CRYPTOGRAPHY TOPIC V
STRINGS, PERMUTATIONS, AND CRYPTOSYSTEMS

PAUL L. BAILEY

1. Functions

We begin by recalling some definitions and results from Topic II.

Definition 1. Let A be a set. The *identity function* on A is the function

$$\mathrm{id}_A : A \to A \quad \text{given by} \quad f(a) = a.$$

Let $f : A \to B$ and $g : B \to C$. The *composition* of f and g is the function

$$g \circ f : A \to C \quad \text{given by} \quad (g \circ f)(a) = g(f(a)).$$

Let A and B be sets, and let $f : A \to B$.

(a) f is *injective* if $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$;
(b) f is *surjective* if for every $b \in B$ there exists $a \in A$ such that $f(a) = b$;
(c) f is *bijective* if f is injective and surjective;
(d) f is *invertible* if there exists $g : B \to A$ such that $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{id}_A$;
(e) if $C \subset A$, the *image* of C under f is

$$f(C) = \{b \in B \mid b = f(c) \text{ for some } c \in C\}.$$

(f) if $D \subset B$, the *preimage* of D under f is

$$f^{-1}(D) = \{a \in A \mid f(a) \in D\}.$$

We see that f is invertible if and only if f is bijective. Moreover, f is bijective if and only if the preimage of every singleton in B is a singleton set in A.

If f is invertible, its inverse is unique, and is denoted by f^{-1}. It is immediate from the definition that if f is invertible, then so is f^{-1}. Thus f and f^{-1} are bijective.

Date: October 19, 2007.

2. Strings

A string is a finite sequence, or synonymously, an ordered n-tuple. We make a formal definition.

Definition 2. Let A be a set.

A *string of length* n in A is a function $\widehat{a} : \{1, \ldots, n\} \to A$, where n is a positive integer. We may write a_i instead of $\widehat{a}(i)$, and we may write $(a_1, \ldots, a_n)$ to denote the entire string. The set of all strings in A of length n is denoted A^n:

$$A^n = \{\widehat{a} : \{1, \ldots, n\} \to A\}.$$

The *empty string*, or *string of length zero*, is the empty set $\varnothing$.

A *string in* A is either a string of length n for some n, or is the empty string. The set of all strings in A is denoted A^ω:

$$A^\omega = \left(\cup_{n=1}^{\infty} A_n \right) \cup \{\varnothing\}.$$

If $\widehat{a} \in A^\omega$, we define its *length* to be

$$\text{len}(\widehat{a}) = \begin{cases} n & \text{if } \widehat{a} \in A^n; \\ 0 & \text{if } \widehat{a} = \varnothing. \end{cases}$$

3. Permutations

Definition 3. Let X be a set. A *permutation* of X is a bijective function $\alpha : X \to X$.

The set of all permutations of X is called the *symmetry group* of X, and is denoted $\text{Sym}(X)$:

$$\text{Sym}(X) = \{\alpha : X \to X \mid \alpha \text{ is bijective}\}.$$

The *cardinality* of a let A is (loosely speaking) the number of elements in it, and is denoted $|A|$. Let us investigate $|\text{Sym}(X)|$.

Suppose that $|X| = n$, where $n \in \mathbb{N}$, and enumerate the element of X as $x_1, x_2, \ldots, x_n$. Decide how many choices α has to permute this set. First, α can send x_1 to any other element, so there are n choices for $\alpha(x_1)$. Having chosen that, since α should be bijective, $\alpha(x_2)$ cannot equal $\alpha(x_1)$, but it can be anything else, for $n-1$ choices. In general, having chosen $\alpha(x_1), \ldots, \alpha(x_i)$, there are $n-i$ possible choices for $\alpha(x_i)$. Finally, $\alpha(x_n)$ must be the single remaining element. Thus,

$$|\text{Sym}(X)| = \text{ number of ways to construct alpha } = n(n-1)(n-2)\cdots 2 \cdot 1 = n!.$$

Recall that the factorial of n, denoted $n!$, is the product of the distinct natural numbers between 1 and n:

$$n! = \prod_{i=1}^{n} i.$$

We define $0! = 1$. These grow very quickly: the first nine are

$$1! = 1, \quad 2! = 2, \quad 3! = 6, \quad 4! = 24, \quad 5! = 120,$$
$$6! = 720, \quad 7! = 5040, \quad 8! = 40320, \quad 9! = 362880.$$

4. Groups of Permutations

Clearly, the composition of functions from X to X is another function from X to X. Moreover, the composition of bijective functions is bijective. Therefore, the composition of permutations of X is another permutation of X. So, we can compose any two members of $\mathrm{Sym}(X)$ and get another member of $\mathrm{Sym}(X)$. That is,

$$\alpha, \beta \in \mathrm{Sym}(X) \quad \Rightarrow \quad \alpha \circ \beta \in \mathrm{Sym}(X).$$

The *identity permutation* on X, denoted ϵ_X or simply ϵ, is the identity function on X. Note that $\epsilon \in \mathrm{Sym}(X)$.

If $\alpha \in \mathrm{Sym}(X)$, the inverse of α is denoted α^{-1}. Note that $\alpha^{-1} \in \mathrm{Sym}(X)$. Moreover, if $k \in \mathbb{N}$, let α^k denote α composed with itself k times, inductively defined by $\alpha^0 = \epsilon$, $\alpha^1 = \alpha$, and $\alpha^k = \alpha^{k-1} \circ \alpha$. Define $\alpha^{-k} = (\alpha^{-1})^k$. Then clearly α^{-k} is the inverse of α^k.

Let $G \subset \mathrm{Sym}(X)$.

- **(a)** We say that G *contains the identity* if $\epsilon \in G$.
- **(b)** We say that G is *closed under composition* if $\alpha, \beta \in G$ implies $\alpha \circ \beta \in G$.
- **(c)** We say that G is *closed under inverses* if $\alpha \in G$ implies $\alpha^{-1} \in G$.

Definition 4. Let X be a finite set. A *group of permutations* of X is a nonempty subset $G \subset \mathrm{Sym}(X)$ such that

$$\alpha, \beta \in G \quad \Rightarrow \quad \alpha \circ \beta \in G.$$

A *subgroup* of a group of permutations is a subset which is itself a group of permutations.

From the definition, it follows that $\mathrm{Sym}(X)$ is a group of permutations of X. Also, every group of permutations is a subgroup of itself.

Proposition 1. *Let X be a finite set, and let G be a group of permutations of X. Then*

- **(a)** $\epsilon \in G$;
- **(b)** $\alpha \in G \Rightarrow \alpha^{-1} \in G$.

Proof. First we prove **(b)**. Now since X is finite, we have $|X| = n$ for some $n \in \mathbb{N}$. Then $|\mathrm{Sym}(X)| = n!$, and in particular, $\mathrm{Sym}(X)$ is finite. Since $G \subset \mathrm{Sym}(X)$, G is finite.

Let $\alpha \in G$, and consider the set

$$H = \{\alpha^k \mid k \in \mathbb{N}\}.$$

Since G is closed under composition, $H \subset G$, and since G is finite, H is finite. Therefore, there must exist $i, j \in \mathbb{N}$ such that $i < j$ and $\alpha^j = \alpha^i$. Composing both sides with α^{-i} gives $\alpha^{j-i} = \epsilon$, so $\alpha \circ \alpha^{j-i-1} = \epsilon$, and α^{j-i-1} is the inverse of α. Thus G is closed under inverses, which proves **(b)**.

Finally, since G is nonempty, there exists some $\alpha \in G$. By **(b)**, $\alpha^{-1} \in G$, and since G is closed under composition, $\alpha \circ \alpha^{-1} = \epsilon \in G$. □

5. Encryption Schemes

Let $\mathrm{Bij}(A, B)$ denote the set of all bijective functions from A to B. Then $\mathrm{Sym}(A) = \mathrm{Bij}(A, A)$.

Definition 5. An *encryption scheme* (P, C, K, E) consists of

- a set P, called the *plaintext space*;
- a set C, called the *ciphertext space*;
- a set K, called the *key space*;
- a function $E : K \to \mathrm{Bij}(P, C)$.

The elements of P are called *plaintexts*. The elements of C are called *ciphertexts*. The elements of K are called *keys*. The elements of the image of E are called *encryption functions*. The inverses of the encryption functions are called *decryption functions*. We may denote the encryption function $E(k)$ by E_k.

Encryption is accomplished by applying an encryption function E_k to a plaintext. Since an encryption function E_k is bijective, it is invertible, and decryption is accomplished by applying the function E_k^{-1} to the ciphertext.

For example, in the shift cipher as we implemented it:

- $P = \{\texttt{'a'}, \texttt{'b'}, \ldots, \texttt{'z'}\}$;
- $C = \{\texttt{'A'}, \texttt{'B'}, \ldots, \texttt{'Z'}\}$;
- $E_k : P \to C$ is given by $E_k(p) = ((p - \texttt{'a'}) + k)\%26) + \texttt{'A'}$.

Encryption is the process of using an encryption scheme to input a plaintext and output ciphertext. We realize that this can be done sequentially through repeated application. This realization allows us to focus on a smaller plaintext space. We describe this using mathematical jargon.

Let (P, C, K, E) be an encryption scheme. We may produce a new encryption scheme by allowing this encryption scheme to act on strings in P to produce strings in C. Without changing the key space, we obtain an encryption scheme $(P^\omega, C^\omega, K, \widehat{E})$, where

$$\widehat{E} : P^\omega \to C^\omega \text{ is given by } \widehat{E}_k(\widehat{p}) = E_k \circ \widehat{p}.$$

That is, if $\widehat{p} \in P^\omega$, then $\widehat{p}$ is a string in P, so $\widehat{p} : \{1, \ldots, n\} \to P$, and $\widehat{p}(i) = p_i \in P$. Then $\widehat{E}_k(\widehat{p}) = \widehat{c} \in C^\omega$, where $\widehat{c}$ is the string in C defined by $c_i = E_k(p_i)$.

In this way, an encryption scheme induces an encryption on strings of plaintext; We can always take an encryption scheme and implement it on strings. For this reason, it simplifies matters to make the plaintext space as small as is necessary to correctly describe the encryption process.

Moreover, we do not have a practical need for the level of generality whereby the plaintext space and ciphertext space are independent; in discussing the theory, we may safely assume that the plaintext space and the ciphertext space are equal. Above, for example, we may convert the plain text into upper case before beginning the encryption. This leads to our next definition.

6. Cryptosystems

Definition 6. A *cryptosystem* (T, K, E) is an encryption scheme (P, C, K, E) such that $T = P = C$, in which case the cryptosystem is given by

- a set T, called the *text space*;
- a set K, called the *key space*;
- a function $E : K \to \mathrm{Sym}(T)$

The cryptosystem is *balanced* if

$$\alpha \in E(K) \implies \alpha^{-1} \in E(K).$$

The cryptosystem is a *closed* if

$$\alpha, \beta \in E(K) \Rightarrow \alpha \circ \beta \in E(K).$$

The image of the key space is

$$E(K) = \{\alpha \in \mathrm{Sym}(T) \mid \alpha = E_k \text{ for some } k\}.$$

In a balanced cryptosystem, $E(K)$ is a subgroup of $\mathrm{Sym}(T)$, which implies that $E(K)$ is closed under inverses, so that the cryptosystem is also balanced.

In a balanced cryptosystem, the decryption functions are encryption functions with a different key; that is, for each $k_1 \in K$ there exists $k_2 \in K$ such that $E_{k_1}^{-1} = E_{k_2}$. We call k_2 the *inverse key* of k_1. This does not imply that, given k_1, the appropriate k_2 is easy to find. A cryptosystem is called *symmetric* if it is balanced, and the inverse key to a given key is easy to compute. Otherwise, the cryptosystem is *asymmetric*.

In practice, in a balanced cryptosystem, decryption can be accomplished using the same computer program as encryption.

In a closed cryptosystem, double encryption using key k_1 and then key k_2 does not increase security, because there exists a key k_3 such that $E_{k_2} \circ E_{k_1} = E_{k_3}$. This does not imply, however, that such a k_3 is easy to find given k_1 and k_2.

7. Primal Cryptosystems

Definition 7. A *primal cryptosystem* is a cryptosystem (A, K, E) such that

- the text space A is called an *alphabet* whose elements are called *letters*;
- the function $E : K \to \mathrm{Sym}(A)$ is injective.

The first condition above simply introduces new jargon, and the second says that distinct keys correspond to distinct permutations of A. This will be more distinguished from cryptosystems in general when we discuss block ciphers.

Example 1. We describe a subset of the `xor` cipher as a primal cryptosystem (A, K, E) in this way:

- the alphabet is $A = \mathbb{Z}_{256}$, the set of all bytes;
- the key space is $K = \mathbb{Z}_{256}$;
- the encryption functions are given by $E_k : x \mapsto x \oplus k$.

Here, $\oplus$ represents the operation of bitwise exclusive or. For every $a \in \mathbb{Z}_{256}$, $a \oplus a = 0$, so $E_k(E_k(x)) = E_k(x \oplus k) = x \oplus k \oplus k = x$. Thus E_k is its own inverse, and $E(K)$ is closed under inverses. So, this is a balanced cryptosystem. Moreover, $E_{k_2} \circ E_{k_2} = E_{k_2 \oplus k_1}$, so this is a closed cryptosystem, and $E(K)$ is a group of permutations.

For the next examples, keep in mind that arithmetic in the set $\mathbb{Z}_n$ is performed modulo n, so if $a, b \in \mathbb{Z}_n$, then $a + b$ and ab are reduced modulo n to land in $\mathbb{Z}_n$. Also, $-a$ equals $n - a$ and a^{-1} means the multiplicative inverse of a in $\mathbb{Z}_n$ (if it exists).

Recall that $\mathbb{Z}_n^*$ denotes the set of invertible elements in $\mathbb{Z}_n$. This set is closed under multiplication and inverses.

Example 2. We describe the `shif` cipher as a primal cryptosystem (A, K, E) in this way:

- the alphabet is $A = \{\texttt{'A'}, \texttt{'B'}, \ldots, \texttt{'Z'}\}$;
- the key space is $\mathbb{Z}_{26}$;
- the encryption functions are $E_k = f^{-1} \circ \alpha_k \circ f$, where $f : A \to \mathbb{Z}_{26}$ is given by $f : x \mapsto x - \texttt{'A'}$ is bijective, and $\beta_k : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ is given by $\beta_k : x \mapsto x + k$ (arithmetic in $\mathbb{Z}_{26}$ is performed modulo 26).

Then $E(K)$ is closed under inverses, since $\beta_k^{-1} = \beta_{-k}$. Moreover, $E(K)$ is a group, because $\beta_{k_1} \circ \beta_{k_2} = \beta_{k_1 + k_2}$ (the addition $k_1 + k_2$, being performed in $\mathbb{Z}_{26}$, is modulo 26).

Example 3. We describe the `affine` cipher as a primal cryptosystem (A, K, E) in this way:

- the alphabet is $A = \{\texttt{'A'}, \texttt{'B'}, \ldots, \texttt{'Z'}\}$;
- the key space is $\mathbb{Z}_{26}^* \times \mathbb{Z}_{26}$;
- the encryption functions are $E_k = f^{-1} \circ \beta_k \circ f$, where $f : A \to \mathbb{Z}_{26}$ is given by $f : x \mapsto x - \texttt{'A'}$ is bijective, and $\alpha_k : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ is given by $\alpha_{(a,b)} : x \mapsto ax + b$.

Then $E(K)$ is closed under inverses, since $E_{(a,b)}^{-1} = E_{(a^{-1}, a^{-1}b)}$. Moreover, $E(K)$ is a group, because $E_{(c,d)} \circ E_{(a,b)} = E_{(ac, bc+d)}$.

Let us generalize our last two examples:

Definition 8. A *shift cryptosystem* on an alphabet A is a primal cryptosystem (A, K, E), with $|A| = n$, together with a bijective function

$$f : A \to \mathbb{Z}_n,$$

satisfying

- $K = \mathbb{Z}_n$;
- $\beta_k : \mathbb{Z}_n \to \mathbb{Z}_n$ is given by $\beta_k : x \to x + k$;
- $E_k : A \to A$ is given by $E_k = f^{-1} \circ \beta_k \circ f$.

Let $\mathrm{Shf}(A) = E(K)$; then $\mathrm{Shf}(A)$ is a subgroup of $\mathrm{Sym}(A)$, which we may call the *group of shift ciphers on* A.

Definition 9. An *affine cryptosystem* on an alphabet A is a primal cryptosystem (A, K, E), with $|A| = n$, together with a bijective function

$$f : A \to \mathbb{Z}_n,$$

satisfying

- $K = \mathbb{Z}_n^* \times \mathbb{Z}_n$;
- $\beta_k : \mathbb{Z}_n \to \mathbb{Z}_n$ is given by $\beta_{(a,b)} : x \to ax + b$;
- $E_k : A \to A$ is given by $E_k = f^{-1} \circ \beta_k \circ f$.

Let $\mathrm{Aff}(A) = E(K)$; then $\mathrm{Aff}(A)$ is a subgroup of $\mathrm{Sym}(A)$, which we may call the *group of affine ciphers on* A. Note that $\mathrm{Shf}(A)$ is a subgroup of $\mathrm{Aff}(A)$.

We see that the level of security tends to increase as the size of $E(K)$ increases, and there is nothing preventing us from considering the case where $E(K) = \mathrm{Sym}(A)$.

Definition 10. A *substitution cryptosystem* on an alphabet A is a primal cryptosystem (A, K, E), where $K = \mathrm{Sym}(A)$ and E is the identity function.

The logistical problem with a substitution cryptosystem is finding a concise way to describe a permutation of A.

8. String Cryptosystems

Definition 11. Let (A, K, E) be a primal cryptosystem. The *stream cryptosystem* induced by (A, K, E) is the cryptosystem $(A^\omega, K, \widehat{E})$ whose encryption map

$$\widehat{E} : K \to \mathrm{Sym}(A^\omega) \quad \text{is given by} \quad \widehat{E}_k(\widehat{a}) = E_k \circ \widehat{a}.$$

This is a theoretical description of how we use a primal cryptosystem to encrypt strings of letters from an alphabet. The significant point here is that a single permutation for a given key acts on each letter independently, preserving the relative order of the input and output.

We can make the cryptosystem more secure by altering the key as we proceed through the string. This is the idea behind the vigenere cipher,

Definition 12. Let (A, K, E) be a primal cryptosystem. The *string cryptosystem* induced by (A, K, E) is the cryptosystem $(A^\omega, K^\omega, E^\omega)$ whose encryption map

$$E^\omega : K^\omega \to \mathrm{Sym}(A^\omega) \quad \text{is given by} \quad E^\omega_{\widehat{k}}(\widehat{p}) = \widehat{q},$$

where

$$q_i = E_{k(\bar{i})}(p_i) \text{ with } n = \mathrm{len}(\widehat{k}) \text{ and } \bar{i} = i \pmod{n}.$$

Example 4. We may view the `xor` cipher which we implemented in code as the string cryptosystem $(A^\omega, K^\omega, E^\omega)$ induced by the partial `xor` cryptosystem (A, K, E) described in Example 1.

Example 5. We may view the traditional vigenere cipher, as described by Trappe and Washington, as the string cryptosystem $(A^\omega, K^\omega, E^\omega)$ induced by the `shif` cryptosystem (A, K, E) described in Example 2.

9. Block Cryptosystems

Definition 13. A *block cryptosystem* (B, K, E) consists of

- an alphabet A;
- a key space K
- a positive integer m, the *block size*;
- $B = A^n$;
- $E : K \to \mathrm{Sym}(B)$

A block cryptosystem acts on fixed length blocks from the alphabet A. Unlike the primal and string cryptosystems, the key does not establish a bijective correspondence between input characters and output characters; it mixes the input bits across characters in the block.

The Hill cipher is a block cipher which uses invertible matrices for encryption. We need some facts about matrices.

A *square matrix over* $\mathbb{Z}_n$ *of dimension* m is an $m \times m$ array of entries from $\mathbb{Z}_n$, These are added and multiplied just like matrices over $\mathbb{R}$, except all arithmetic on the entries is performed modulo n.

We view a square matrix A over $\mathbb{Z}_n$ of dimension m as a function $A : \mathbb{Z}_n^m \to \mathbb{Z}_n^m$, defined on the set of strings of length m over $\mathbb{Z}_n$. If $\vec{v} \in \mathbb{Z}_n^m$, view $\vec{v}$ as a column; then $A(\vec{v})$ is the matrix product $A\vec{v}$.

Determinants are computed as with matrices over $\mathbb{R}$, except that the determinant is computed modulo n, so that the determinant is an element of $\mathbb{Z}_n$.

Such a matrix A is *invertible* if there exists another such matrix B such that $AB = I$, where I is the identity $m \times m$ matrix. A matrix is invertible if and only if the function induced by the matrix is an invertible function. The set of all invertible $m \times m$ matrices with entries from $\mathbb{Z}_n$ is denoted $\mathbf{GL}_m(\mathbb{Z}_n)$; we call this the *general linear group*. Then $\mathbf{GL}_m(\mathbb{Z}_n)$ is a subgroup of $\mathrm{Sym}(\mathbb{Z}_n^m)$. Cramer's rule implies the following result.

Fact 1. Let A be an $m \times m$ matrix over $\mathbb{Z}_n$. Then A is invertible if and only if $\det(A)$ is invertible in $\mathbb{Z}_n$.

Example 6. The *Hill cipher* of dimension n is a block cryptosystem (B, K, E) where

- $A = \{\texttt{'A'}, \ldots, \texttt{'Z'}\}$, for simplicity viewed as the numbers $\{0, \ldots, 25\}$;
- $B = A^m$;
- $K = \mathbf{GL}_n(\mathbb{Z}_{26})$;
- E_k is a matrix, and encryption is performed by matrix multiplication on tuples of numbers corresponding to blocks of letters.

We implement this in practice as a stream cipher; the input needs to have length divisible by the block length, so pad with `A`'s.

For example, let $m = 2$ and let $E_k = A = \begin{bmatrix} 11 & 5 \\ 6 & 7 \end{bmatrix}$. If the plaintext is `PLAIN`, pad to get `PLAINA`, viewed as the string of numbers $(15, 11, 0, 8, 13, 0)$. We break this up into blocks of length two, view each block as a column vector, and multiply by the matrix A:

$$\begin{bmatrix} 11 & 5 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} 15 \\ 11 \end{bmatrix} = \begin{bmatrix} 12 \\ 11 \end{bmatrix}, \quad \begin{bmatrix} 11 & 5 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 8 \end{bmatrix} = \begin{bmatrix} 14 \\ 4 \end{bmatrix}, \quad \begin{bmatrix} 11 & 5 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} 13 \\ 0 \end{bmatrix} = \begin{bmatrix} 13 \\ 0 \end{bmatrix};$$

thus the ciphertext is $(12, 11, 14, 4, 13, 0)$ = `MLOENA`. We note that each pair of characters `ML`, `OE`, and `NA` in the ciphertext depend on both of the characters in the corresponding pairs `PL`, `AI`, and `NA` of plaintext.

10. Feistel Systems

Definition 14. A *Feistel system* is a block cryptosystem (B, K, E) such that

- the alphabet is $A = \{0, 1\}$, that is, bits;
- n is a positive integer, the *semiblock size*;
- $B = A^{2n}$, or more accurately, $B = A^n \times A^n$; that is, blocks of $2n$ bits which are viewed as pairs (L, R) of the left and right constituent members from A^n;
- K is the key space, probably $\mathbb{Z}_m$ for some m;
- r is a positive integer, the *number of rounds*;
- K' is a set, the *round key space*;
- $\kappa_k : \{0, \ldots, r-1\} \to K'$ produces $k_i = \kappa_k(i)$ from the pair (k, i) (with $k \in K$); we call k_i the i^{th} *round key*;
- $f : K' \to \mathrm{Sym}(A^n)$, so that $f_{k_i} \in \mathrm{Sym}(A^n)$;
- $E_k \in \mathrm{Sym}(B)$ is produced in r rounds, splitting the left and right constituents of a block and modifying them as given (for $k \in K$) by the algorithm

  `for` $i \in \{0, \ldots, r-1\}$ `set` $(L_{i+1}, R_{i+1}) = (R_i, L_i \oplus f_{k_i}(R_i))$
  `set` $(L_r, R_r) = (R_{r-1}, L_{r-1})$.

Note that if $(L_{i+1}, R_{i+1}) = (R_i, L_i \oplus f_{k_i}(R_i))$, then

$$(L_i, R_i) = (R_{i+1} \oplus f_{k_i}(R_{i+1}), L_{i+1}).$$

Because of this, and the last step of the algorithm which switches the two semiblocks, decryption is given by encryption except with reversed round key sequence.

Department of Mathematics and CSci, Southern Arkansas University
E-mail address: plbailey@saumag.edu