MTH6115 Cryptography Exercises 4 Solutions

Q1 Suppose π is the permutation of A which is used by the substitution cipher. Choose $x \in A$ and let the keyword be $k = xxxxx\ldots$. Let S be the substitution table in which each column is the same and is given by the action of π on A. So if $A = \{x_1, x_2, \ldots, x_q\}$ then each column of S is equal to $(\pi(x_1), \pi(x_2), \ldots, \pi(x_q))^T$. The resulting stream cypher replaces each symbol x_i in the plain text by $x_i \oplus x = \pi(x_i)$. This is the same as the substitution cipher. (This solution is not unique. For example we could take any keyword k' with the substitution table S since the keyword is irrelevant, or take any substitution table S' with the keyword k as long as the column of S' labeled by x corresponds to π, since the other columns are irrelevant. In general we could take any keyword and any substitution table with the property that the columns in the substitution table labeled by the letters in the keyword correspond to π.)

Q2 (a)

	0	1	2	3
0	2	3	0	1
1	0	1	2	2
2	1	0	3	3
3	3	2	1	0

(b) (i) Each column of S_1 corresponds to a permutation of A. We construct S_2 by replacing each column of S_2 by the column corresponding to the inverse permutation.
(ii) For $S_1 = S_2$ we need the permutation corresponding to each column of S_1 to be equal to its own inverse.
(c)

	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

Note, solution is not unique. We can permutate the columns of the above table and obtain another example.

Q3 (a) Let $k_1 = a_1a_2\ldots$ and $k_2 = b_1b_2\ldots$. Number the letters of the alphabet by $0, 1, \ldots, 25$ and suppose that for all $i \geq 1$, a_i is the letter of the alphabet numbered m_i and b_i is the letter of the alphabet numbered n_i. Let $p = p_1p_2\ldots$ be a plaintext. For each $i \geq 1$, C_1 encrypts p_i by shifting it m_i places to the right, then C_2 shifts it n_i places further to the right. Thus C is a Vigenère cipher obtained by shifting p_i $m_i + n_i$ places to the right. The corresponding keyword is $k = c_1c_2\ldots$ where c_i is the letter of the alphabet numbered $m_i + n_i$ (modulo 26). (Equivalently k is obtained by encrypting the keyword k_1 using the Vigenère cipher C_2).

(b) Let $k = c_1c_2\ldots$ and $A = \{x_1, x_2, \ldots, x_q\}$. For each $x_j \in A$, let α_j, respectively β_j, be the permutation of A corresponding to the column of S_1, respectively S_2, labeled by x_j. Let $p = p_1p_2\ldots$ be a plain text. Choose $i \geq 1$

and suppose that $k_i = x_j$. Then C_1 encrypts p_i as $\alpha_j(p_i)$ and C_2 then encrypts $\alpha_j(p_i)$ as $\beta_j(\alpha_j(p_i))$. Thus C encrypts p_i is $\gamma_j(p_i)$ where γ_j is the permutation of A given by $\gamma_j = \alpha_j \circ \beta_j$. It follows that C is a stream cipher with keyword k and substitution table S, where for each $x_j \in A$, the column of S labelled by x_j corresponds to the permutation $\gamma_j = \alpha_j \circ \beta_j$ of A.

(c) Suppose that C is a stream cipher with keyword $k = c_1 c_2 \ldots$ and substitution table S. Consider a plaintext $p = p_1 p_2 p_3 p_4 \ldots$. If $p_1 = 0$ then C_1 encrypts p_1 as 0, and then C_2 encrypts as 0. So C encrypts $p_1 = 0$ as 0. We can see similarly that C encrypts $p_1 = 1$ as 1 and C encrypts $p_1 = 2$ as 2. This implies that the column of S labeled by c_1 is $(0, 1, 2)^T$. Using a similar argument we see that the columns of S labeled by c_2, c_3 and c_4 are $(1, 2, 0)^T$, $(1, 0, 2)^T$,and $(2, 0, 1)^T$, respectively. This is impossible since S is a 3×3 matrix so it cannot have four different columns.