the Hill Cipher program you wrote for Assignment 1, so as to implement the following *Permutation Cipher*: (Following π is a permutation of plain text letters positioned at {1, …, 8})

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	1	6	2	7	3	8	5

Test the operation of your encryption and decryption programs using the above π and its corresponding π^{-1}. Hence decrypt the following cipher text, which was encrypted using the above π:

TGEEMNELNNTDROEOAAHDOETCSHAEIRLM

HINT: The key of a transposition cipher may be represented as a matrix of zeros and ones.

(In the following assignment you may consider plaintext, ciphertext and key-streams as bit sequences.)

4. A One-Time Pad (OTP) is a stream cipher which uses True Random Number Generator (TRNG) to generate its key-stream, hence the name OTP.

It uses the XOR-operation as both encryption and decryption functions.

a) Implement an OTP.

(You may use any Pseudo-Random Number Generator (PRNG) to generate the key-stream here considering that following a physical process is infeasible for this laboratory.)

b) Assuming the PRNG looks like:

$$S_0 = \text{seed}$$
$$S_{i+1} \equiv AS_i + B \bmod m,\ i = 0,1, \ldots$$

where $m = 26$ is public, the secrets are A, B and the seed, where all A, B, S_i belong to Z_{26}, and an outsider is provided with the knowledge of only first 15 bits of plaintext, implement a way for (known-plaintext) cryptanalysis of the OTP.

[Hint: Note that $2^4 < 2^6 < 2^5$]