COMP5631: Cryptography and Security
2025 Spring – Written Assignment Number 2
Handed out: on Feb. 21, 2023
Due: on March 9 by 11:30pm.

Please upload your solution paper into Canvas by 23:30 on March 9. No email submission will be accepted.

Q1. Please read the transposition cipher documented in the Appendix of Lecture 2. Then use the example transposition cipher on Slide No. 25 to encrypt the message `killthem`. Write down the corresponding ciphertext. [10 marks]

Q2. There are ten pieces of ciphertext in the following URL:
[Click here]
Each of them is obtained by encrypting an English article with a simple substitution cipher. Let ℓ denote the last digit in your student ID number, please then choose the $((\ell + 1) \bmod 10)$-th ciphertext and recover the original plaintext.

You may write your own computer programs or use the following online software to compute the frequencies of single letters, digraphs and trigraphs in the ciphertext for you:

`https://www.cryptoclub.org/#vCiphers`

Please write down certain details of your decryption process. You need to write down your decrypted text (i.e., the readable text), but do not need to write down the one-to-one function used for encryption. [30 marks]

Q3. Consider the example cipher on Slide No. 22 of Lecture 3, where p is a prime. Let $\ell = 2$ (i.e., the cipher has two rounds of iteration of the round function $f_h(x)$). Write down the encryption function $E_k(m)$ and decryption function $D_k(c)$ of this cipher. [20 marks]

Q4. Given a one-key block cipher $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E_k, D_k)$, where $\mathcal{M} = \mathcal{C}$ and E_k maps an n-bit block into an n-bit block, we can construct a new one-key block cipher by picking up two keys k_1 and k_2 for the original cipher to form a key $k = (k_1, k_2)$ for the new block cipher. The encryption and description of the new cipher go as follows:

Encryption: $c = E_{k_2}(E_{k_1}(m))$.
Decryption: $m = D_{k_1}(D_{k_2}(c))$.

Thus the new block cipher has the same block length as the original cipher, but its key length doubles that of the original cipher. This is the double encryption introduced in Lecture 5.

Design a specific one-key cipher and show that double-encryption with this cipher does not increase the security level of the original cipher at all. [Hint: Consider some of the ciphers on some lecture sides.] [20 marks]

Q5. Show that the Diffie-Hellman Key Exchange (Agreement) Protocol is insecure with respect to active attacks. [20 marks]