COMP5631: Cryptography and Security
2016 Fall – Written Assignment Number 1
Sample Solutions

Q1. Find the multiplicative inverse of 29 modulo 1137. Write down all steps of your computation. Please use the extended Euclidean algorithm, which is a slight modification of the Euclidean algorithm. $\boxed{\text{20 marks}}$

Solution: It is 941. Details of the computation are omitted here.

Q2. You are given a piece of ciphertext with 2000 English letters whose original plaintext is a piece of English writing. You are told that the encryption was with either a transposition cipher or a simple substitution cipher. How do you detect the type of the cipher used for the encryption? Justify your answer please. $\boxed{\text{20 marks}}$

Solution: Count the frequencies of single English letters in the ciphertext and the frequencies of digraphs (also bigrams). Then compare them with the standard frequency distribution of single English letters in the English language. If they match, it must be a transposition cipher. If they differ by a large extent, it must be simple substitution cipher. If they differ by a small extent, we compare the set of the frequencies of digraphs in the ciphertext with that in the English language. If they differ, it is a transposition cipher. Otherwise it is a simple substitution cipher.

This method works as transposition ciphers do not change the frequencies of single English letters when it is used to encrypt the plaintext, while simple substitution ciphers usually do.

Q3. There are ten pieces of ciphertext in the following URL:
http://www.cs.ust.hk/faculty/cding/COMP581/c685-5.html
Each of them is obtained by encrypting an English article with a simple substitution cipher. According to the last digit in your student ID number, please choose the corresponding ciphertext and recover the original message.

You may use the following online software to compute the frequencies of single letters, digraphs and trigraphs in the ciphertext for you:

[Click here]

Please write down details of your decryption process. $\boxed{\text{20 marks}}$

Solution: Omitted here.

Q4. We identify each English letter with an integer between 0 and 25 as follows:

$$\begin{array}{cccccc} A & B & C & \cdots & Y & Z \\ 0 & 1 & 2 & \cdots & 24 & 25 \end{array}$$

Take any pair (k_0, k_1) of integers such that $\gcd(k_0, 26) = 1$ and $0 \leq k_i \leq 25$, and define the 1-to-1 mapping f by

$$f(x) = (xk_0 + k_1) \bmod 26.$$

So f is a permutation (substitution) of the English alphabet.

A **simple substitution cipher** based on f is a 5-tuple $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E_k, D_k)$, where

- $\mathcal{M}$ and $\mathcal{C}$ are the set of all finite strings of English letters;
- $\mathcal{K}$ is the set of all possible f;
- $k = (k_0, k_1) \in \mathcal{K}$ is the encryption and decryption key.
- For a message $m = m_0 m_1 m_2 \cdots$,

$$E_k(m) = f(m_0) f(m_1) f(m_2) \cdots$$

- For a ciphertext $c = c_0 c_1 c_2 \cdots$,

$$D_k(c) = f^{-1}(c_0) f^{-1}(c_1) f^{-1}(c_2) \cdots$$

Use the secret key $(k_0, k_1) = (3, 1)$ to encrypt the message "lecture" (20 marks)

Solution: We have

- $E_k(l) = f(l) = (11 \times 3 + 1) \bmod 26 = 8 = i.$
- $E_k(e) = f(e) = (4 \times 3 + 1) \bmod 26 = 13 = n.$
- $E_k(c) = f(c) = (2 \times 3 + 1) \bmod 26 = 7 = h.$
- $E_k(t) = f(t) = (19 \times 3 + 1) \bmod 26 = 6 = g.$
- $E_k(u) = f(u) = (20 \times 3 + 1) \bmod 26 = 9 = j.$
- $E_k(r) = f(r) = (17 \times 3 + 1) \bmod 26 = 0 = a.$
- $E_k(e) = f(e) = (4 \times 3 + 1) \bmod 26 = 13 = n.$

So the ciphertext is: INHGJAN

Q5. Read Slide Nos. 18 – 25 of Lecture 3. Let $a(x) = x + x^2 + x^6 \in \mathrm{GF}(2^8)$ and $b(x) = 1 + x + x^3 + x^7 \in \mathrm{GF}(2^8)$. Then work out the following:

- Find out $-a(x)$. (2 marks)
  Solution: $-a(x) = a(x)$.
- Compute $a(x) + b(x)$. (2 marks)
  Solution: $a(x) + b(x) = 1 + x^2 + x^3 + x^6 + x^7$.
- Compute $a(x) \times b(x)$. (6 marks)
  Solution: We have

$$\begin{aligned} a(x) \times b(x) &= a(x)b(x) \bmod p(x) \\ &= (x^{13} + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x) \bmod x^8 + x^4 + x^3 + x + 1 \\ &= x^2 + x^3 + x^5 + x^7. \end{aligned}$$

- Find out the multiplicative inverse $c(x)$ of $a(x)$, i.e., $c(x) \in \mathrm{GF}(2^8)$ such that $a(x) \times c(x) = 1$. 10 marks)
  Solution: Since $p(x) = x^8 + x^4 + x^3 + x + 1$ is irreducible over GF(2) and $a(x)$ is not the zero polynomial, $\gcd(a(x), p(x)) = 1$. Applying the extended Euclidean algorithm for polynomials to $a(x)$ and $p(x)$, we obtain

$$\gcd(a(x), p(x)) = 1 = u(x)a(x) + v(x)p(x),$$

where $u(x) = x^7 + x^6 + x^5 + x^4 + x^2 + 1$ and $v(x) = x^5 + x^4 + x^3 + x^2 + 1$. It then follows that the multiplicative inverse $c(x)$ of $a(x)$ is given by

$$c(x) = u(x) \bmod p(x) = u(x) = 1 + x^2 + x^4 + x^5 + x^6 + x^7.$$