Palestine Journal of Mathematics

Vol 14(2)(2025) , 194–203

Permutation Polynomials Over Fields of Characteristic 7: Implication for Cryptographic Algorithms

F. Aggoun Laid, A. Ait Mokhtar and O. Özer

Communicated by Ayman Badawi

MSC 2020 Classifications: Primary 33C20; Secondary 33C65.

Keywords and phrases: Permutation Polynomials, Finite Fields, Characteristic 7, symétric groupe, Cryptography.

We learned that the results in this paper are special cases of the paper by June Bok Lee and Young Ho Park, Some permuting trinomials over finite fields, Acta Mathematica Sinica vol. 17, no. 3, 1997, pp. 250--254 where much more general results were proved 28 years ago. This note added by the Editor in chief.

Corresponding Author: O. Özer

Abstract In this article we are interested in the class of permutation polynomials of the form:

$$H(x) = x^r f(x^{\frac{(q-1)}{d}})$$

where d and r are positive integers and d divides $q-1$. We give necessary conditions and sufficient for this family of polynomials to be permutations in a finite field $\mathbb{F}_q$ of characteristics 7, based on the Lidl-Wan criterion. Then we will give an application in cryptography for this family of polynomials on $\mathbb{F}_q$.

1 Introduction

The study of permutation polynomials is a subject dating from the 19th century, it began by being initiated by Hermite in 1863 then by Dickson in 1896. It is a vast field which has experienced a wave of enthusiasm. In recent years there has been much interest in the study of permutation polynomials due to their applications in cryptography and coding theory [1, 5, 2, 3]. In general it is difficult to characterize permutation polynomials. In reality there are only a few classes of permutation polynomials that are known.
A polynomial $f \in \mathbb{F}[X]$ is of permutation of a finite field $\mathbb{F}_q = p^\alpha$, p prime, α positive integer, if it induces a bijection f of $\mathbb{F}_q$ in $\mathbb{F}_q$.

2 Preliminaries and results

In Mathematics, a permutation polynomial of a given ring A is a polynomial that acts as a permutation of the elements of that ring.

Definition 2.1. Let A be a ring and $f \in A[x]$ a polynomial. We say that f is a permutation polynomial of A if and only if the map :

$$\begin{array}{rcl} g : A & \longrightarrow & A \\ x & \longmapsto & g(x) = f(x) \end{array}$$

is bijective.

Example 2.2. In the case of a finite ring $\mathbb{Z}/n\mathbb{Z}$ we can give examples of permutation polynomials of $\mathbb{Z}/n\mathbb{Z}$ for $n = \prod_{i=0}^{k} p_i^{\alpha_i}$, p_i primes and α_i positive integers , $k \in \mathbb{N}^*$.

For $A = \mathbb{Z}/4\mathbb{Z}$, consider the permutation polynomial :

$$f(x) = 2x^2 + x$$

We have :

x	0	1	2	3
$f(x)$	0	3	2	1

and we can then associate to $f(x)$ the permutation $\sigma = g$ defined on $S_4 \simeq S(A)$ by :

$$\begin{array}{rcl} \sigma : A & \longrightarrow & A \\ x & \longmapsto & \sigma(x) = g(x) \end{array}$$

where :

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 3 & 2 & 1 \end{pmatrix} \in S_4$$

Same thing for $A = \mathbb{Z}/8\mathbb{Z}$ and for $A = \mathbb{Z}/12\mathbb{Z}$.
An example of a polynomial of $\mathbb{Z}[x]$ which is not a permutation of $\mathbb{Z}/4\mathbb{Z}$:
Let be $f(x) = x^2 + 1$. We have :

x	0	1	2	3
$f(x)$	1	2	1	2

f does not induce a permutation on the set of elements of $\mathbb{Z}/4\mathbb{Z}$ because σ is not injective, where

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 1 & 2 \end{pmatrix}$$

So f is not a permutation polynomial of $\mathbb{Z}/4\mathbb{Z}$.

Remark 2.3. When the ring $A = \mathbb{F}_q$ is a finite field, $q = p^\alpha$, p prime and α a positive integer then the definition of a permutation polynomial of $\mathbb{F}_q$ is the same as that given in the case of a ring A.
And any permutation of the elements of this field can be written as a polynomial function.

Proposition 2.4. *([6, 7]) The polynomial $f(x) = ax^i + bx^j + c, a \neq 0, i > j \geq 1$ such that $gcd(i-j, q-1) = 1$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $b = 0$ and $gcd(i, q-1) = 1$.*

Example 2.5. For $i = 8$ and $j = 3$, the polynomials $ax^8 + bx^3 + c$ are permutation polynomials of $\mathbb{F}_q$ if and only if $b = 0$ with $q = 7^\alpha$, α is a positif integer.

Definition 2.6. Let $q \in \mathbb{N}^*$, d be a positive integer dividing $q-1$, g be a fixed generator of the multiplicative group $\mathbb{F}_q^*$ of the finite field $\mathbb{F}_q$ and $\omega = g^{\frac{q-1}{d}}$ a primitive root d^{eme} of unity in $\mathbb{F}_q$.
We define the multiplicative character ψ by :

$$\begin{array}{rcl} \psi : \mathbb{F}^*{}_q & \longrightarrow & \mathbb{Z}/d\mathbb{Z} \\ a & \longmapsto & \psi(a) = Ind_g(a)(mod\ d) \end{array}$$

where $Ind_g(a)$ is the residual class of $b\ (mod\ (q-1))$ with $a = g^b$.

Remark 2.7.

$$a^{\frac{q-1}{d}} = g^{\frac{b(q-1)}{d}} = \omega^{\psi(a)}$$

With this definition, Da Qing Wan and Rudolf Lidl introduced the following criterion :

Proposition 2.8. *(LIDL-WAN criterion[8]) Let d and r be two positive integers such that d divides $q-1$, $f(x) \in \mathbb{F}_q[x]$ and ω the primitive d-root of unity on $\mathbb{F}_q$. So the polynomial*

$$H(x) = x^r f(x^{\frac{q-1}{d}})$$

is a permutation polynomial of $\mathbb{F}_q$ if and only if the following conditions are satisfied :

(i) $(r, \frac{q-1}{d}) = 1$;

(ii) For all $0 \leq i < d, f(\omega^i) \neq 0$;

(iii) For all $0 \leq i < j < d, \quad \psi(f(\omega^i)/f(\omega^j)) \not\equiv r(j-i)(mod\ d)$.

3 Main results

In this section, we will give our main results.

Proposition 3.1. *Let $q \in \mathbb{N}^*$. For all $(a,b) \in \mathbb{F}_q^* \times \mathbb{F}_q$ the polynomial of $\mathbb{F}_q[x]$, $f(x) = ax + b$, is a permutation polynomial of $\mathbb{F}_q$.*

Proof. $f(x) = ax + b$ induces a bijection :

$$\begin{array}{rcl} g : \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ x & \longmapsto & g(x) = f(x) \end{array}$$

The proof is clear. Indeed, g is injective of a finite field $\mathbb{F}_q$, therefore it is bijective. Then f is a permutation polynomial of $\mathbb{F}_q$. □

Remark 3.2. For $b = 0$, the polynomial $fx) = ax$ is a permutation polynomial of $\mathbb{F}_q$.

Proposition 3.3. *Let $f, g \in \mathbb{F}_q[x]$. Then fog is a permutation polynomial of $\mathbb{F}_q$ if and only if f and g are also permutation polynomials on $\mathbb{F}$.*

Proof. - Suppose that fog is a permutation polynomial of $\mathbb{F}_q$. Then fog is bijective.
On the one hand, we have:
fog bijective implies that g is injective of the finite field $\mathbb{F}_q$, so g is bijective of $\mathbb{F}_q$ and consequently $g \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$
On the other hand we have fog bijective implies f is surjective of the finite field $\mathbb{F}_q$, therefore f is bijective and consequently $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$.

- Suppose that $f, g \in \mathbb{F}_q[x]$ are permutation polynomials on $\mathbb{F}_q$. Then the applications associated respectively with f and g are bijective on $\mathbb{F}_q$ and consequently the application fog is bijective on $\mathbb{F}_q$ therefore $fog \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$.

Recall the following proposition where an incomplete proof is in [4] and [7]. Using the indications given in [4] and [7], we give a detailed proof. □

Proposition 3.4. *The polynomial ax^k, $a \neq 0$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $gcd(k, q-1) = 1$.*

Proof. - Suppose that $gcd(k, q-1) = 1$. Let

$$\begin{array}{rcl} g : \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ x & \longmapsto & g(x) = ax^k \end{array}$$

the map associated with the polynomial ax^k. We have : $g(0) = 0$
And for $(x, y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$, we have :

$$\begin{array}{rcl} g(x) = g(y) & \Longrightarrow & ax^k = ay^k \\ & \Longrightarrow & (\frac{x^k}{y^k}) = (\frac{x}{y})^k = 1 \end{array}$$

then the order of the element $\frac{x}{y}$ in the multiplicative cyclic group $\mathbb{F}_q^*$ divides k and it divides $(q-1)$ since $|\mathbb{F}_q^*| = q-1$, so the order $(\frac{x}{y})$ divides $gcd(q-1, k) = 1$ hence $|< \frac{x}{y} >| = 1$ and therefore $\frac{x}{y} = 1$, therefore $x = y$.
g is injective on finite $\mathbb{F}_q$ where g is bijective.

- Suppose that $gcd(k, q-1) = d \neq 1$. Then there exists $k' \in \mathbb{N}$ such that $k = dk'$ and d divides $q-1$. Let $\xi \in \mathbb{F}_q^*$ be an element of order d then :

$$\begin{array}{rcl} \xi^d = 1 & \Longrightarrow & (\xi^d)^{k'} = 1 \\ & \Longrightarrow & \xi^{dk'} = 1 \\ & \Longrightarrow & \xi^k = 1 \end{array}$$

thus $a\xi^k = a1^k = g(\xi) = a \neq 0$.
Therefore g is not surjective on finite $\mathbb{F}_q$ and therefore g is not bijective and consequently the polynomial f is not a permutation polynomial of $\mathbb{F}_q$. □

Remark 3.5. The polynomial $f(x) = ax^k + b, a \neq 0, k \in \mathbb{N}^*$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $gcd(k, q-1) = 1$

Theorem 3.6. *Let $\mathbb{F}_q$ be a finite field, $q = 7^\alpha$, α and u two integers positive such that $gcd(u, \frac{q-1}{3}) = 1$. Then the polynomials of the form*

$$H(x) = x^u(1 + x^{\frac{q-1}{3}} - x^{\frac{2(q-1)}{3}})$$

are permutation polynomials of $\mathbb{F}_q$ if and only if $q \equiv 1(mod\ 18)$ and $u \not\equiv 0(mod\ 3)$

Proof. Let $H(x) = x^u(1 + x^{\frac{q-1}{3}} - x^{\frac{2(q-1)}{3}})$ be a polynomial of permutation on F_7^α where $gcd(u, \frac{7^\alpha-1}{3}) = 1$ and ω a primitive root of 3^{th} of unit.
Taking $f(x) = -x^2 + x + 1 \in \mathbb{F}[x]$ then $H(x)$ is of the form $x^u f(x^{\frac{q-1}{3}})$, $q = 7^\alpha$.

Noticed : $\forall n \in \mathbb{N}$, $7^n - 1$ is divisible by 3.
According to the conditions of the L.W criterion we have :

(i) $gcd(u, \frac{7^\alpha-1}{3}) = 1$.

(ii) for all $0 \leq i < 3$, $f(\omega^i) \neq 0$.

(iii) for all $0 \leq i < j < 3$, $\quad \psi(f(\omega^i)/f(\omega^j)) \not\equiv u(j-i)(mod\ 3)$.

Let ω primitive root 3^{th} of unity.

- The first condition is checked by hypothesis.
- The second condition is verified because $H(x)$ is a permutation polynomial which admits the only root 0 and therefore $f(\omega^i) \neq 0, \forall i, 0 \leq i \leq 2$.
- For the third condition we have :

(i) $\frac{f(\omega^0)}{f(\omega^j)} = \frac{1}{-2\omega^{2j}}$.

We notice that $(-2)^6 \equiv 1(mod\ 7)$ so (-2) is of order 6 of $F_{7^\alpha}^*$.
Let g be a generator of $F_{7^\alpha}^*$. We have :

$$-2 = g^{\frac{(7^\alpha-1)k}{6}} \quad with \quad gcd(k, 6) = 1$$

$$and$$

$$\frac{f(\omega^0)}{f(\omega^j)} = g^b \quad with \quad b = \frac{-(4j+k)(q-1)}{6}$$

We want to show that 3 does not divide $b - u(j-i)$ *i.e.*, $d = 3$ does not divide

$$\frac{-(4j+k)(q-1)}{6} - u(j-i), \quad q = 7^\alpha$$

We have two cases to study :
First case : $i = 0, j = 1$

- 3 does not divide $b - u$ for$k = \pm 1$ implies that 3 does not divide u and 3 does not divide $u - \frac{q-1}{6}$, so 3 divides $\frac{q-1}{6}$,$q = 7^\alpha$
  Then there exists $k' \in \mathbb{F}$ such that $\frac{q-1}{6} = 3k'$ therefore $q \equiv 1(mod\ 18)$

- For $i = 0, j = 2$
  We have : $j - i = 2$ and 3 does not divide $b - 2u$ implies that 3 does not divide $\frac{(4j+k)(q-1)}{6} + 2u$, *i.e.*, 3 does not divide $\frac{(-1\pm1)(q-1)}{6} - u$ and we find the same result as above $q \equiv 1(mod\ 18)$.

Second case : $i = 1, j = 2$:
We have : $\frac{f(\omega^i)}{f(\omega^j)} = \frac{f(\omega^i)}{f(\omega^0)} \times \frac{f(\omega^0)}{f(\omega^j)} = g^b$

So for $i = 1$ and $j = 2$

$$g^b = \frac{f(\omega^1)}{f(\omega^0)} \times \frac{f(\omega^0)}{f(\omega^2)}$$
$$= \frac{f(\omega^0)}{f(\omega^2)} \times \frac{1}{f(\omega^0)/f(\omega^1)}$$

g is a generator of $\mathbb{F}_q^*$, $q = 7^\alpha$.

On the hand, we have : $\frac{f(\omega^0)}{f(\omega^1)} = \frac{1}{-2\omega^2}$ (1)

(-2) is of order 6 then $\exists k \in \mathbb{N}^*$ tel que $-2 = g^{\frac{(q-1)k}{6}}, gcd(k, 6) = 1$.

On the other hand, we have : $\frac{f(\omega^0)}{f(\omega^2)} = \frac{1}{-2(\omega^4)} = \frac{1}{-2\omega}$ (2)

(-2) is of order 6 then $\exists k' \in \mathbb{N}^*$ tel que $(-2) = g^{\frac{(q-1)k'}{6}}, gcd(k', 6) = 1$.

So by replacing ω by $g^{\frac{q-1}{3}}$ in (1) and (2) (ω is the primitive root 3^{eme} of the unit).
We obtain :

$$g^b = g^{\frac{(k-k^{'})(q-1)}{6} - \frac{q-1}{6}}$$

thus $$b = \frac{(k-k^{'})(q-1)}{6} - \frac{q-1}{6}.$$

For $j-i = 1$, 3 does not divide $b-(j-i)u$ is equivalent to 3 does not divide $b-u$ therefore equivalent to 3 does not divide not $(\frac{(k-k^{'})(q-1)}{6} - \frac{q-1}{6}) - u$ so 3 does not divide $(\frac{(k-k^{'}-1)(q-1)}{6}) - u$.
By setting $t = k - k^{'} - 1$ for $k = \pm 1$ and $k^{'} = \pm 1$ so 3 does not divide $u - \frac{t(q-1)}{6}$ with $t = +1, -1, -3(mod\ 3)$.
Therefore, $u \not\equiv \frac{(q-1)}{6}(mod\ 3)$, where $\frac{(q-1)}{6} = 0, 1, 2(mod\ 3)$
$(*)$ For $\frac{(q-1)}{6} = 3k, k \in N, q \equiv 1(mod\ 18), u \not\equiv 0(mod\ 3)$
$(**)$ For $\frac{(q-1)}{6} = 3k + 1 \Rightarrow q \equiv 7(mod\ 18), u \not\equiv t(mod\ 3)$
$(***)$ For $\frac{(q-1)}{6} = 3k + 2 \Rightarrow q \equiv 13(mod\ 18), u \not\equiv t(mod\ 3)$
The cases $(**)$ and $(***)$ do not admit solutions, so the only remaining case is $(*)$.
Conversely, suppose that $q \equiv 1(mod\ 18), u \not\equiv 0(mod\ 3)$, and check the conditions of the L.W. criterion.

- The first condition is verified by the hypothesis.

- $f(\omega^0) = f(1) = 1$ therefore $f(\omega^0) \neq 0$
- $f(\omega^1) = 1 + \omega - \omega^2 = -2\omega^2$, so $f(\omega) \neq 0$.
- $f(\omega^2) = -2\omega$, so $f(\omega^2) \neq 0$.

- By taking the different values of i, j, $0 \leq i < j < 3$, we obtain with the conditions $(q-1) \equiv 0(mod\ 18)$ and $u \not\equiv 0(mod\ 3)$ that $\psi(\frac{f(\omega^i)}{f(\omega^j)}) \not\equiv (j-i)(mod\ 3)$.

Indeed, according to the calculations carried out previously for $i = 0$ and $j = 1$:

$$b - u(j-1) = \frac{-(4+k)(q-1)}{6} - u(1-0) = \frac{-(4+k)(q-1)}{6} - u$$

hence , $q - 1 \equiv 0(mod\ 18) \Longrightarrow \exists k_0 \in \mathbb{N}^* \ / \ q - 1 = 18k_0$.

So, $b = \frac{-(4+k)18k'}{6} \equiv 0(mod\ 3)$

thus $b-u \not\equiv 0(mod\ 3$ because $u \not\equiv 0(mod\ 3)$ by hypothesis, consequently $b \not\equiv u(1-0)(mod\ 3)$.
- Same thing for the case $i = 0$ and $j = 2$.
- For $i = 1$ and $j = 2$:

According to the calculations carried out in the first implication we have :

$$b = \frac{(q-1)(k-k')}{6} - \frac{q-1}{6}$$

Like $q - 1 \equiv 0(mod\ 18)$ $\exists k_1 \in \mathbb{N}^*$ such that $q - 1 = 18k_1$.
So

$$b = \frac{18(k-k')k_1}{6} - \frac{18k_1}{6}$$
$$= 3((k-k')k_1 - k_1)$$

Consequently

$$b \equiv 0(mod\ 3)$$
$$u \not\equiv 0(mod\ 3) \Longrightarrow b - u \not\equiv 0(mod\ 3)$$

Thus $b \not\equiv (j-i)(mod\ 3)$ for $j = 2$ and $i = 1$ □

Corollary 3.7. *Let $q = 7^{3n}$ and u be two positive integers such that $gcd(u, \frac{q-1}{3}) = 1$ and $u \not\equiv 0(mod\ 3)$. Then the polynomials*

$$H(x) = x^u(1 + x^{\frac{7^{3n}-1}{3}} - x^{\frac{2(7^{3n}-1)}{3}})$$

are permutation polynomials of $F_{7^{3n}}$.

Proof. It suffices to verify the two conditions of Theorem 3.6.

- $u \not\equiv 0(mod\ 3)$ by hypothesis;
- We easily show by induction that ($7^n - 1) \equiv 0(mod\ 18)$

□

Corollary 3.8. *Let $\mathbb{F}_q$ be a finite field, $q = 7^\alpha$ and p prime, α and k positive integers such that $gcd(u, \frac{q-1}{3}) = 1$ and $gcd(k, q-1) = 1$, then the polynomials*

$$F(x) = x^{u'}(1 + x^{\frac{q-1}{3}} - x^{\frac{2(q-1)}{3}})^k$$

with $u' = ku$ are permutation polynomials of $\mathbb{F}_q$ if and only if $u \not\equiv 0(mod\ 3)$ and $q \equiv 1(mod\ 18)$.

Proof. It is enough to use proposition 3.3 by taking :

$g(x) = H(x) = x^u(1 + x^{\frac{q-1}{3}} - x^{\frac{2(q-1)}{3}})$ and $f(x) = x^k$ with $F(x) = (fog)(x)$ □

Corollary 3.9. *Let $q = 7^{3n}$, where u,n and k are positive integers such that $gcd(k, 18) = 1$, $gcd(u, \frac{q-1}{3}) = 1$ and $u \not\equiv 0(mod\ 3)$. So the polynomials*

$$G(x) = x^{ku}(1 + x^{\frac{7^{3n}-1}{3}} - x^{\frac{2(7^{3n}-1)}{3}})^k$$

are permutation polynomials on $F_{7^{3n}}$.

Proof. This corollary is only a consequence of Corollary 3.8.
For $gcd(u, \frac{q-1}{3}) = 1$ with $q = 7^{3n}$ and setting

$$g(x) = H(x) = x^u(1 + x^{\frac{q-1}{3}} - x^{\frac{2(q-1)}{3}})$$
$$f(x) = x^k$$

then the polynomials $G(x) = (fog)(x) = x^{ku}(1 + x^{\frac{7^{3n}-1}{3}} - x^{2(\frac{7^{3n}-1}{3})})^k$ are permutation polynomials of $\mathbb{F}_7^{3n}$ if and only if $u \not\equiv 0(mod\ 3)$ and we have :
$7^{3n} \equiv 1(mod\ 18)$ if and only if $gcd(k, 18) = 1$ because $gcd((7^{3n} - 1, k) = 1$. □

Example 3.10. By taking in corollary 3.7,

$$P_u(x) = x^u(1 + x^{\frac{7^{3n}-1}{3}} - x^{2(\frac{7^{3n}-1}{3})})$$

with $u \not\equiv 0(mod\ 3)$.
The following polynomials are permutation polynomials of $\mathbb{F}_{7^{3n}}$.
For $n = 1$, $\frac{7^3-1}{3} = 114$, $q - 1 = 241 = 18 \times 19$
$P_u(x) = x^u(1 + x^{114} - x^{228})$are permutation polynomials of $\mathbb{F}_{7^3} = \mathbb{F}_{343}$.

- $P_1(x) = x(1 + x^{114} - x^{228})$ $gcd(114, 1) = 1$
- $P_5(x) = x^5(1 + x^{114} - x^{228})$ $gcd(114, 5) = 1$
- $P_7(x) = x^7(1 + x^{114} - x^{228})$ $gcd(114, 7) = 1$
- $P_{11}(x) = x^{11}(1 + x^{114} - x^{228})$ $gcd(114, 11) = 1$
- $P_{13}(x) = x^{13}(1 + x^{114} - x^{228})$ $gcd(114, 13) = 1$
- $P_{17}(x) = x^{17}(1 + x^{114} - x^{228})$ $gcd(114, 17) = 1$
- $P_{23}(x) = x^{23}(1 + x^{114} - x^{228})$ $gcd(114, 23) = 1$

$P_1,\ P_5,\ P_7,\ P_{11},\ P_{13},\ P_{17},\ P_{23}$ are permutation polynomials of F_{343}.

For $n = 2$, $\frac{7^6-1}{3} = 39216$, $q - 1 = 18 \times 6536$, $gcd(u, 39216) = 1\ \forall n \in \mathbb{N}^*$.
The polynomials $Q_u(x) = x^u(1 + x^{39216} - x^{78423})$ are permutation polynomials of $\mathbb{F}_{7^6} = \mathbb{F}_{1177649}$.

- $Q_1(x) = x(1 + x^{39216} - x^{78423})$ $gcd(1, 39216) = 1$
- $Q_5(x) = x^5(1 + x^{39216} - x^{78423})$ $gcd(5, 39216) = 1$
- $Q_7(x) = x^7(1 + x^{39216} - x^{78423})$ $gcd(7, 39216) = 1$
- $Q_{11}(x) = x^{11}(1 + x^{39216} - x^{78423})$ $gcd(11, 39216) = 1$
- $Q_{13}(x) = x^{13}(1 + x^{39216} - x^{78423})$ $gcd(13, 39216) = 1$
- $Q_{17}(x) = x^{17}(1 + x^{39216} - x^{78423})$ $gcd(17, 39216) = 1$
- $Q_{25}(x) = x^{23}(1 + x^{39216} - x^{78423})$ $gcd(25, 39216) = 1$

$Q_1,\ Q_5,\ Q_7,\ Q_{11},\ Q_{13},\ Q_{17},\ Q_{25}$ are permutation polynomials of $F_{7^6} = F_{117649}$.

4 Application in cryptography

4.1 Recalls and preliminaries

We recall that the readable and understandable text that we send is called the plain text and the method allowing it to be concealed by masking its content is called encryption. The latter consists of transforming the plain text into an unintelligible text called the ciphertext. The reverse process is called decryption.
Public key cryptography is a process associated with a public key which corresponds to encryption and a secret key which corresponds to decryption.
Permutation polynomials play a crucial role in the field of cryptography, particularly in the design and analysis of cryptographic algorithms that operate in finite fields. Finite fields, also known as Galois fields, are mathematical structures used in various cryptographic applications, including encryption, digital signatures, and error-correcting codes. Permutation polynomials are a special class of polynomials that have desirable properties when used in finite field arithmetic.

Definition 4.1. Cryptography is defined as the art or the process of writing or reading secret messages or codes. So, it is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message.

Definition 4.2. In the language of cryptography, the codes are called by ciphers. The information to be disguised is called as plaintext. After transformation to a secret form, the message is called by ciphertext.

Definition 4.3. The process of converting from plaintext to ciphertext is defined as encrypting or enciphering. The inverse process from ciphertext back to plaintext is called by decrypting or deciphering.

Definition 4.4. A cryptosystem is a system for encrypting and decrypting secret messages.

Recall that the cryptography with a public key is a process associated to a public key which corresponds to the encrypting and the secret key corresponds to the decrypting.

Let $E = \{A, B, C, \cdots, Y, Z\}$ and $F = \{00, 01, 02, 03, \cdots, 24, 25\}$. Consider the bijection from E into F given by :

A	B	C	D	E	F	G	H	I	J	K	L	M
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
00	01	02	03	04	05	06	07	08	09	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$
13	14	15	16	17	18	19	20	21	22	23	24	25

Let $M = M_1 M_2 \cdots M_d$ be the plain text, that is to say, the message to be encrypted, where $d \in \mathbb{N}, (d \geq 2)$ and $M_i \in E, (1 \leq i \leq d)$. The integer d represents the number of letters in the plaintext.
In this example, taking $u = 1 \not\equiv 0(mod\ 3)$, we consider the following permutation polynomial :

$$P(x) = x\Big(1 + x^{\frac{q-1}{3}} - x^{\frac{2(q-1)}{3}}\Big)$$

such that $q = 7^n$, where the polynomial P is the public key and the positive integer n is the secret key. (it is clear that $1 \not\equiv 0(mod\ 3)$ and $gcd\Big(1, \frac{q-1}{3}\Big) = 1$).
Therefore, we know there exists a permutation $\sigma \in S_q$ such that :

$$\begin{array}{rccc} \sigma : & \frac{\mathbb{Z}}{q\mathbb{Z}} & \longrightarrow & \frac{\mathbb{Z}}{q\mathbb{Z}} \\ & x & \longmapsto & \sigma(x) = P(x) \end{array}$$

Consider the restriction of σ to $E = \{0, 1, \ldots, 25\}$, *i.e.*,

$$\sigma_{/E} = \begin{pmatrix} 0 & 1 & \cdots & 25 \\ \sigma(0) & \sigma(1) & \cdots & \sigma(25) \end{pmatrix} = \begin{pmatrix} 0 & 1 & \cdots & 25 \\ P(0) & P(1) & \cdots & P(25) \end{pmatrix}$$

This permutation $\sigma_{/E}$ is the second secret key.
note that $\sigma(0) = \sigma(00),\ \sigma(1) = \sigma(01), \ldots,\ \sigma(09) = \sigma(9)$.

4.2 Procedure for encryption and decryption

Encryption. To encrypt the plaintext message $M = M_1 M_2 \ldots . M_d$ into the ciphertext message $C = C_1 C_2 \ldots . C_d$, we proceed by the following way :

(i) We translate each letter M_i into its digital equivalent, using the bijection mentioned above to a positive integer $\alpha_i \in F,\ 1 \leq i \leq d$.

(ii) We calculate $P(0), P(1), \ldots, P(25)$ modulo 26, to obtain the numbers $\beta_1, \ldots, \beta_d$, *i.e*, we have : $P(\alpha_i) \equiv \beta_i\ (mod\ 26)$, then we pose, $\sigma_{/E}(\alpha_i) = \beta_i$, $1 \leq i \leq d$, where $\sigma_{/E}$ is the second secret key.

(iii) The number $\beta_1\beta_2\ldots\beta_d$ is transformed into letters by the bijection mentioned above into $C = C_1C_2\ldots C_d$. So the plaintext M is encrypted by the ciphertext C.

Decryption. To decrypt the ciphertext message C, the recipient first begins to translate it into letters. Then, knowing the keys $P(x)$, n and $\sigma_{/E}$, he determines the permutation $(\sigma_{/E})^{-1}$ which gives C in numbers. Then these numbers are transformed into letters which give the plaintext message M.

Remark 4.5. We can crypt the message by proceeding word by word. If we want to code an entire sentence, we add to the set E the letter Δ which will correspond to the number 00. Then will take $E = \{\Delta, A, B, C, \ldots, Y, Z\}$, $F = \{00, 01, 02, 03, \ldots, 25, 26\}$ and the bijection will be:

$$\Delta \leftrightarrow 00,\ A \leftrightarrow 01,\ B \leftrightarrow 02,\ C \leftrightarrow 03, \ldots Y \leftrightarrow 25,\ Z \leftrightarrow 26$$

Then work $(mod\ 27)$.

Example 4.6. Let us encrypt the plaintext message $TRAVEL$.
First, we replace the letters of this message by the corresponding digits. This produces the number :

$$\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5\alpha_6 = 191700210411$$

The polynomial considered is :

$$P(x) = x\Big(1 + x^{114} - x^{228}\Big)$$

where $q = 343 = 7^3$ and $gcd(1, 114) = 1$. We obtain, after calculations :

$$\sigma_{/E}(19) = P(19) \equiv 07(mod\ 26)$$

$$\sigma_{/E}(17) = P(17) \equiv 17(mod\ 26)$$

$$\sigma_{/E}(00) = P(00) \equiv 00(mod\ 26)$$

$$\sigma_{/E}(21) = P(21) \equiv 05(mod\ 26)$$

$$\sigma_{/E}(04) = P(04) \equiv 04(mod\ 26)$$

$$\sigma_{/E}(11) = P(11) \equiv 15(mod\ 26)$$

After calculations of $P(i)$, $0 \leq \alpha(i) \leq 25$, $modulo$ 26, we obtain that $\sigma_{/E}$ is given by :

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	1	24	3	4	21	20	19	18	9	10	15	12	13	14	11	16	17	8	7

20	21	22	23	24	25
6	5	22	23	2	25

Then, we obtain the following number :

$$\beta_1\beta_2\beta_3\beta_4\beta_5\beta_6 = 071700050415$$

wich is translated into letters by :

$$C = HRAFEP$$

wich is the ciphertext.

To decrypt the ciphertext message HRAFEP, which replaces the letters by the corresponding

digits, we find the number : 071700050415. knowing the polynomial and the value of n and the permutation $\sigma_{/E}$, then we apply $(\sigma_{/E})^{-1}$ and we obtain :

$$\begin{aligned}(\sigma_{/E})^{-1}(07) = (\sigma_{/E})^{-1}(7) &= 19\\ (\sigma_{/E})^{-1}(17) &= 17\\ (\sigma_{/E})^{-1}(00) &= 00\\ (\sigma_{/E})^{-1}(05) = (\sigma_{/E})^{-1}(5) &= 21\\ (\sigma_{/E})^{-1}(04) = (\sigma_{/E})^{-1}(4) = 4 &= 04\\ (\sigma_{/E})^{-1}(15) &= 11\end{aligned}$$

which is translated into letters and this gives the plaintext message $TRAVEL$.

References

[1] S. Badidja, A. Ait Mokhtar, O. Özer, *Representation of integers by k-generalized Fibonacci sequences and applications in cryptography*, Asian-Eur. J. Math. **14**(9), Article ID 2150157, (2021), 11 p..

[2] J. N. Doliskani, E. Malekian, A. Zakerolhosseini, *A Cryptosystem Based on the Symmetric Group S_n*, International Journal of Computer Science and Network Security, **8**(2), 226–234, (2008).

[3] N. Koblitz, *A Course in Number Theory and Cryptography*, Graduate Texts in Mathematics, 114. New York etc.: Springer-Verlag. viii, 208 p.; DM 74.00 (1987)

[4] Y. Laigle-Chapuy, *Permutation polynomials and applications to coding theory*, Finit fields Appl., **13**(1), 58–70, (2007).

[5] K. H. Rosen, *Discret Mathematics and its Applications*, 5th edition, Boston, MA: McGraw-Hill. xxi, 928 p. (2003).

[6] C. Small, *Arithmetic of finite fields*, Pure and Applied Mathematics (Marcel Dekker). 148. New York etc.: Marcel Dekker, Inc.. xii, 216 p. (1991).

[7] C. Small, *Permutation binomials*, Int. J. Math. Math. Sci., **13**(2), 337–342, (1990).

[8] D. Wan and R. Lidl, *Permutation polynomials of the form $h(x) = x^r f(x^{\frac{q-1}{d}})$ and their group structure*, Monatsh. Math. **112**(2), 149–163, (1991).

Author information

F. Aggoun Laid, Labotory of Fixed Point and Applications
Height Normal School Kouba, Algiers, BP 92, Algeria.
E-mail: fadhila.laid@g.ens-kouba.dz

A. Ait Mokhtar, Labotory of Fixed Point and Applications
Height Normal School Kouba, Algiers, BP 92, Algeria.
E-mail: ahmed.aitmokhtar@yahoo.fr, ahmed.aitmokhtar@g.ens-kouba.dz

O. Özer, Department of Mathematics
Faculty of Science and Arts Kirklareli University Kirklareli-39100, Turkey.
E-mail: ozenozer39@gmail.com

Received: 2024-05-10
Accepted: 20255-04-21