LATIN SQUARES GENERATED BY SINGLE - CYCLE BIJECTION

AND

METHODS FOR CRYPTOGRAPHY

INTRODUCTION

What is a Latin quare?

We make a brief reminder about the mathematical objects called Latin squares.

Let E be a set of n elements . A Latin square defined on E is a table with n columns and n rows in which each element belonging to E appears only one time in each column and one time in each row. For example if E = {1 , 2 , 3 , 4} , for which n = 4 , a Latin square defined on E can be :

4	**3**	**1**	**2**
2	**1**	**4**	**3**
3	**4**	**2**	**1**
1	**2**	**3**	**4**

Each column and each row of the Latin square is therefore a permutation of the elements of E. The integer n is called the order (in the sense of the « size ») of the Latin square. Here this Latin square is order 4.

The purpose of our work is to show how to construct a Latin square for any set E of cardinal n using a single-cycle bijection. In particular we will show that this method enables to easily construct Latin squares defined on sets of type $\{0,1\}^n$. For example if E = $\{0,1\}^3$, which is the set of bit triplets, one can check that the array below is a Latin square whose elements are the bit triplets.

101	011	110	000	111	100	001	010
011	010	111	001	100	000	101	110
010	110	100	101	000	001	011	111
110	111	000	011	001	101	010	100
111	100	001	010	101	011	110	000
100	000	101	110	011	010	111	001
000	001	011	111	010	110	100	101
001	101	010	100	110	111	000	011

The set $\{0,1\}^3$ = { 000 ,010 , 111 , 110 , 001 , 101 , 100 , 011 } is the set of eight triplets of bits. This array is a Latin square, each triplet of bits belonging to $\{0,1\}^3$ appears only once in each row and in each column.

The description of the mathematical tools and methods that enable the construction of Latin squares from a single-cycle bijection, as well as the study of this last notion, will be seen in part I.

Secondly, and this is the essential object of our study, we will show how to use in symmetric cryptography these objects that are the Latin squares and the single-cycle bijections to design disposable key generators (Part II and III). We will also see how to use these disposable key generators for authentication protocols (Part IV). The domain of use of these cryptographic techniques can be, according to us, the military or diplomatic domain. We will also see in a supplement that they can be used in block cipher modes.

PART I – Reminders : cyclic subgroups of symmetric groups, cycle of a bijection , single-cycle bijection.

The results stated in this part are established and therefore no proof of them will be given, with some exceptions.

§ 1 – Symmetric Group of a set E

Let E be any finite set of elements. Let $\circ$ be the operation of function composition . In mathematics, the set of all bijections (one-to-one mappings) from E to E is called the symmetric group of E . It is an algebraic group structure that we denote (Se , $\circ$) . The symmetric group of E , denoted Se , is also the set of all permutations of the elements of E if E is an ordered set . For example , if E = {1,2,3} with the natural order of integers one permutation *p* of the elements of E can be (3 1 2) , which will then be defined by the following bijection :

$1 \rightarrow 3$
$2 \rightarrow 1$
$3 \rightarrow 2$

or, using the bijection symbol *p* (we use symbol *p* as it refers to the first letter of ‘’permutation’’):

$p(1) = 3$
$p(2) = 1$
$p(3) = 2$

If the order relation over E is $2 < 3 < 1$, and no longer $1 < 2 < 3$, then the bijection from E to E defining the permutation (3 1 2) would be :

$p(2) = 3$
$p(3) = 1$
$p(1) = 2.$

§ 2 – Cycle of a permutation of E

Let *p* be a permutation (bijection) belonging to the symmetric group Se of a set E . We call cycle of *p* , for one element i from E , the sequence (i , e_1 , e_2 , ….., $p^{h-1}(i)$) , such that :

$p^1(i) = e_1$, $p^2(i) = e_2$, ….., $p^h(i) = i$, in which :

- p^n is the bijection $p \circ p \circ ....\circ p$, where the operation $\circ$ (function composition) being iterated n-1 times,
- h is the smallest integer number such as $p^h (i) = i$,

Example

Let *p* be the permutation of the set { 1,2,3,4,5,6,7,8,9} defined and written as follows (the order relation on this set is the natural order of integers) :

$$p = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 6 & 9 & 1 & 4 & 3 & 5 & 2 & 8 \end{matrix}$$

(when the permutation is given in this way with the rank numbers written above its elements it is generally said that it is given in matrix form) .

Now, the permutation of the elements of { 1,2,3,4,5,6,7,8,9} written above in matrix form , obviously denoted also *p,* can also be written as a bijection , defined by :

$p(1) = 7$
$p(2) = 6$
$p(3) = 9$
$p(4) = 1$
$p(5) = 4$
$p(6) = 3$
$p(7) = 5$
$p(8) = 2$
$p(9) = 8$

That means : "7 is first element of the permutation (i.e. of the sequence) " , "6 is the second element" , 9 is the third element" , etc .

So, we can obtain a cycle of *p* by noting that :

$p(1) = \mathbf{7}$,
$p^{\mathbf{2}}(1) = \mathbf{5}$,
$p^{\mathbf{3}}(1) = \mathbf{4}$,
$p^{\mathbf{4}}(1) = \mathbf{1}$

since :

$p(1) = \mathbf{7}$,
$p^{\mathbf{2}}(1) = p \circ p = p(p(1)) = p(7) = \mathbf{5}$,
$p^{\mathbf{3}}(1) = p \circ p \circ p = p(p^{\mathbf{2}}(1)) = p(5) = \mathbf{4}$,
$p^{\mathbf{4}}(1) = p \circ p \circ p = p(p^{\mathbf{3}}(1)) = p(4) = \mathbf{1}$.

Then , if we choose 1 as first element of the cycle , *p* has a first cycle which is $\mathbf{C}_{p1} = \mathbf{(1\ 7\ 5\ 4)}$.

For i = 2 we have a second cycle : $\mathbf{C}_{p2} = \mathbf{(2\ 6\ 3\ 9\ 8)}$, since $p(2) = 6$, $p^2(2) = 3$, $p^{\mathbf{3}}(2) = 9$, $p^{\mathbf{4}}(2) = 8$, $p^{\mathbf{5}}(2) = 2$.

All elements of E are in $\mathbf{C}_{p1}$ or $\mathbf{C}_{p2}$, thus *p* has two cycles that are :

$\mathbf{C}_{p1} = \mathbf{(1\ 7\ 5\ 4)}$
$\mathbf{C}_{p2} = \mathbf{(2\ 6\ 3\ 9\ 8)}$

What we have also to note is that a cycle of a permutation can be written with "exponents" as

below, since $(p \circ p)$ can be written p^2 , $(p \circ p \circ p)$ can be written p^3 etc , so :

$\mathbf{C}_{p1}$ is : $p^0(1) = \mathbf{1}$, $p^1(1) = \mathbf{7}$, $p^2(1) = 5$, $p^3(1) = 4$, $p^4(1) = 1$
$\mathbf{C}_{p2}$ is: $p^0(2) = 2$, $p^1(2) = 6$, $p^2(2) = 3$, $p^3(2) = 9$, $p^4(2) = 8$, $p^5(2) = 2$

$\mathbf{C}_{p1}$ and $\mathbf{C}_{p2}$ above are the two cycles of p written with exponents .

The length of a cycle is the number of elements which are in the cycle ($\mathbf{C}_{p1}$ is length 4 and $\mathbf{C}_{p2}$ is length 5). For a cycle with exponents the length of the cycle is always the integer h (such that $p^h(i) = i$) . And for any integer n we have $p^n(i) = p^r(i)$ with r = n mod h , which is obvious by definition of a cycle. For example in cycle $\mathbf{C}_{p1}$ above we can check that $p^6(1) = p^2(1)$, since $2 = 6$ mod 4 .

The first element of a cycle , here denoted i , is written at the end of the cycle but also at the beginning of the cycle as we can see in the two cycles $\mathbf{C}_{p1}$ and $\mathbf{C}_{p2}$ above . At the end of the cycle we write $p^h(i) = i$, and at the beginning $p^0(i) = i$, by convention (since h = 0modh) . This is done to make more easy the function composition calculations which will be studied §5 below .

The cycles of a permutation will most often be presented subsequently by cycles with exponents and written in columns in the following way :

$\mathbf{C}_{p1}$ =	$\mathbf{C}_{p2}$ =
$p^0(1) = 1$	$p^0(2) = 2$
$p^1(1) = 7$	$p^1(2) = 6$
$p^2(1) = 5$	$p^2(2) = 3$
$p^3(1) = 4$	$p^3(2) = 9$
$p^4(1) = 1$	$p^4(2) = 8$
	$p^5(2) = 2$

Supplements

A simple and quick and ‘’visual’’ method to build the cycles of a permutation is to write the permutation with the rank numbers above the elements of the sequence in form of a matrix:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 6 & 9 & 1 & 4 & 3 & 5 & 2 & 8 \end{pmatrix}$$

Then , we simply read , or watch , in the matrix: below rank number (or column number) 1 is 7 , thus $p(1) = 7$; next watch what is below rank 7 : below rank number 7 is 5 , thus $p^2(1) = 5$; next watch what is below rank 5 : below rank number 5 is 4 , thus $p^3(1) = 4$, next watch what is below rank number 4: below rank number 4 is 1 , thus $p^4(1) = 1$ and the first cycle is closed . In this way the cycles of the bijection (permutation) are built.

Finally, it can be noted that the first element of a given cycle can be any element of that cycle. Thus, the cycle $\mathbf{C}_{p2}$ = (2 6 3 9 8) can for example be written (3 9 8 2 6) where the base element (the first element) is 3 and no longer 2 . This result is obvious.

Therefore,with exponents the following cycle :

$\mathbf{C}_{p2}$ =
$p^0(2) = 2$
$p^1(2) = 6$
$p^2(2) = 3$
$p^3(2) = 9$
$p^4(2) = 8$
$p^5(2) = 2$

would be , with 3 as first element :

$p^0(3) = 3$
$p^1(3) = 9$
$p^2(3) = 8$
$p^3(3) = 2$
$p^4(3) = 6$
$p^5(3) = 3$

One way of representing the cycles of a bijection that is sometimes useful is to put them in "arrowed" form. Indeed, we can write the two cycles $\mathbf{C}_{p1}$ and $\mathbf{C}_{p2}$ above in this way:

$\mathbf{C}_{p1}$ **= 1→ 7 →5 →4**
$\mathbf{C}_{p2}$ **= 2 →6 →3 →9 →8**,

This means intuitively, for example for $\mathbf{C}_{p1}$ **,** that $p(1)= 7$, $p(7) = 5$ $p(5) = 4$, or equivalently with exponents of p that $p^1(1) = 7$, $p^2(1) = 5$, $p^3(1) = 4$.

As a last point , we mention that in the following, for simplicity, permutations of elements of a set will often be written as a sequence of symbols in parentheses such (7 6 9 1 4 3 5 2 8) for example , in place of the matrix notation :

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 6 & 9 & 1 & 4 & 3 & 5 & 2 & 8 \end{pmatrix}$$

But in order not to confuse them with cycles that can be also written in this form of symbols in parentheses we will write the name of the bijection (that is, the letter by which the bijection is denoted) at the beginning of the sequence, as follows : p = (7 6 9 1 4 3 5 2 8),while for cycles these will be written in general with the symbol C as follows:

$\mathbf{C}_{p1} = (1\ 7\ 5\ 4)$

$\mathbf{C}_{p2} = (2\ 6\ 3\ 9)$

But in the following the cycles of bijections will most often be written in the form of exponents of the bijection p.

§ 3 – Cyclic subgroups of permutations.

What is cyclic subgroup of symmetric groups ?

Let E be a set of elements . S_e is the symmetric group of E. A cyclic subgroup of Se , called **G** , generated by a permutation p belonging to Se, is the set of permutations (bijections) defined by :

$\{ p , p^2 , \ldots p^j,\ldots,p^{\mathbf{a}} \}$, such as $p^1 = p$, $p^2 = p \circ p$, $p^3 = p \circ p \circ p$, etc .

The integer denoted **a** is the Last Common Multiple (LCM) of the integers representing the lengths of the cycles of p. If cycles C_1 , C_2 , … , C_k of p have length h_1 , h_2 , ...h_k , then p generates a cyclic subgroup **G** of S_e which is $\mathbf{G} = \{ p , p^2 , \ldots p^j,\ldots,p^{\mathbf{a}} \}$, in which **a** = LCM (h_1 , h_2 , ...h_k).

(So, note that in the following we call the set **G** "cyclic subgroup" of S_e whereas this is not entirely correct, since this term refers rather to the algebraic structure (**G**, $\circ$)).

The function composition operation $\circ$ is used to construct the subset **G** of E from a given permutation of E, it is also the internal composition law of the algebraic structure (**G**, $\circ$).

Properties of the set **G**

In **G** we obviously have for each integer j and h : $p^j \circ p^h = p^h \circ p^j = p^{j+h}$.

For example, $(p \circ p) \circ (p \circ p \circ p) = p^2 \circ p^3$, and $(p \circ p) \circ (p \circ p \circ p) = (p \circ p \circ p \circ p \circ p) = p^5$. This is due to the characteristics of the function composition applied to the same function. This means that the structure (**G**, $\circ$) is a commutative group.

The integer **a** is also the smallest integer such as the function $p^{\mathbf{a}}$ is identity bijection (i.e. $p^{\mathbf{a}}(i) = i$, for each i) .The integer **a** is also the cardinality of **G** : **a** is the number of permutations that the set **G** contains.

This subgroup **G** is cyclic modulo **a** and commutative. It is cyclical modulo **a** in the sense that $p^{a+1} = p^1$, $p^{a+2} = p^2$, ..etc . If x > **a** , then $p^x = p^r$ with r = remainder (x/a) , what means $p^x = p^r$ with r = x mod **a** .

To summarize, the cyclic subgroup $\{p^1,p^2,\ldots p^j,\ldots , p^a\}$ of the symmetric group S_e of a set E generated by a bijection (permutation) p belonging to S_e is simply the set $\{ p^1 = p , p^2 = p \circ p , p^3 = p \circ p \circ p ,\ldots , p^j = p \circ p \circ \ldots\ldots \circ p$ (the operation $\circ$ applied j - 1 time)..... , $p^{\mathbf{a}} = p \circ p \circ \ldots\ldots \circ p$ (the operation $\circ$ applied **a** – 1 time) } , with **a** defined as above. More exactly it is the algebraic structure ($\{p^1,p^2,\ldots p^j,\ldots , p^a\}$, $\circ$) where $\circ$ is the operation of function composition.

The group defined by the algebraic structure (**G** , $\circ$) is commutative. Indeed, the symmetric group (S_e , $\circ$) for a finite set E is a group. **G** is a subset of S_e. As we've seen above for two elements p^j and p^h belonging to **G** we have $p^j \circ p^h = p^h \circ p^j$, so the algebraic structure (**G** , $\circ$) is a commutative group. Now we give some examples of cyclic subgroups of symmetric groups and at the same time examples of constructions of such structures.

These examples can make more clear what we have said about cyclic sub-groups of symmetric groups above.

Example 1

Let p be a permutation of the set E = {1,2,3,4,5,6,7 } , defined and written as follows (the order relation on E is the natural order of integers) :

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 2 & 6 & 1 & 4 \end{pmatrix}$$

p has two cycles (this can be checked) , which are :

$\mathbf{C}_{p1}$ = (1 3 5 6) , length = 4
$\mathbf{C}_{p2}$ = (2 7 4) , length = 3

The base elements (first elements) of these two cycles are 1 and 2 . They correspond to columns 1 and 2 of the table below which represents **G .**The LCM of the two integers representing the lengths of this two cycles is : LCM(4,3) = 12.Therefore , the cyclic subgroup **G** of S_e , generated by p , is made up with twelve permutations of the set E as we can see below . If we represent **G** by an array it can be checked that :

G =

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 5 & 2 & 6 & 1 & 4 \end{pmatrix}$$

$p^2 = (5\ 4\ 6\ 7\ 1\ 3\ 2\ ) = p \circ p = p^2$
$p^3 = (6\ 2\ 1\ 4\ 3\ 5\ 7\ ) = p \circ p \circ p = p^3$, etc,
$p^4 = (1\ 7\ 3\ 2\ 5\ 6\ 4\ )$
$p^5 = (3\ 4\ 5\ 7\ 6\ 1\ 2\ )$
$p^6 = (5\ 2\ 6\ 4\ 1\ 3\ 7\ )$
$p^7 = (6\ 7\ 1\ 2\ 3\ 5\ 4\ )$
$p^8 = (1\ 4\ 3\ 7\ 5\ 6\ 2\ )$
$p^9 = (3\ 2\ 5\ 4\ 6\ 1\ 7\ )$
$p^{10} = (5\ 7\ 6\ 2\ 1\ 3\ 4\ )$
$p^{11} = (6\ 4\ 1\ 7\ 3\ 5\ 2\ )$
$p^{12} = (1\ 2\ 3\ 4\ 5\ 6\ 7\ )$

This table can be constructed very quickly by the so-called "visual" method described in §2 (see