Permutation polynomials over Finite Fields and their application to Cryptography

Katia Benseba

Department of Mathematics and Statistics

Submitted in partial fulfillment of the requitements for the degree of

Master of Science

Faculty of Mathematics and Science
Brock University
St. Catharines, Ontario

ABSTRACT

The aim of the paper is the study of Permutation Polynomials over finite fields and their application to cryptography. In my talk, I will begin by a brief review of finite fields, define permutation polynomials over finite fields and their properties. I will present old results such as Hermite-Dickson's Theorem as well as some most recent ones. After introducing cryptography, I will give a historical overview, by explaining some cryptosystems such as RSA and ElGamal. Finally, I will present some cryptographical protocols based on Permutation Polynomials over Finite Fields.

Acknowledgement

I would like to express my sincere gratitude to my supervisor Dr Omar Kihel, for his continuous help and guidance. I also would like to thank Dr Pouria Ramazi for serving as the supervisory committee.

I would also want to thank my parents, Papa, Maman, who have worked for my success, with their love, their support and their precious advises. As well as my dear little sister and brother whom I love so much.

To my dearest husband Reda, thank your for all your love and support.

I am also grateful for my friend Leila Meskine's precious advises and constant support, and thankful for all the help she provided in helping me complete my degree.

Katia

CONTENTS

INTRODUCTION

The need to share information with some people without others being able to read their content has probably always existed. From the simple substitution methods of the ancient Greeks to today's computerized algorithms, various codes and ciphers have been used by both individuals and governments to send secure messages. As an increasing amount of our personal communications and data have moved online, understanding the underlying ideas of internet security has become increasingly important and have led each civilization to develop solutions to the problem of confidentiality.

The first thing that comes to mind, to get a message across, is simply to hide that message, so that its existence is unknown by those who should not read it. The techniques used to dissimulate a message are in the domain of steganography. The Greeks shaved the heads of their soldiers to write a message, well concealed once the hair had grown back. Steganography is not considered part of cryptography, which does not seek to conceal a message, but rather transform it into an incomprehensible message for an untrained person.

The fundamental objective of cryptography is to allow two people, commonly referred to as Alice and Bob, to send information over an insecure channel. Ideally this communication is such that an unknown adversary eavesdropping on the channel cannot understand what is being said. We may assume the information we wish to communicate is simply an element in $\mathbb{F}_{2^n}$. Thus the encryption of the plaintext and decryption of the ciphertext are (invertible) maps of $\mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ therefore, permutation polynomials can be used to construct cryptographic systems. Although nowadays breaking the codes that the online world currently runs on would be an almost hopeless task, when quantum computers appear, they will be threatened. That is why, in this paper we will be introducing some cryptosystems based on some special permutation polynomials that we believe almost unbreakable by this future technology.

In the first chapter, we present some finite fields basis, giving the definition of a finite field and a survey of results needed to understand the underlying of permutation polynomials theory.

In the second chapter, we introduce permutation polynomials, give some criteria to determine if a polynomial is of permutation as well as presenting some classes of linear and non-linear permutation polynomials that will be of great use in constructing the cryptographical schemes.

In the third chapter, we define what cryptography is, determine its use in ancient and most nowadays cryptographical protocols.

Finally, in the last chapter, we see the use of permutation polynomial in constructing encryption algorithms.

CHAPTER 1

FINITE FIELDS

The theory of finite fields is a key part of number theory and computer science. Not only that many questions about the integers and the rational numbers can be translated into questions about arithmetic in finite fields which tends to be more tractable. But it is well-suited to computer calculations in many modern cryptographic applications.

In this chapter, we will see some definition and results on Finite fields.

Definition 1.1. *A field is a set F with two binary operations $+$ and $.$ such that:*

1. $(F,+)$ *is a commutative group with identity element* 0.
2. $(F-\{0\},.)$ *is a commutative group with identity element* 1.
3. *The distributive law* $a.(b+c) = ab+ac$ *holds* $\forall\ a,b,c \in F$.

Example 1. $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, *and* $\mathbb{Z}_p$ *for* p *a prime are fields with the usual operations of addition and multiplication.*

Definition 1.2. *A subfield of a field F is a subset of F which is itself a field with the same operations as F.*

Lemma 1.1. *Let F be a finite field containing a subfield K with q elements. Then F has q^m elements, where $m = [F:K]$.*

Proof. F is a finite vector space over K where m denote its dimension. Then F has a basis over K consisting of m elements say $v_1,\ldots,v_m$. So every element of F can be written uniquely as a combination of elements of the basis as follow $a_1v_1+\ldots+a_mb_m$, $a_i \in K$. Since each a_i is in K then a_i can take q values then F must have exactly q^m elements. □

Example 2. $\mathbb{Q}$ *is a subfield of* $\mathbb{R}$. $\mathbb{R}$ *is a subfield of* $\mathbb{C}$. $\mathbb{Z}_p$ *has no subfields other than itself.*

1.1 Extension Fields

If K is a subfield of a field F, then we say that F is an extension or extension field of K. F is naturally a vector space over K, hence the degree of the extension is its dimension $[F:K] := dim_K F$.

Definition 1.3. *Let K a subfield of F. An element $\alpha \in F$ is called algebraic over K if it is a root of some nonzero polynomial with coefficients in K.*

Definition 1.4. *A field extension F over K is called a simple extension if there exists an element α in F with $F = K(\alpha)$.*

Example 3. *$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}/a, b \in \mathbb{Q}\}$ is a field containing $\mathbb{Q}$ it is then an extension field of $\mathbb{Q}$ and $\sqrt{2}$ is algebraic over $\mathbb{Q}$ as it is a root of a polynomial in $\mathbb{Q}[x]$ for instance $x^2 - 2$.*

Proposition 1.1. *The sum, difference, product and quotient of algebraic elements are again algebraic.*

Theorem 1.1. *If L is a finite extension of K and M is a finite extension of L, then M is a finite extension of K with*

$$[M : K] = [M : L][L : K].$$

Proof. Let $[M : L] = m$, $[L : K] = n$ and $\{\alpha_1, \ldots, \alpha_m\}$ be a basis of M over L and let $\{\beta_1, \ldots, \beta_m\}$ be a basis of L over K. We can use them to form a basis of M over K. Any element x in M can be expressed as follow:

$$x = l_1\alpha_1 + \ldots + l_m\alpha_m$$

where $l_1, \ldots, l_m$ are in L. Therefore they can all be rewritten as a linear combination of L's basis $\{\beta_1, \ldots, \beta_m\}$. Then

$$\begin{aligned} x &= \sum_{i=1}^{m} l_i\alpha_i \\ &= \sum_{i=1}^{m} (\sum_{j=1}^{n} k_{ij}\beta_j)\alpha_i \\ &= \sum_{i=1}^{m}\sum_{j=1}^{n} k_{ij}\beta_j\alpha_i \end{aligned}$$

where k_{ij} are coefficients in K. We now have to show that the mn elements $\beta_j\alpha_i$ form a basis of M over K. We clearly see that with these elements span M, so we now need to prove they are linearly independent over K. To do so we will have to show that if $\sum_{i=1}^{m}\sum_{j=1}^{n} k_{ij}\beta_j\alpha_i = 0$ then $k_{ij} = 0$ for i and j. Suppose we have:

$$\sum_{i=1}^{m}\sum_{j=1}^{n} k_{ij}\beta_j\alpha_i = 0 \Leftrightarrow \sum_{i=1}^{m}(\sum_{j=1}^{n} k_{ij}\beta_j)\alpha_i = 0$$

and since α_i are linearly independent over L we must have:

$$\sum_{j=1}^{n} k_{ij}\beta_j = 0$$

for $1 \leq i \leq m$, and since β_j are linearly independent over K it follows $k_{ij} = 0$ for all i and j. □

Theorem 1.2. *Every finite extension of K is algebraic over K.*

Proof. Let L be a finite extension of K and let $[L:K]=m$. For α in L, the $m+1$ elements $1,\alpha,\ldots,\alpha^m$ must be linearly dependent over K therefore there exist $a_0,a_1,\ldots,a_m$ in K (not all zero) such that $a_0+a_1\alpha+\ldots+a_m\alpha^m=0$. Therefore α is algebraic over K. Then L is algebraic over K, since all its elements are algebraic. □

Theorem 1.3. *Let F be an extension field of K and α in F be algebraic of degree n over K and let g be the minimal polynomial of α over K. Then $K(\alpha)$ is isomorphic to $K[x]/(g)$.*

Proof. Let φ a mapping defined as follow:

$$\begin{aligned}\varphi : K[x] &\longrightarrow K(\alpha)\\ \varphi(f) &\longrightarrow f(\alpha)\end{aligned}$$

where $ker(\varphi)=\{f\in K[x]/f(\alpha)=0\}=\{hinK[x]/h(\alpha)g(\alpha)=0\}=(g)$. Then by the First Isomorphism Theorem, $K[x]/(g)\cong Im(\varphi)$ and since g is irreducible then (g) is a prime ideal of the principal ideal domain $K[x]$ therefore the residue class ring $K[x]/(g)$ is a field and so is $Im(\varphi)$. Moreover, $K\subset Im(\varphi)\subset K(\alpha)$. and since α is in $Im(\varphi)$ then $Im(\varphi)=K(\alpha)$. □

Example 4. *Consider the extension $\mathbb{R}(i)$ of $\mathbb{R}$. The minimal polynomial of i over $\mathbb{R}$ is x^2+1. So $\mathbb{R}(i)\cong\mathbb{R}[x]/(x^2+1)$ and $\{1,i\}$ is a basis for $\mathbb{R}(i)$ so $\mathbb{R}(i)=\{a+bi/a,b\in\mathbb{R}\}=\mathbb{C}$.*

Theorem 1.4. *If K is a field and $f\in K[x]$ a non-constant polynomial, then there exists a simple algebraic extension field F of K containing a zero of f.*

Proof. Let $F=K[x]/(f)$, F is the field since f is irreducible. Its elements are the residue classes $[k]=k+(f)$ with k in $K[x]$.F can be viewed as an extension of K, and for every $k=a_0+a_1x+\ldots+a_mx^m$ in $K[x]$ we have:

$$\begin{aligned}[k]&=[a_0+a_1x+\ldots+a_mx^m]\\ &=[a_0]+[a_1][x]+\ldots+[a_m][x]^m\\ &=a_0+a_1[x]+\ldots+a_m[x]^m\end{aligned}$$

so any element of F can be expressed as a polynomial in $[x]$ with coefficient in K. Since any field containing K and $[x]$ must contain these expressions then F is a simple extension of K obtained by adjoining $[x]$ and if $f=\sum_{i=0}^n b_ix^i$ then $f([x])=\sum_{i=0}^n b_i[x]^i=[f]=[0]$ which means $[x]$ is a root of f thus F is a simple algebraic extension of K. □

Corollary 1.1. *A simple extension field $F(\alpha)$ is finite if and only if α is algebraic over F.*

Definition 1.5. *Let f in $K[x]$ be a polynomial of positive degree and F an extension field of K. Then we say that f splits in F if f can be written as a product of linear factors in $F[x]$, in other words there exist elements $\alpha_1,\ldots,\alpha_n$ in F such that $f=a(x-\alpha_1)\ldots(x-\alpha_n)$ where a is the leading coefficient of f.*

Definition 1.6. *The field F is called a splitting field of f over K if it splits in F and if $F=K(\alpha_1,\ldots,\alpha_n)$.*

1.2 Characterization of Finite Fields

Since 1 is in any field and addition is a closed operation (the sum of any two elements is another element of the field) we have that; 1, $1+1$, $1+1+1$, $1+1+1+1$, $1+1+1+1+1$, etc. are all elements of the field. Two possibilities exist for this sequence of elements:

- some sum of 1's will equal 0
- or not in which case none of the elements of the sequence are the same and we get an infinite number of elements in the field.

The smallest positive number of 1's whose sum is 0 is called the **characteristic** of the field. If no number of 1's sum to 0, we say that the field has characteristic zero. In other words,
Let F a field. The mapping

$$\begin{aligned} \varphi\colon \mathbb{Z} &\to F \\ n &\mapsto n1_F \end{aligned}$$

is a ring homomorphism and the image of this ring map is a domain being a subring of a feild hence the kernel of φ is a prime ideal in $\mathbb{Z}$. Hence the kernel of φ is either (0) or (p) for some prime number p. If the kernel is 0 then the characteristic of F is 0, if not then the characteristic of F is p.

Proposition 1.2. *Let F a finite field of characteristic a prime p, then F has p^n elements with $n \in \mathbb{N}^*$ the degree of F over its prime subfield.*

Proposition 1.3. *Let F a finite field of cardinal q, then for all $a \in F$, $a^q = a$.*

Proof. When $a = 0$, $a^q = a$ is satisfied. The non-zero elements form a group of order $q-1$ under multiplication. Knowing that for a group G, $a^{|G|} = 1_G$ for any element of the group, then by looking at F^* as a group, we have $a^{|F^*|} = a^{q-1} = 1$ for any a in F^* and by multiplying by a both sides we get $a^q = a$ for any a in F^*. □

Lemma 1.2. *If F is a field of characteristic p, then for n in $\mathbb{N}^*$*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}, \forall a, b \in F.$$

Lemma 1.3. *If F is a finite field with q elements and K is a subfield of F, then the polynomial $x^q - x$ in $K[x]$ factors in $F[x]$ as*

$$x^q - x = \prod_{a \in F} (x - a)$$

and F is a splitting field of $x^q - x$ over K.

Proof. Since the polynomial $x^q - x$ has degree q, it has at most q roots in F, and by *Proposition* 2.2 all elements of F are roots of the polynomial and there are exactly q. Therefore the polynomial can be written as the product of $x - a$ where a an element of F. □

Theorem 1.5. *For every prime number p and every positive integer n, there exists a finite field with $q = p^n$ elements isomorphic to the splitting field of $x^q - x$ on $\mathbb{F}_p$.*

Proof. (Existence) For $q = p^n$, consider $x^q - x$ in $\mathbb{F}_p[x]$ and let F be its splitting field over $\mathbb{F}_p$. Since the derivative $(x^q - x)' = qx^{q-1} - 1 = -1$ meaning the $gcd(x^q - x, qx^{q-1} - 1) = 1$ so $x^q - x$ is separable and has q different roots. Let $S = \{a \in F / a^q - a = 0\}$, then S is a subfield of F (S contains 0 - for any a, b in S, $(a-b)^q = a^q - b^q = a - b$ is in S and $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$ is in S). On the other hand $x^q - x$ must split in S since S contain all its roots so F which is the splitting field of $x^q - x$ is a subfield of S therefore $F = S$ and since S has q elements then F has $q = p^n$ elements.

(Uniqueness) Let F be a finite field with $q = p^n$ elements, then by *Proposition* 2.2, F has characteristic p if it contains $\mathbb{F}_p$ as a subfield. And by *Lemma* 2.3, F is a splitting field of $x^q - x$ and unique up to isomorphism.

□

Example 5. *Let $\mathbb{F}_2[\alpha]$ a field where α is a root of the polynomial $x^2 + x + 1 \in \mathbb{F}_2[x]$ then then by the theorem above $\mathbb{F}_2[\alpha]$ contains $2^2 = 4$ elements and $\mathbb{F}_2[\alpha] = \mathbb{F}_4$ (not to confuse with $\mathbb{Z}/4\mathbb{Z}$ which is not a field.*

Proposition 1.4. *Let $n, m \in \mathbb{N}^*$, then $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ if and only if $m|n$.*

Proof. If m divides n, then $p^m - 1$ divides $p^n - 1$ and so $x^{p^m-1} - 1$ divides $x^{p^n-1} - 1$ in $\mathbb{F}_p[x]$, so every root of $x^{p^m-1} - 1$ is a root of $x^{p^n-1} - 1$ hence belongs to $\mathbb{F}_q$. It follows that $\mathbb{F}_q$ contains a splitting field of $x^{p^m-1} - 1$ as a subfield of $\mathbb{F}_p$ and by *Theorem* 1.5 such a splitting field has order p^m therefore $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$.

A subfield of $\mathbb{F}_{p^n}$ must have order p^m for some positive integer $m \leq n$ but p^n must be a p^m so m must divide n. □

Example 6. *The subfields of the finite field $\mathbb{F}_{p^{36}}$ can be found through the divisors of* 36*, as shown in the diagram below:*

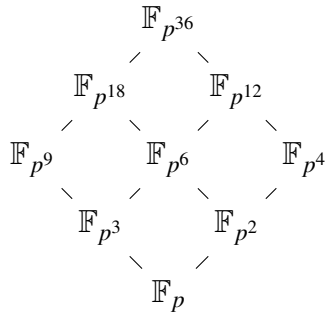

Figure 1.1: Subfields of $\mathbb{F}_{p^{36}}$

Theorem 1.6. *For every finite field $\mathbb{F}_q$ the multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$ is cyclic.*

Proof. Let $o = q-1$, the order of $\mathbb{F}_q^*$, and let $o = p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}$ be its prime factor decomposition. For each i, $1 \leq i \leq m$, the polynomial $x^{o/p_i} - 1$ has at most o/p_i roots in $\mathbb{F}_q$. Since $o/p_i < o$, it follows that there are nonzero elements of $\mathbb{F}_q$ which are not roots of this polynomial. Let a_i be such an element, and set $b_i = a_i^{o_i/p_i^{e_i}}$, then $b_i^{p_i^{e_i}} = a_i^{o_i} = 1$ so the order of b_i divides $p_i^{e_i}$ therefore their order are of the form $p_i^{d_i}$ for some $0 \leq d_i \leq e_i$. We then have:

$$b_i^{p_i^{d_i-1}} = a_i^{o/p_i} \neq 1$$

so the order of b_i is precisely $p_i^{e_i}$.
Let $b = b_1 b_2 \dots b_m$, then its order is o which means b is a generator for the group. Suppose it is not, and that the order of b is a proper divisor of o. It is therefore a divisor of at least one of the m integers o/p_i, say o/p_1, then:

$$1 = b^{o/p_1} = b_1^{o/p1} b_2^{o/p1} \dots b_m^{o/p1}$$

Thus $p_i^{e_i}$ divides o/p_1 so $b_i^{o/p_1} = 1$ which leads to $b_1^{o/p_1} = 1$ therefore the order of b_1 must divide o/p_1, which is impossible since the order of b_1 is $p_1^{e_1}$.Contradiction, thus $\mathbb{F}_q^*$ is a cyclic group with generator b. □

Definition 1.7. *A generator of the multiplicative group (cyclic) $\mathbb{F}_q^*$ is called a primitive element of $\mathbb{F}_q$.*

Example 7. *$\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ has two primitive elements, namely 2 and 3.*

1.3 Irreducible polynomials over finite fields

The important role of irreducible polynomials is that one can explicitly construct fields using irreducible polynomials through factor rings. If one wants to make explicit calculations in say a finite field, it is often required to find an irreducible polynomial, in order to get information of the structure of the field. This is important for applications of field theory, for instance cryptography.

Definition 1.8. *The element α in some extension field $\mathbb{F}_{p^n}$ has a minimal polynomial when α is algebraic over $\mathbb{F}_p$, that is when $f(\alpha) = 0$ for some non-zero polynomial $f(x)$ in $\mathbb{F}_p[x]$. Then the minimal polynomial of α is defined as the monic polynomial of least degree among all polynomials in $\mathbb{F}_p[x]$ having α as a root and denoted M_α.*

Proposition 1.5. *Let α in $\mathbb{F}_{p^n}$ and M_α be its minimal polynomial over $\mathbb{F}_p$. Then*

1. *M_α is irreducible over $\mathbb{F}_p$.*
2. *$deg(M_\alpha) \leq n$.*
3. *If α is a root of P in $\mathbb{F}_p[x]$, then M_α divides P. In particular, M_α divides $X^{p^n} - X$*

Proof. 1. If it weren't the case, then M_α can be factor into the product of two monic polynomials, say P and Q. Then $M_\alpha(\alpha) = P(\alpha)Q(\alpha) = 0$ that implies that either $P(\alpha) = 0$ or $Q(\alpha) = 0$. Say $P(\alpha) = 0$, since $deg(P) < deg(M_\alpha)$ it means that we found a new monic polynomial with less degree then the minimal polynomial which is impossible.

2. Since $\mathbb{F}_{p^n}$ is a vector space of dimension n over $\mathbb{F}_p$, then the $n+1$ elements $1, \alpha, \alpha^2, \ldots, \alpha^n$ can't be linearly independent, it means there exist $k_0, \ldots, k_n$ in $\mathbb{F}_p$ such that

$$\sum_{i=0}^{n} k_i \alpha^i = 0$$

Then α is a root of $P(x) = \sum_{i=0}^{n} k_i x^i$. It follows that the degree of M_α is at most n.

3. If $P(\alpha) = 0$ we write $P(x) = Q(x)M_\alpha(x) + R(x)$ with $0 < deg(R) < deg(M_\alpha)$. Then $R(\alpha) = 0$ which leads $R = 0$ since there is no polynomial with degree less then the degree of M_α with α as a root. Therefore M_α divides P. In particular M_α divides $X^{p^n} - X$.

□

Corollary 1.2. *For every finite field $\mathbb{F}_q$ and every positive integer n there exists an irreducible polynomial in $\mathbb{F}_q[x]$ of degree n.*

Proof. Let $\mathbb{F}_s$ be the extension field of $\mathbb{F}_q$ of order q^n, so that $[\mathbb{F}_s : \mathbb{F}_q] = n$. Then $\mathbb{F}_s = \mathbb{F}_q(\alpha)$ for some α in $\mathbb{F}_r$. Then, let $p(x)$ the minimal polynomial of α over $\mathbb{F}_q$, it is an irreducible polynomial in $\mathbb{F}_q[x]$ of degree n. □

Lemma 1.4. *Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial over finite field $\mathbb{F}_q$ and let α be a root of f in an extension field of $\mathbb{F}_q$. Then for a polynomial $h \in \mathbb{F}_q[x]$ we have $h(\alpha) = 0$ if and only if f divides h.*

Proof. The minimal polynomial of α over $\mathbb{F}_q$ is given by $a^{-1}f$, where a is the leading coefficient of f since it is monic and irreducible in $\mathbb{F}_q[x]$. Then by *Proposition* 1.5, $M_\alpha = a^{-1}f$ divides h, therefore f divides h. □

Lemma 1.5. *Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial over $\mathbb{F}_q$ of degree m. Then $f(x)$ divides $x^{q^n} - x$ if and only if m divides n.*

Proof. Suppose f divides $x^{q^n} - x$. Let α be a root of f in the splitting field of f over $\mathbb{F}_q$. Then $\alpha^{q^n} = \alpha$, so α is in $\mathbb{F}_{q^n}$. Thus $\mathbb{F}_q[\alpha]$ is a subfield of $\mathbb{F}_{q^n}$. Since $[\mathbb{F}_q[\alpha] : \mathbb{F}_q] = m$ and $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ we have

$$[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q[\alpha]][\mathbb{F}_q[\alpha] : \mathbb{F}_q]$$
$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q[\alpha]].m$$

so m divides n.
Now suppose m divides n. Then by *Proposition* 1.3 $\mathbb{F}_{q^n}$ contains $\mathbb{F}_{q^m}$. Let α be a root of f in the splitting field of f over $\mathbb{F}_q$. Then $[\mathbb{F}_q[\alpha] : \mathbb{F}_q] = m$ and so $\mathbb{F}_q[\alpha] = \mathbb{F}_{q^m}$ then α is in $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^n}$ so $\alpha^{q^n} = \alpha$, thus α is a root of $x^{q^n} - x$ in $\mathbb{F}_q[x]$ and by *Lemma* 1.4 f divides $x^{q^n} - x$. □

Theorem 1.7. *Let F_q be a finite field and let $f \in F_q[x]$ be irreducible over F_q, $deg f = n$. Then the splitting field of f is F_q^n. Furthermore, if α is a zero of f , then the other zeros of f are given by $\alpha^q, \ldots, \alpha^{q^{n-1}}$.*

Proof. Let α be a root of f in the splitting field of f over $\mathbb{F}_q$. Then $[\mathbb{F}_q[\alpha] : \mathbb{F}_q] = m$, hence $\mathbb{F}_q[\alpha] = \mathbb{F}_{q^m}$ and so α is in $\mathbb{F}_{q^m}$. We will now prove that if $\beta \in \mathbb{F}_{q^m}$ is a root of f then β^q is also a root of f. Let $f = a_0 + a_1 x + \ldots + a_m x^m$ and by *Proposition* 1.2 we get:

$$\begin{aligned} f(\beta^q) &= a_0 + a_1\beta^q + \ldots + a_m\beta^{qm} \\ &= a_0^q + (a_1\beta)^q + \ldots + (a_m\beta^m)^q \\ &= f(\beta)^q \\ &= 0 \end{aligned}$$

Then the elements $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ are roots of f.
We now need to check that they are all distinct. Suppose not then for some power q^j and q^k where $0 \leq j < k \leq m-1$ we have $\alpha^{q^j} = \alpha^{q^k}$ and raising to the power q^{m-k} we get $\alpha^{q^{m-k+j}} = \alpha^{q^m} = \alpha$ then $\alpha^{q^{m-k+j}} - \alpha = 0$ so α is a root of $x^{q^{m-k+j}} - x$ and by *Lemma* 1.4 f divides $x^{q^{m-k+j}} - x$ but by *Lemma* 1.5 this is only possible if m divides $m-k+j$ which is impossible since $m > m-k+j$. □

Corollary 1.3. *Let f be an irreducible polynomial in $\mathbb{F}_q[x]$ of degree m. Then the splitting field of f over $\mathbb{F}_q$ is given by $\mathbb{F}_{q^m}$.*

Proof. The theorem above shows that f splits in $\mathbb{F}_{q^m}$, and we have $\mathbb{F}_q(\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}} = \mathbb{F}_q[\alpha] = \mathbb{F}_{q^m}$. □

Corollary 1.4. *Any two irreducible polynomials in $\mathbb{F}_q[x]$ of the same degree have isomorphic splitting fields.*

Theorem 1.8. *For every finite field $\mathbb{F}_q$ and every n in $\mathbb{N}$, the product of all monic irreducible polynomials over $\mathbb{F}_q$ whose degrees divide n is equal to $x^{q^n} - x$.*

Proof. By *Lemma* 1.5 the monic irreducible polynomials over $\mathbb{F}_q$ that appear in the canonical factorization of $x^{q^n} - x$ are those whose degrees divide n. And since $(x^{q^n} - x)' = q^n x^{q^n-1} - 1 = -1$ then it has no multiple roots in its splitting field over $\mathbb{F}_q$. Therefore each monic irreducible polynomial over $\mathbb{F}_q$ whose degree divides n occurs exactly once in the canonical factorization of $x^{q^n} - x$ in $\mathbb{F}_q[x]$. □

Example 8. *Let $q = n = 2$ the monic irreducible polynomials over $\mathbb{F}_2[x]$ whose degrees divide 2 are x, $x+1$ and x^2+x+1. And we can easily see that $x^{2^2} - x = x^4 - x$ indeed factors as follow in $\mathbb{F}_2[x]$:*

$$x^4 - x = x(x+1)(x^2+x+1)$$

1.4 Automorphisms and bases

Definition 1.9. *Let $\mathbb{F}_{q^m}$ be an extension of $\mathbb{F}_q$ and let $\alpha \in \mathbb{F}_{q^m}$. Then the elements $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ are called the conjugates of α with respect to $\mathbb{F}_q$.*

Theorem 1.9. *The conjugates of $\alpha \in \mathbb{F}_q^*$ with respect to any subfield of $\mathbb{F}_q$ have the same order in the group $\mathbb{F}_q^*$.*

Proof. We know that for a finite cyclic group $< a >$ or order m the elements a^k are of order $\frac{m}{gcd(k,m)}$, then this applies to the cyclic group $\mathbb{F}_q^*$ where all the power α^{q^k} are of order $\frac{q-1}{gcd(q^k,q-1)}$ but $gcd(q^k, q-1) = 1$ hence the elements α^{q^k} are of order $q-1$. □

Corollary 1.5. *If α is a primitive element of $\mathbb{F}_q$, then so are all its conjugates with respect to any subfield of $\mathbb{F}_q^*$.*

Example 9. *$\mathbb{F}_4$ can be seen as an extension of degree 2 of $\mathbb{F}_2$, ie, $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ where α is a root of an irreducible polynomial of degree 2 with coefficients in $\mathbb{F}_2$ for instance $x^2 + x + 1$. So $\mathbb{F}_2(\alpha) = \{0, \alpha, \alpha^2\}$ but α^2 can also be written as $\alpha + 1$ therefore $\mathbb{F}_2(\alpha) = \{0, \alpha, \alpha + 1\}$*

Definition 1.10. *An automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ is an automorphism σ of $\mathbb{F}_{q^m}$ which fixes the elements of $\mathbb{F}_q$ pointwise (acts as identity: $\forall\ x \in \mathbb{F}_q$, $\sigma(x) = x$). Thus, σ is a one-to-one mapping from $\mathbb{F}_{q^m}$ onto itself and for all α, β in $\mathbb{F}_{q^m}$ we have:*

1. $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$.
2. $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$.

Theorem 1.10. *The distinct automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ are exactly the mappings $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$, defined by:*

$$\sigma_j(\alpha) = \alpha^{q^j} \text{ for } \alpha \in \mathbb{F}_{q^m} \text{ and } 0 \leq j \leq m-1.$$

for $\alpha \in \mathbb{F}_{q^m}$ and $0 \leq j \leq m-1$.

Proof. Let's first prove that the mappings are indeed automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, to do so we will have to show that they are bijectives endomorphisms.

- **Endomorphism** for each σ_j and $\forall\ \alpha, \beta \in \mathbb{F}_{q^m}$ we have $\sigma_j(\alpha\beta) = \sigma_j(\alpha)\sigma_j(\beta)$ and $\sigma_j(\alpha + \beta) = \sigma_j(\alpha) + \sigma_j(\beta)$, then σ_j is clearly an endomorphism.
- **Injectivity** $\sigma_j(\alpha) = 0 \Leftrightarrow \alpha = 0$.
- **Surjectivity** Since $\mathbb{F}_{q^m}$ is a finite set, σ_j is surjective.

Let's now show that any automorphism of $\mathbb{F}_{q^m}$ is precisely one of the σ_j for some $0 \leq j \leq m-1$.
Let β be a primitive element of $\mathbb{F}_{q^m}$ and let $f = x^m + a_{m-1}x^{m-1} + \ldots + a_0 \in \mathbb{F}_q[x]$ be its minimal polynomial over $\mathbb{F}_q$, then

$$\begin{aligned} f(\beta) &= \beta^m + a_{m-1}\beta^{m-1} + \ldots + a_0 \\ &= 0 \end{aligned}$$

and by applying *sigma* to both sides we get

$$\begin{aligned} 0 &= \sigma(\beta^m + a_{m-1}\beta^{m-1} + \ldots + a_0) \\ &= \sigma(\beta^m) + \sigma(a_{m-1}\beta^{m-1}) + \ldots + \sigma(a_0) \\ &= \sigma(\beta)^m + a_{m-1}\sigma(\beta)^{m-1} + \ldots + a_0 \end{aligned}$$

so $\sigma(\beta)$ is a root of f in $\mathbb{F}_{q^m}$ and by *Theorem* 1.4 any root is a power of the primitive one so $\sigma(\beta) = \beta^{q^j}$ for some j, $0 \leq j \leq m-1$. Since σ is a homomorphism and β primitive, we get that $\sigma(\alpha) = \alpha^{q^j}$ for all α in $\mathbb{F}_{q^m}$. □

Remark. *The automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ form a group under composition of mappings, called the Galois group of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and denoted $Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$. This group of automorphisms is a cyclic group of order m, generated by σ_1.*

1.5 Traces and Norms

Definition 1.11. *For α in $\mathbb{F}_{q^m}$, the trace $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ of α over $\mathbb{F}_q$ is defined by:*

$$\begin{aligned} Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) &= \text{sum of conjugates of } \alpha \text{ in } \mathbb{F}_q \\ &= \alpha + \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{m-1}} \end{aligned}$$

If $q = p$, where p is the characteristic of $\mathbb{F}_{p^m}$, then $Tr_{\mathbb{F}_{p^m}/\mathbb{F}_p}(\alpha)$ is called the absolute trace of α and is denoted $Tr(\alpha)$.
Moreover, when looking at the minimal polynomial of α then $Tr_{F/K}(\alpha) = -a_{m-1}$.

Proposition 1.6. *Let $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^m}$. Then $\forall\, k \in K$ and $\forall\, \alpha$ and $\beta \in F$ the trace function $Tr_{F/K}$ satisfies the following properties:*

1. $Tr_{F/K}(\alpha+\beta) = Tr_{F/K}(\alpha) + Tr_{F/K}(\beta)$,
2. $Tr_{F/K}(k\alpha) = kTr_{F/K}(\alpha)$,
3. $Tr_{F/K}(a) = ma$,
4. $Tr_{F/K}(\alpha^q) = Tr_{F/K}(\alpha)$.

Proof. 1. For α and β in F:

$$\begin{aligned} Tr_{F/K}(\alpha+\beta) &= (\alpha+\beta) + (\alpha+\beta)^q + \ldots + (\alpha+\beta)^{q^{m-1}} \\ &= \alpha + \beta + \alpha^q + \beta^q + \ldots + \alpha^{q^{m-1}} + \beta^{q^{m-1}} \\ &= Tr_{F/K}(\alpha) + Tr_{F/K}(\beta) \end{aligned}$$

2. Knowing that for k in K we have $k^{q^i} = k\ \forall\, i \geq 0$. Then for α in F:

$$\begin{aligned} Tr_{F/K}(k\alpha) &= k\alpha + (k\alpha)^q + \ldots + (k\alpha)^{q^{m-1}} \\ &= k\alpha + k^q\alpha^q + \ldots + k^{q^{m-1}}\alpha^{q^{m-1}} \\ &= k\alpha + k\alpha^q + \ldots + k\alpha^{q^{m-1}} \\ &= k(\alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}) \\ &= kTr_{F/K}(\alpha) \end{aligned}$$

3. $Tr_{F/K}(a) = aTr_{F/K}(1) = a[1 + (1)^q + \ldots + (1)^{q^{m-1}}] = ma$.

4.

$$\begin{aligned} Tr_{F/K}(\alpha^q) &= \alpha^q + (\alpha^q)^q + \ldots + (\alpha^q)^{q^{m-2}} + (\alpha^q)^{q^{m-1}} \\ &= \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{m-1}} + \alpha^{q^m} \\ &= \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{m-1}} + \alpha \\ &= \alpha + \alpha^q + \alpha^{q^2} + \ldots \alpha^{q^{m-1}} \\ &= Tr_{F/K}(\alpha). \end{aligned}$$

□

Remark. *We clearly see that $Tr_{F/K}$ is a linear transformation from F onto K.*

Theorem 1.11. *Let F be a finite extension of a finite field K. Then the $K-$linear transformations from F into K are precisely the mappings L_β with β in F given by $L_\beta(\alpha) = Tr_{F/K}(\beta\alpha)$ for all α in $\mathbb{F}$. And if α and β are distinct element of F then $L_\alpha \neq L_\beta$.*

Definition 1.12. *For α in $\mathbb{F}_{q^m}$, the norm $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ of α over $\mathbb{F}_q$ is defined by:*

$$\begin{aligned} N_{F/K}(\alpha) &= \textit{product of conjugates of}\alpha \\ &= \alpha.\alpha^q.\alpha^{q^2}\ldots\alpha^{q^{m-1}} \\ &= \alpha^{1+q+q^2+\ldots+q^{m-1}} \\ &= \alpha^{\frac{q^m-1}{q-1}} \end{aligned}$$

When looking at the minimal polynomial of α then $N_{F/K}(\alpha) = (-1)^m a_0$.

Proposition 1.7. *Let $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^m}$. Then $\forall\ k \in K$ and $\forall\ \alpha$ and $\beta \in F$ the norm function $N_{F/K}$ satisfies the following properties:*

1. $N_{F/K}(\alpha\beta) = N_{F/K}(\alpha)N_{F/K}(\beta)$,
2. $N_{F/K}(a) = a^m$,
3. $N_{F/K}(\alpha^q) = N_{F/K}(\alpha)$.

Proof. The above properties can easily be shown using the definition of the norm the same way it was done for the *trace*. □

Theorem 1.12. *Transitivity of Trace and Norm Let K be a finite field, let F be a finite extension of K and E a finite extension of F. Then:*

$$Tr_{E/K}(\alpha) = Tr_{F/K}(Tr_{E/F}(\alpha))$$

and

$$N_{E/K}(\alpha) = N_{F/K}(N_{E/F}(\alpha))$$

Proof. Let $K = \mathbb{F}_q$, let $[F : K] = m$ and let $[E : F] = n$, so $[E : K] = mn$. Then for α in E we have:

$$\begin{aligned} Tr_{F/K}(Tr_{E/F}(\alpha)) &= \sum_{i=0}^{m-1} Tr_{F/K}(\alpha)^{q^i} \\ &= \sum_{i=0}^{m-1} (\sum_{j=0}^{n-1} \alpha^{q^{jm}})^{q^i} \\ &= \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \alpha^{q^{jm+i}} \\ &= \sum_{k=0}^{mn-1} \alpha^{q^k} \\ &= Tr_{E/K}(\alpha). \end{aligned}$$

and

$$\begin{aligned} N_{F/K}(N_{E/F}(\alpha)) &= N_{F/K}(\alpha^{\frac{q^{mn}-1}{q^m-1}}) \\ &= (\alpha^{\frac{q^{mn}-1}{q^m-1}})^{\frac{q^m-1}{q-1}} \\ &= \alpha^{\frac{q^{mn}-1}{q-1}} \\ &= N_{E/K}(\alpha). \end{aligned}$$

□

1.6 Bases

$\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$ can be seen as $\mathbb{F}_q[x]/(f)$ where f is an irreducible polynomial of degree m and α is a root of f in $\mathbb{F}_{q^m}$. Then every element of $\mathbb{F}_{q^m}$ can be written uniquely as a polynomial in α over $\mathbb{F}_q$ of degree less than m, therefore for any α, the set $\{1, \alpha, \ldots, \alpha^{q^{m-1}}\}$ form a basis for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

Definition 1.13. *A polynomial basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ is a basis of the form $\{1, \alpha, \ldots, \alpha^{q^{m-1}}\}$, where α is a set of elements of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.*

Remark. *The element α mentioned above can be a primitive element however it is not required to be.*

Example 10. *Let $K = \mathbb{F}_3$ and $F = \mathbb{F}_9 = \mathbb{F}_{3^2}$ then F is an extension of K of degree 2. Therefore there exist α a root of an irreducible polynomial of degree 2 over K. Let this polynomial be $x^2 + 1$ in $\mathbb{F}_3[x]$, then $\{1, \alpha\}$ is a polynomial basis for $\mathbb{F}_9$ over $\mathbb{F}_3$ but α is not primitive since $\alpha^4 = 1$.*
However if we take α to be the root of the irreducible polynomial $x^2 + x + 2$ then $\{1, \alpha\}$ is a polynomial basis and α is a primitive element of $\mathbb{F}_9$.

Definition 1.14. *A normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ is a basis of the form $\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$, consisting of a suitable element α in $\mathbb{F}_{q^m}$ and all its conjugates with respect to $\mathbb{F}_q$. And such element is called a normal element.*

Theorem 1.13. *For any finite extension F of a finite field K, there exists a primitive normal basis of F over K that consists of primitive elements of F.*

Example 11. *Let $K = \mathbb{F}_2$ and $F = \mathbb{F}_8 = \mathbb{F}_{2^3} = K(\alpha)$ where α is a root of an irreducible polynomial of degree 3 over K. Let $x^3 + x^2 + 1$ be such polynomial. Then the set $\{\alpha, \alpha^2, \alpha^4\}$ form a basis of $\mathbb{F}_8$ over $\mathbb{F}_2$ and since $\alpha^4 = \alpha(\alpha^3) = \alpha(\alpha^2 + 1) = \alpha^3 + \alpha = \alpha^2 + \alpha + 1$ then $\{\alpha, \alpha^2, \alpha^4 = \alpha^2 + \alpha + 1\}$ is a normal basis. And since α is a primitive elements of F then $\{\alpha, \alpha^2, \alpha^2 + \alpha + 1\}$ is a primitive normal basis for F over K.*

CHAPTER 2

PERMUTATION POLYNOMIALS OVER FINITE FIELDS

Permutation polynomials are of great importance because of their link to modern cryptography, used to secure data transmission and storage. As for a message M (being an element of $\mathbb{F}_q$) that Alice would want to send Bob. Bob would receive a ciphered message $M_c = P(M)$, where $P(x)$ is a permutation polynomial of $\mathbb{F}_q$. The issue is that, P being a bijection, the original message can be easily recovered. To prevent any attacker from doing so, the permutation must have additional properties.
The aim of this chapter is to present a survey of results on permutation polynomials as well as explaining the way of determining them. Furthermore, we will be looking into the criteria for a random polynomial to be a permutation one.

2.1 Permutations

Definition 2.1. *Let S be a finite set of cardinal n, $n \in \mathbb{N}^*$. A bijective function from a set S to itself is called a permutation of the set S.*

We denote by S_n the set of all permutations of the set $\{1,2,\ldots,n\}$ and $|S_n| = n!$. An element $\sigma \in S_n$ is of the form:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

The set S_n forms a group under the function composition "$\circ$" and therefore called the symmetric group.

Example 12. *The group S_3 consist of* 3! *elements. These six elements are:*

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

2.2 Permutation Polynomials

A polynomial $f \in \mathbb{F}_q[x]$, where q is a prime power, is called a permutation polynomial of $\mathbb{F}_q$ if the associated polynomial function below is a permutation of $\mathbb{F}_q$, in other words bijective.

$$\begin{aligned} f\colon \mathbb{F}_q &\to \mathbb{F}_q \\ x &\mapsto f(x) \end{aligned}$$

Obviously, if f is a permutation polynomial of $\mathbb{F}_q$, then the equation $f(x) = a$ has exactly one solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$.

Proposition 2.1. *Below are some permutation polynomials:*

- *For all $(a,b) \in \mathbb{F}_q^* \times \mathbb{F}_q$, the polynomial $aX + b$ is a permutation polynomial.*
- *X^k is a permutation polynomial of $\mathbb{F}_q$ if and only if $gcd(k, q-1) = 1$.*

Proof.
- $ax + b = y \Leftrightarrow x = (y-b)/a$, the function is clearly bijective.
- 0 has a unique antecedent which is 0. $\mathbb{F}_q^*$ is a cyclique group of order $q-1$. Let α be a generator, the group generated by α^k is of order $(q-1)/gcd(k, q-1)$.

□

Example 13. *Let $g(x) = 2x^2 + x$ is a permutation polynomial over $\mathbb{Z}/4\mathbb{Z}$ as $g(0) = 0$, $g(1) = 3$, $g(2) = 2$ and $g(3) = 1$, and $g(x)$ defines the permutation:*

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

Example 14. *Consider the polynomial $h(x) = x^2 + 3x + 5 \in \mathbb{F}_{11}$ which takes the following values in $\mathbb{F}_{11}$:*

x	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
h(x)	*5*	*9*	*4*	*1*	*0*	*1*	*4*	*9*	*5*	*3*	*3*

We clearly see that $h(x)$ is not bijective, therefore h is not a permutation polynomial.

2.3 Criteria for determining Permutation Polynomials

In order to study these polynomials, it is important to have theoretical and algorithmic means to test whether a polynomial is of permutation. In this section, we give simple criteria that, although ineffective from an algorithmic point of view, yield to numerous theoretical results.

2.3.1 Hermite's Criterion

Hermite's criterion is used to show that some polynomial families are of permutation. Testing it in real life is hardly possible as it is of complexity $O(q^2)$, which is way to high to be used in real life.

Theorem 2.1. *Let $\mathbb{F}_q$ be of characteristic p. Then $f \in F_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following two conditions hold:*

1. *f has exactly one root in $\mathbb{F}_q$;*
2. *for each integer t with $1 \leq t \leq q-2$ and $t \not\equiv 0 \mod p$, the reduction of $f(x)^t \mod x^q - x$ has degree $\leq q-2$.*

Proof. $\rightarrow$ Let f be a permutation polynomial of $\mathbb{F}_q$. Then (1) is trivial since $f(x) = 0$ has a unique root because of the fact that f is bijective. The reduction of $f(x)^t \mod x^q - x$ is some polynomial $\sum_{j=0}^{q-1} b_j^{(t)} x^j$, where $b_{q-1}^{(t)} = -\sum_{c \in \mathrm{F}_q} f(a_i)^t$ (by the *Lagrange* polynomial), and according to Lemma 3.2,$b_{q-1}^{(t)} = 0$ for $t = 1, 2, \ldots, q-2$, hence (2) follows.

$\leftarrow$ Conversly, let (1) and (2) be satisfied. Then (1) implies $\sum_{i=0}^{q-1} f(a_i)^{q-1} = -1$ and from (2), $\sum_{i=0}^{q-1} f(a_i)^t = 0$, $1 \leq t \leq q-2$ and $t \not\equiv 0 \mod p$. Since $\mathbb{F}_q$ is of characteristic p, then using the following formula:

$$\sum_{i=0}^{q-1} f(a_i)^{tp^j} = (\sum_{i=0}^{q-1} f(a_i)^t)^{p^j},$$

we get $\sum_{c \in \mathrm{F}_q} f(a_i)^t = 0$ for $1 \leq t \leq q-2$, and this identity holds trivially for $t = 0$. Therefore Lemma 2.2 implies that f is a permutation polynomial of $\mathbb{F}_q$. □

Corollary 2.1. *If $q > 2$ and $f(x)$ is a permutation polynomial of $\mathbb{F}_q$ then the reduction of f modulo $x^q - x$ has degree at most q-2.*

Proof. By setting $t = 1$ in the theorem stated above, this gives us the assertion. □

2.3.2 Images' Criterion

The easiest algorithm is to calculate, for a permutation polynomial P, all $P(a)$ values for one in $\mathbb{F}_q$, and see if they are distinct (as done above in Example 14). For a polynomial of degree n this requires $O(qn)$ operations since only one assessment is performed in $O(n)$ computations, along with $O(q)$ in order to check if the values are distinct. Since we can stop as soon as we get the same value twice, the average complexity will actually be $O(n\sqrt{q})$, however if P is a permutation polynomial then we must calculate all values.

Alternatively, the following property can be tested:

Lemma 2.1. *$P \in \mathbb{F}_q[x]$ is a permutation polynomial if and only if:*

$$\prod_{a \in \mathbb{F}_q} (X - P(a)) = X^q - X.$$

2.3.3 Inverse images' Criterion

We can also prefer to check the following criteria, which allows us to perform fewer operations f the polynomial is not of permutation.

Lemma 2.2. *$P \in \mathbb{F}_q[x]$ is a permutation polynomial if and only if:*

$$\forall a \in \mathbb{F}_q, deg(gcd(X^q - X, P(X) - a)) = 1.$$

2.4 Classes of Permutation Polynomials

2.4.1 Linearized Polynomials

These type of polynomials are of great use in cryptography. For instance, let $\mathbb{F}_q$ the finite field of order q. We will denote an extension of $\mathbb{F}_q$ of degree m by $\mathbb{F}_{q^m}$. An element $\vartheta \in \mathbb{F}_{q^m}$ is said to be normal over $\mathbb{F}_q$ if the elements $\vartheta, \vartheta^q, \ldots, \vartheta_{q^{m-1}}$ form a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Any element x of $\mathbb{F}_{q^m}$ can be expressed as $x = \sum_{i=0}^{m-1} x_i \vartheta_{q^i}$ where $x_i \in \mathbb{F}_q$. Thus $\mathbb{F}_{q^m}$ can be identified by $\mathbb{F}_q^m$, the set of all m-tuples over $\mathbb{F}_q$, and $x \in \mathbb{F}_{q^m}$ can be written as $(x_0, x_1, \ldots x_{m-1})$. If $q = 2$, then $x_i \in \{0, 1\}$ and in this case the weight of x is defined to be the number of 1's in $(x_0, x_1, \ldots x_{m-1})$, and denote it by $w(x)$.

Consequently, a polynomial $L(x) \in \mathbb{F}_{q^m}[x]$ is called a linearized polynomial or p-polynomial over $\mathbb{F}_q$ if $L(x) = \sum_{i=0}^{k} \alpha_i x^{q^i}$ and satisfies:

- $L(x+y) = L(x) + L(Y)$ for all $x, y \in \mathbb{F}_{q^m}$.
- $L(ax) = aL(x)$ for all $x \in \mathbb{F}_{q^m}$ and $a \in \mathbb{F}_q$.

Therefore, corresponding to an element $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{m-1})$ of finite field $\mathbb{F}_{q^m}$, we define a polynomial function L_α on $\mathbb{F}_{q^m}$ as:

$$L_\alpha(x) = \sum_{i=0}^{m-1} \alpha_i x^{q^i}$$

where $L_\alpha(x)$ are linearized p-polynomials in $\mathbb{F}_{q^m}$.

The theorem below states when such polynomials are of permutation.

Theorem 2.2. *Let $\mathbb{F}_q$ be of characteristic p. Then the p-polynomial:*

$$L(x) = \sum_{i=0}^{m} a_i x^{p^i} \in \mathbb{F}_q[x]$$

is a permutation polynomial if and only if $L(x)$ only has the root 0 in $\mathbb{F}_q$.

Proof. Suppose that $L(x)$ has only one root, then from above we have $L(a) = L(b)$ if and only if $L(a-b) = 0$. But since *zero* is the only root then $a - b$ must equal 0 thus $a = b$. Therefore $L(x)$ is one-to-one, hence a permutation polynomial. □

Corollary 2.2. *If $m = 2^k$ for some $k \geq 0$ and $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) \in \mathbb{F}_{2^m}$. Then the polynomial $L_\alpha(x)$ is a permutation of $\in \mathbb{F}_{2^m}$ if and only if $w(\alpha)$ is odd.*

Proposition 2.2. *An element α of $\mathbb{F}_{q^m}$ is a normal element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ if and only if $L_\alpha(x)$ is a permutation polynomial of $\mathbb{F}_{q^m}$.*

Proof. Suppose α a normal element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Let y in $\mathbb{F}_{q^m}$, then $y = \sum_{i=0}^{m-1} y_i \alpha^{q^i}$ for some y_i in $\mathbb{F}_q$. If $z = \sum_{i=0}^{m-1} y_i v^{q^i}$, where $\mathscr{B} = \{v, v^q, \ldots, v^{q^{m-1}}\}$ is the fixed norla basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then $y = L_z(\alpha) = L_\alpha(z)$ thus L_α is surjective and therefore $L_\alpha(x)$ is a permutation polynomial of $\mathbb{F}_{q^m}$.

Conversly suppose $L_\alpha(x)$ is of permutation, then $L_\alpha(x) = L_x(\alpha) = y$ has a unique solution for all y in $\mathbb{F}_{q^m}$, which implies that α is a normal element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. □

2.4.2 Some Classes of Nonlinear Permutation Polynomials

Definition 2.2. *For α in $\mathbb{F}_{||^>}$, the trace $Tr(\alpha)$ of α over $\mathbb{F}_q$ is defined as*

$$Tr(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}$$

Theorem 2.3. *Let m be an odd positive integer, and $\beta = (\beta_0, \ldots, \beta_{m-1})$ be an element of $\mathbb{F}_{2^m}$ such that $w(\beta)$ is even and that 0 and 1 are the only roots of $L_\beta(x)$ in $\mathbb{F}_{2^m}$. Suppose k_1 and k_2 are non negative integers such that $gcd(2^{k_1} + 2^{k_2}, 2^m - 1) = 1$. Let l be any positive integer with $(2^{k_1} + 2^{k_2}).l \equiv 1 \mod 2^m - 1$ and γ be an element of $\mathbb{F}_{2^m}$ with $Tr(\gamma) = 1$. Then*

$$f(x) = (L_\beta(x) + \gamma)^l + Tr(x)$$

is a permutation polynomial of $\mathbb{F}_{2^m}$.

Proof. Since $Tr(L_\beta(x)) = 0$ then $Tr(L_\beta(x) + \gamma) = Tr(\gamma) = 1$, therefore $L_\beta(x) + \gamma \neq 0$ in $\mathbb{F}_{2^m}$. Suppose that x and y are distinct elements of $\mathbb{F}_{2^m}$ such that $f(x) = f(y)$. First, suppose that $Tr(x) = Tr(y)$. Then $f(x) = f(y)$ gives $(L_\beta(x) + \gamma)^l = (L_\beta(y) + \gamma)^l$ then when raising both sides to the power $2^{k_1} + 2^{k_2}$ we get $L_\beta(x) + \gamma = L_\beta(y) + \gamma)$ which gives us $L_\beta(x) + L_\beta(y) = 0)$ which is equivalent to $L_\beta(x + y) = 0$.

Since the only roots of $L_\beta(x)$ are 0 and 1 then $x + y$ must be 1 (since we assumed they were distinct). Therefore $Tr(x + y) = Tr(1) = m.1 = 1$, thus $Tr(x) + Tr(y) \neq 0$ therefore $Tr(x) \neq Tr(y)$ which contradict our assumption.

Let's now assume $Tr(x) = 0$ and $Tr(y) = 1$, then $f(x) = f(y)$ implies $(L_\beta(x) + \gamma)^l = (L_\beta(y) + \gamma)^l + 1$ then after raising both sides to the power $2^{k_1} + 2^{k_2}$ we get:

$$\begin{aligned}
L_\beta(x) + \gamma &= [(L_\beta(y) + \gamma)^l + 1]^{2^{k_1} + 2^{k_2}} \\
&= [(L_\beta(y) + \gamma)^l + 1]^{2^{k_1}} [(L_\beta(y) + \gamma)^l + 1]^{2^{k_2}} \\
&= [(L_\beta(y) + \gamma)^{l.2^{k_1}} + 1][(L_\beta(y) + \gamma)^{l.2^{k_2}} + 1] \\
&= (L_\beta(y) + \gamma)^{l.(2^{k_1} + 2^{k_2})} + (L_\beta(y) + \gamma)^{l.2^{k_1}} + (L_\beta(y) + \gamma)^{l.2^{k_2}} + 1 \\
&= L_\beta(y) + \gamma + (L_\beta(y) + \gamma)^{l.2^{k_1}} + (L_\beta(y) + \gamma)^{l.2^{k_2}} + 1
\end{aligned}$$

Since $Tr(L_\beta(x)) = 0$ and $Tr((L_\beta(y)+\gamma)^{l.2^{k_1}}) = Tr((L_\beta(y)+\gamma)^{l.2^{k_2}}) = Tr((L_\beta(y)+\gamma)^l)$, if we apply the trace to the relation above we get

$$Tr(\gamma) = Tr(\gamma) + Tr(1)$$

which means $Tr(1) = 0$ which is a contradiction to the definition of the trace since m is odd. □

Example 15. *The polynomial x^2+x has only 0 and 1 as roots in $\mathbb{F}_{2^m}$ so we can set $L_\beta(x) = x^2+x$. Let's take $\gamma = 1$, $m = 3$, $k_1 = 1$, $k_2 = 0$ and $l = 5$. Therefore, from the above theorem we know that $(x^2+x+1)^7 + Tr(x)$ is a permutation polynomial of $\mathbb{F}_{2^3}$.*

Lemma 2.3. *The polynomial $f(x) = x^{2^{2^r.k+2^r}} + x^{2^{2^r.k}} + x^{2^r}$ where r and k are positive integers, is a permutation polynomial if and only if $(2^{k.2^r}+2^r)$ and 2^m-1 are co-prime.*

Theorem 2.4. *The polynomial $g(x) = (x^{2^{2^r.k}} + x^{2^r} + \alpha)^l + x$ is a permutation polynomial of $\mathbb{F}_{2^m}$ if $Tr(\alpha) = 1$ and $(2^{k.2^r}+2^r).l \equiv 1 \mod 2^m - 1$.*

Proof. To show that $g(x)$ is a permutation polynomial, we will show that for any element β the equation $g(x) = \beta$ has a unique solution in other words, showing that $g(x) - \beta$ is a permutation polynomial.
Since $Tr(x^{2^{2^r.k}} + x^{2^r} + \alpha) = Tr(\alpha) = 1$ then $x^{2^{2^r.k}} + x^{2^r} + \alpha \neq 0$ for all x in $\mathbb{F}_{2^m}$. Let β be an element of $\mathbb{F}_{2^m}$, then $g(x) = \beta$ implies $(x^{2^{2^r.k}} + x^{2^r} + \alpha)^l = x + \beta$ and raising both sides to the power $2^{k.2^r}+2^r$ we get $(x^{2^{2^r.k}} + x^{2^r} + \alpha) = (x+\beta)^{2^{k.2^r}+2^r}$ therefore $(x^{2^{2^r.k}} + x^{2^r} + \alpha) + (x+\beta)^{2^{k.2^r}+2^r} = 0$.

Let $h(x) = (x^{2^{2^r.k}} + x^{2^r} + \alpha) + (x+\beta)^{2^{k.2^r}+2^r}$, note that $h(x+\beta)$ and $h(x)$ have the same number of solutions and that $h(x+\beta) = x^{2^{2^r.k+2^r}} + x^{2^{2^r.k}} + x^{2^r} + \beta^{2^{2^r.k}} + \beta^{2^r} + \alpha$, and since $x^{2^{2^r.k+2^r}} + x^{2^{2^r.k}} + x^{2^r}$ is a permutation polynomial then the equation $h(x+\beta) = 0$ has a unique solution and so does $h(x) = 0$ therefore $g(x)$ is a permutation polynomial. □

2.4.3 Dickson Polynomials

Dickson Polynomials were first introduced by Leonard Eugene Dickson, an American mathematician in 1897. In this section we will define them and give a brief survey of some of their important properties.

Definition 2.3. *The Dickson polynomial $D_n(x,a)$ of the first kind over $\mathbb{F}_q$ is defined by:*

$$D_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}$$

where $\lfloor n/2 \rfloor$ is the largest integer $\leq n/2$. It satisfies the following recurrence:

$$D_n(x,a) = xD_{n-1}(x,a) - aD_{n-2}(x,a), n \geq 2$$

where $D_0(x,a) = 2$ and $D_1(x,a) = x$, and $\forall\, x \neq 0$, $D_n(x+\frac{a}{x},a) = x^n + (\frac{a}{x})^n$.

Dickson polynomials have plenty of properties, and below are the main ones related to our work

Lemma 2.4. *The following properties are satisfied:*

i. $D_n(x,0) = x^n$

ii. $D_{mn}(x,a) = D_m(D_n(x,a),a^n)$

iii. $b^n(D_n(x,a)) = D_n(bx,b^2a)$

iv. if the field's characteristic is a prime p then $D_{np}(x,a) = (D_n(x,a))^p$.

Proof. Let's prove the above properties:

i. $D_n(x,0) = x^n$:

$$\begin{aligned} D_n(x,a) &= \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-0)^i x^{n-2i} \\ &= \frac{n}{n-i}\binom{n-i}{i}(-0)^0 x^{n-2i} + \sum_{i=1}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-0)^i x^{n-2i} \end{aligned}$$

Since $\forall\, i > 0,\ 0^i = 0$ then $\sum_{i=1}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-0)^i x^{n-2i} = 0$ thus $D_n(x,0) = x^n$.

- We prove *ii.*, *iii.*, and *iv.* by introducing a new variable u such as $x = u + \frac{u}{a}$.

□

Lemma 2.5. *The Dickson polynomial* $D_1(x,1) = x$ *is a permutation polynomial modulo* 2^n *where* $n \in \mathbb{N}$ *and* $n \geq 2$.

Proof. $f(x) = x$ is clearly a bijective polynomial, therefore $D_1(x,1) = x$ is a permutation polynomials over the finite field $\mathbb{F}_{2^n}$. □

Lemma 2.6. *Let* $P(x) = a_0 + a_1x + \ldots + a_mx^m$ *be a polynomial with integral coefficients. Then* $P(x)$ *is a permutation polynomials modulo* 2^n *if and only if* a_1 *is odd, and both* $(a_2 + a_4 + \ldots)$ *and* $(a_3 + a_5 + \ldots)$ *are even.*

Theorem 2.5. *Dickson polynomial* $D_n(x,1)$ *of an even degree is not a permutation polynomial modulo* 2^n.

Proof. The result above derives from *Lemma* 4.7. □

Lemma 2.7. *Let m be an odd integer with* $m \geq 1$. *If* $D_m(x,1)$ *is a permutation polynomial modulo* 2^n *where* $n \geq 2$ *then* $D_{m+2}(x,1)$ *is also a permutation polynomials modulo* 2^n.

Theorem 2.6. *Let m be an odd integer with* $m \geq 1$, *then* $D_m(x,1)$ *is a permutation polynomial modulo* 2^n.

Theorem 2.7. *The Dickson polynomial $D_n(x,a)$ is a permutation polynomial if and only if $gcd(n,q^2-1)=1$*

Proof. See [9] page 356. □

Definition 2.4. *Let R be a commutative ring with identity, for any $m \in \mathbb{Z}^+$, and given y and u. The problem of calculating the value of m such that $y = D_m(u,1)$ is called discrete Dickson problem (DDP).*

Theorem 2.8. *The difficulty of solving DDP is equal to that of solving DLP over a finite field $\mathbb{F}_q$.*

CHAPTER 3
A JOURNEY THROUGH CRYPTOGRAPHY

Humans have always felt the need to hide information, even before the first computers and calculating machines appeared. Since its creation, the Internet has evolved to such an extent that it has become an essential communication tool. However, this communication increasingly involves strategic issues related to business activity on the Web. Transactions made through the network can be intercepted, especially since the laws have difficulty to set up on the Internet, so it is necessary to guarantee the security of this information, that is when cryptography comes in. Cryptography nowadays serves not only to preserve the confidentiality of data but also to guarantee its integrity and authenticity.

3.1 What is cryptography ?

Cryptography is the science of using mathematics to encrypt and decrypt data. It is a word designating all the techniques used to disguise a plaintext in such a way as to hide its content (encrypt), which results in a ciphertext. And the process of reverting the ciphertext to its original plaintext is called decryption.

Cryptography enables you to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient.

3.2 Why Cryptography ?

The primary goal of cryptography is to secure important data on the hard disk or as it passes through a canal that may not be secure. Cryptography can therefore provide secrecy as it ensures no one can read or intercept the message except for whom it is intended, thus data is kept secret from those without the proper credentials even if the data was sent through an insecure canal (the internet for example). It also assures the receiver that the message received was not altered in any way from the original (integrity) and provides a mechanism to prove that it was not sent from a third party, and does so, by establishing identity for authentication purposes.

3.3 History of Cryptography

Cryptography is the science of writing codes and encryption for secure communication, and techniques used nowadays are the result of a rich history of development. Since ancient times, cryptography has made it possible to transmit information securely. The development of the techniques employed for current digital encryption may be traced back through the fascinating history of cryptography.

3.3.1 Caesar Cipher

One of the oldest evidence of cryptography is its use when it comes to military, when Julius Caesar sent messages to his generals, he didn't trust his messengers so he replaced every A in his messages with a D and every B with an E and so on through the alphabet. This shift of letters is called Caesar cipher. If a shift by a number n was applied to the message then the recipient of the message had to shift the letters back by n to obtain the original message.

Example 16. *Let $P = katia$ be the plaintext and $n = 5$ then k becomes p, a becomes f, t becomes y and i becomes n. Therefore the cyphertext is $C = pfynf$.*

It is clear that these cyphers rely on the system's secrecy rather than the encryption key. These encrypted messages are simple to decrypt once the system is understood. In fact, considering the frequency of letters in the language, substitution cyphers can be cracked. This made it necessary for cryptography to progress for it to remain effective. That is when the polyalphabetic algorithm came to life, which consist of using two completely different alphabet. The first one in which the plaintext is written while the second one is in which the ciphertext will appear.

Numerous cryptograms were used between the Middle Ages and the First World War, but one the most famous is *Vigenere Cipher* that appeared on 1586, named after the french diplomat Blaise de Vigenère.

3.3.2 Vigenère Cipher

This cipher was the first to use an encryption key. One of his ciphers involved repeating the encryption key throughout the entire message, and creating the cipher text by adding the message character with the key modulo 26.

Example 17. *Let $P = Brock\ University$ be the plaintext, and $k = crypto$ the key.*

3	18	25	16	20	15	3	18	25	16	20	15	3	18	25
c	r	y	p	t	o	c	r	y	p	t	o	c	r	y
2	18	15	3	11	21	14	9	22	5	18	19	9	20	25
b	r	o	c	k	u	n	i	v	e	r	s	i	t	y

And after adding each cell from row 1 *with the one bellow from row* 4 *modulo* 26 *we obtain the following:*

5	10	14	18	5	10	17	1	21	21	12	8	12	12	24
e	j	n	s	e	j	q	a	u	u	l	h	l	l	x

Therefore ciphertext is $C = ejnsejqaulhllx$.

Vigenere's cypher introduced the concept of using encryption keys. In contrast to Caesar cypher, the message's secrecy is based on the confidentiality of the encryption key rather than the confidentiality of the system.

3.3.3 The Enigma machine

Enigma was invented by Arthur Shebius a german engineer at the end of the first word war and was extensively utilised by the German military during World War II. The Enigma machine performed simple yet clever encryption. The difficulty is in the substitution, which switches from one letter to another with each replacement. As you type on the keyboard, the rotors revolve at various rates and output the proper cypher text letters. The initial setup of the rotors was the cryptosystem's key.

The Second World War might have dragged on for an additional three years if it weren't for Alan Turing's efforts.

3.4 Modern Cryptography

With the rise of computing, cryptography has become much more advanced than it ever was. As mentioned above the goal of cryptography "historically" was to make sure of the communication's secrecy. In particular, cryptography was concerned with creating ciphers enabling secret communication between two parties who had somehow, already shared the secret key, prior to the secret communication. This scheme is now referred to as private-key (or the symmetric-key) cryptography. We stress that in that situation, both sides have the same key, used for both encryption and decryption. As opposed to asymmetric encryption, where the transmitter and receiver use different keys for encryption and decryption and do not share any secrets. And as in many modern settings, parties would have difficulties arranging any prior physical meeting, we would easily assume that the asymmetric encryption also known as public-key cryptography is more suitable for nowadays use. In this section we will first give some modular arithmetic result and then give examples of such schemes (popular ones).

3.4.1 Modular Arithmetic

In the following we will be introducing some computational results use in cryptography.

Definition 3.1. *Let* a *in* $\mathbb{Z}/n\mathbb{Z}$. *A solution* x *in* $\mathbb{Z}/n\mathbb{Z}$ *of the equation* $ax \equiv 1 \mod n$ *is called an inverse of* $a \mod n$ *and denoted* a^{-1}.

Lemma 3.1. *Let* a, b *and* c *in* $\mathbb{N}$. *The equation* $ax + by = c$ *has integers solutions* x *and* y *if and only if* c *is a multiple of the* $gcd(a,b)$.

Theorem 3.1. a *is invertible* $\mod n$ *if and only if* $gcd(a,n) = 1$.

Proof. By definition and element a is said to be invertible $\mod n$ if and only if there exists an integer x with $ax \equiv 1 \mod n$. This is true if and only if there exist an integer y such that $ax + ny = 1$ and this is solvable if and only if $gcd(a,n) = 1$ by *Lemma* 3.1. □

And from the above theorem we have:

Corollary 3.1. *Let p be a prime. Then every non-zero element of $\mathbb{Z}/p\mathbb{Z}$ is invertible.*

The above Corollary gives us a useful information about invertible numbers, which will be of great importance when constructing encryption schemes. And the above theorem states that any number has its unique inverse.

Theorem 3.2. *Let $n > 2$ in $\mathbb{N}$ and a in $\mathbb{Z}$. If a is invertible then its inverse is unique* $\mod n$. *In other word, there is a unique solution to the equation $ax \equiv 1 \mod n$.*

Proof. Suppose it is not unique, then there exists b and c such that $ab \equiv ac \equiv 1 \mod n$. So $a(b-c) \equiv 0 \mod n$ thus $n|a(b-c)$. But by *Theorem* 3.1, $gcd(a,n) = 1$ then $n|(b-c)$ thus $b \equiv c \mod n$, contradiction. □

Definition 3.2. *The Euler Function Let $\phi : \mathbb{N} \to \mathbb{N}$ by:*

$$\phi(n) = \textit{The number of } a \textit{ with } 1 \leq a \leq n \textit{ and } gcd(a,n) = 1.$$

A particular case is when n is of the form $n = pq$ where p and q are prime numbers. It leads to the following result.

Theorem 3.3. *If a and b are relatively prime and $n = ab$, then $\phi(n) = \phi(a)\phi(b)$. In particular when $n = pq$ where p and q are two prime numbers, $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$ (As for a prime number p, the numbers a that are less than p satisfying $gcd(a,p) = 1$ are $1, 2, \ldots, p-1$ so there are $p-1$ numbers relatively prime to p).*

Theorem 3.4. *(Euler) Let n in $\mathbb{N}$. Suppose a in $\mathbb{Z}$ and $gcd(a,n) = 1$. Then*

$$a^{\phi(n)} \equiv 1 \mod n.$$

And from that, when n is a prime we have the following:

Theorem 3.5. *(Fermat's Little Theorem) Let p be a prime. Suppose a in $\mathbb{Z}$ is not divisible by p. Then*

$$a^{p-1} \equiv 1 \mod p.$$

With the results above, we shall now go over a few cryptosystems.

3.4.2 RSA Encryption

The Rivest-Shamir-Adleman (RSA) encryption algorithm is an asymmetric encryption algorithm publicly described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology. The creation of a key pair results from the creation of a private and public key, with the private key remaining a secret known only to the key pair's inventor (Bob). This is ideal for delivering sensitive data via a network or Internet connection, where the recipient of the data sends the data sender their public key. The sender of the data then encrypts the sensitive information with the public key and sends it to the recipient. And as only the owner of the private key can decrypt the sensitive data. Thus even though the data could be intercepted and read in transit, the recipient would be aware that the data had been altered in transit as he would be unable to decrypt the new message. It therefore allows the recipient to confirm that the sender is who they claim to be.

The algorithm of such scheme is described as follow:

Scheme

Assume in the later, the key generator is Bob and the other party Alice.

- **Public Key Generation** : Bob will choose p and q to be two large prime numbers and let $N = pq$. Take e an integer such that $gcd(e, \phi(N)) = 1$ where $\phi(N) = (p-1)(q-1)$.
- **Private Key Generation** : Bob chooses k_{priv} his private key such that $k_{priv} = e^{-1} mod \phi(N)$.
- **Key Publishing** : Bob makes public the pair $k_{pub} = (N, e)$.
- **Encryption** Alice will then send the encrypted version c of a message m by computing $c \equiv m^e \mod N$.
- **Decryption** Bob will retrieve back the original message m by computing $c^{k_{priv}} \equiv (m^e)^{k_{priv}} \equiv m^{ek_{priv}} \equiv m \mod N$

Example 18. *Bob will choose $p = 11$ and $q = 23$ and $e = 3$. He will then publish the key $(N = 253, e = 3)$. Then computes $\phi(N) = 220$, and choose $k_{priv} = 147$, his private key with respect to that.*
To encrypt the binary message $m = 57$ with respect to the key $(N = 253, e = 3)$, Alice will compute $m^e \equiv \mod N$ as follow:

$$c \equiv m^e \equiv 57^3 \equiv 250 \mod 253$$

and send it to Bob who will, in order to retrieve the original message, compute $c^{k_{priv}} \mod N$ as follow:

$$c^{k_{priv}} \equiv (m^e)^{k_{priv}} \equiv m^{ek_{priv}} \equiv m \equiv 57 \mod 253$$

and Bob has finally the original message Alice sent him.

The security of RSA

The public key (N, e) is available to everyone. The cipher is broken if the private key k_{priv} is found, and since $ek_{priv} \equiv 1 \mod \phi(N)$, RSA would immediately be broken if $\phi(N)$ can be calculated from N since then we could easily find k_{priv}.

As, if $\phi(N)$ was somehow found then:

$$\phi(N) = (p-1)(q-1) = pq - (p+q) + 1$$

so

$$p + q = N - \phi(N) + 1$$

thus $p+q$ is know, then if you manage finding $p-q$ then it's done, and as you can see it below:

$$(p-q)^2 = (p+q)^2 - 4pq = (p+q)^2 - 4N$$

therefore

$$p - q = \sqrt{(p+q)^2 - 4N}$$

So we know have both $p+q$ and $p-q$ which makes it easy to recover both p and q.

On the other hand, if we manage factoring N then $\phi(N) = (p-1)(q-1)$ is easily found. And that tells us that the security on RSA entirely depends on the difficulty of factoring a large integer into its prime factors. That is why the choice of those factors is decisive.

3.4.3 ElGamal Encryption

The ElGamal encryption scheme is another popular and widely-used encryption method that provides an alternative to the RSA, by making it rely on the difficulty of computing discrete logs in a large prime modulus instead of it depending on the difficulty of factoring large integers. It was described by the egyptian cryptographer Taher Elgamal in 1985. This cryptosystem is defined over a cyclic group G (in particular over $\mathbb{Z}_p$). It works as follow:

Scheme

Assume in the later, the key generator is Bob and the other party Alice.

- **Public Key Generation** : Bob will choose a cyclic group G of order o_G with generator g and identity element e.
- **Private Key Generation** : Bob chooses B_k his private key to be such that for a random non-zero integer b from $\{1,\ldots,q-1\}$, $B_k = g^b$.
- **Key Publishing** : Bob makes public the values $k_{pub} = (G, o_G, g, B_k)$.
- **Encryption** Once the public key shared Alice will choose a non-zero element a from $\{1,\ldots,q-1\}$ and computes her key $A_k = (B_k)^a$ Alice will then send the encrypted version $c = (c_1, c_2)$ of a message M she wants to send Bob, by first mapping it to an element m of G and by computing both $c_1 = g^a$ and $c_2 = m.A_k$ and sends it to Bob.
- **Decryption** Bob will retrieve back the original message M by computing first $c_1^b = (g^a)^b = g^{ab} = (g^b)^a = B_k^a = A_k$, then look for its inverse in G and computes $c_2 A_k^{-1} = (mA_k)A_k^{-1} = m$. Then finally maps m back to the plaintext M.

Example 19. *Bob chooses the cyclic group G to be Z_p where $p = 107$, a generator $g = 2$ and a secret integer $b = 67$ and computes his private key $B_k = 2^{67} \equiv 94 \mod 107$. His public key is $(Z_{107}, 2, 67, 94)$.*

Alice wants to send the message M = Brock to Bob. She will first choose an integer $a = 45$ from $\{1,\ldots,106\}$ and computes $A_k = B_k^a = 94^{45} = 5 \mod 107$ and $c^1 = 2^{45} = 28 \mod 107$, convert the message using $a = 00$, $b = 01$, …, $z = 25$, which gives the message $m = 01\ 17\ 14\ 02\ 10$, then encrypt it by block, as follow:

$$
\begin{aligned}
01.5 &\equiv 5 \mod 107 \\
17.5 &\equiv 85 \mod 107 \\
14.5 &\equiv 70 \mod 107 \\
02.5 &\equiv 10 \mod 107 \\
10.5 &\equiv 50 \mod 107
\end{aligned}
$$

The ElGamal message Alice sends is $(28,5)$ $(28,85)$, $(28,70)$, $(28,10)$ *and* $(28,50)$ *(in real-life use, we would change the key for every block for much more security).*

Bob will look for the inverse of 5 *which is* $c_1^{-b} = 28^{107-67} = 2^{40} = 43$*, then does the following to retrieve the original message back:*

$$
\begin{aligned}
05.43 &\equiv 01 \mod 107 \\
85.43 &\equiv 17 \mod 107 \\
70.43 &\equiv 14 \mod 107 \\
10.43 &\equiv 02 \mod 107 \\
50.43 &\equiv 10 \mod 107
\end{aligned}
$$

He then maps it back to letters, 1 *corresponds to b,* 17 *to r,* 14 *to* 0, 02 *to c and* 10 *to k, to finally get* $M =$ *brock.*

CHAPTER 4

APPLICATION OF PERMUTATION POLYNOMIALS TO CRYPTOGRAPHY

In this chapter we will see how can permutation polynomials be used to protect information and secure communications so that only those for whom the information is intended can read and process it.

4.1 RSA

Recall that RSA is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. The acronym "RSA" comes from the surnames of Ron Rivest, Adi Shamir and Leonard Adleman, who publicly described the algorithm in 1977. And it is one of the cryptosystem that uses permutation polynomials.

4.1.1 Scheme

Recall that for p and q prime numbers and $N = pq$. Take e an integer such that $\phi(N) = (p-1)(q-1)$ and $d = e^{-1} mod \phi(N)$.
(N, e) will form the public key and d the private.
To cipher a message m, we will simply compute:

$$c \equiv m^e (mod N)$$

and the deciphered text will be obtained by computing,

$$m \equiv c^d (mod N)$$

The polynomial used in the above cryptosystem is X^e, which is clearly a permutation polynomial in $\mathbb{Z}_N$[X] (see Proposition 3.1). It has the following properties:

- Efficiency. Indeed, the fact that it is monic makes the size of the public key smaller.
- Easy to evaluate. The computations are modular exponentiation.
- Secure, as the inverse is hardly computable, since $N = pq$ (the trapdoor) is picked such that it can hardly be factored.

4.2 Public Key Cryptosystem

We will, in this section, introduce a cryptosystem similar to the RSA, based on special permutaions polynomials. We introduce a multivariate public key cryptosystem with structure using the group $\mathscr{L}(2,m)$ where $m = 2^k$ for some positive integer k. Let $\mathbb{B} = \{v, v^q, \ldots, v^{q^{m-1}}\}$ a normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. With respect to the basis, $x = (x_0, x_1, \ldots, x_{m-1}) \in \mathbb{F}_{q^m}$, where $x_i \in \mathbb{F}_q$. Then the operation $x \mapsto x^q$ transforms x to $(x_{m-1}, x_0, x_1, \ldots, x_{m-2})$ which is one left cycle shift of $x = (x_0, x_1, \ldots, x_{m-1})$. We have seen that the convolution of two binary strings is equivalent to the composition of corresponding linearized polynomials and that the convolution of two binary strings of odd weight is a binary string of odd weight. For $x \in \mathbb{F}_{2^m}$ let $(x)^t$ denote the t times convolution of x with itself, denote the linearized polynomials by L_α and the set of odd weight elements of $\mathbb{F}_{2^m}$ by $O\mathbb{F}_{2^m}$. Now, in order to present our cryptosystem, we need the results discussed below.

Definition 4.1. *Suppose $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{m-1})$ and $\beta = (\beta_0, \beta_1, \ldots, \beta_{m-1})$ are two elements of finite fields $\mathbb{F}_{q^m}$ where $\alpha_i, \beta_i \in \mathbb{F}_q$. The convolution $\alpha * \beta$ of α and β is defined by:*

$$\alpha * \beta = (\gamma_0, \gamma_1, \ldots, \gamma_{m-1}) \text{ where } \gamma_k = \sum_{i=0}^{m-1} \alpha_{i[m]} \beta_{k-i[m]} \mod m.$$

Example 20. *Let $\alpha = (1,0,1)$ and $\beta = (0,1,1)$ then:*

$$\begin{aligned}
\alpha * \beta &= (\sum_{i=0}^{2} \alpha_i \beta_{-i}[2], \sum_{i=0}^{2} \alpha_i \beta_{1-i}[2], \sum_{i=0}^{2} \alpha_i \beta_{2-i}[2]) \\
&= (1.0 + 0.1 + 1.1, 1.1 + 0.0 + 1.1, 1.1 + 0.1 + 1.0)[2] \\
&= (1,2,1)[2] \\
&= (1,0,1)
\end{aligned}$$

Lemma 4.1. *For $x = (x_0, x_1, \ldots, x_{m-1}) \in \mathbb{F}_{2^m}$, if $(x)^2 = (y_0, \ldots, y_{m-1})$ then $y_{2i+1} = 0$ and $y_{2i} = x_i + x_{(m/2)+i}$ where $0 \le i \le (m-2)/2$.*

Proof. We have, $y_k = \sum_{i=0}^{m1} x_i . x_{k-i}$, where the suffices will be modulo m. For $0 \le i \le (m2)/2$, we have $y_{2i+1} = x_0 x_{2i+1} + x_1 x_{2i} + \ldots + x_{2i+1} x_0 + x_{2i+2} x_{m1} + \ldots + x_{m1} x_{2i+2}$. All the terms will be canceled out in pairs, so we have $y_{2i+1} = 0$. In a similar manner $y_{2i} = x_0 x_{2i} + x_1 x2i1 + \ldots + x_i x_i + \ldots + x_{2i} x_0 + x_{2i+1} x_{m1} + \ldots + x_{m/2+i} x_{(m/2)+i} + \ldots + x_{m1} x_{2i+1} = x_i^2 + x_{m/2+i}^2$, as $x_i^2 = x_i$ for $x_i \in \mathbb{F}_2$.

□

Above lemma implies that $(x)^2$ is a linear function on the finite field $\mathbb{F}_2$. In general, it can be proved that $(x)^{2k}$ is a linear function on the finite field $\mathbb{F}_{2^m}$.

Lemma 4.2. *The function defined by $h(x) = (x)^t$, where t and m are relatively prime, is a bijection from $O\mathbb{F}_2^m$ onto $O\mathbb{F}_2^m$.*

Proof. Since t and m are co-prime, there exist integers r and k such that $tk + rm = 1$ so $tk = 1 + rm$. Suppose $y = h(x) = (x)^t$, this implies that either $L_y = L_{(x)^t} = L_x^t$ or $L_y^k = L_x^{rm+1}$. And since $(L_x)^m = L_v$ where L_v is the identity mapping, then $L_y^k = ((L_x)^r)m).L_x = ((L_x)^m)r).L_x = L_x = L_{(y)^k}$, or in other words $x = y^k$. □

Lemma 4.3. *Convolution is distributive over addition in finite fields, that is, for all* α,β *and* $\gamma \in \mathbb{F}_{2^m}$*:*

$$\alpha * (\beta + \gamma) = \alpha * \beta + \alpha * \gamma$$

Lemma 4.4. *The convolution of two odd weight binary strings is an odd weight binary string.*

4.2.1 Public Key Generation

Consider a message of $m-1$ bit string $(x_0, x_1, \ldots, x_{m-2})$, where m is of the form 2^k . We are adjoining one more bit x_{m-1} to make the weight odd, which has to be removed after decryption.

So we can assume that the message $X = (x_0, x_1, \ldots, x_{m1})$ is an m bit odd weight element of the finite field $\mathbb{F}_{2^m}$. Suppose L_x, L_y, L_z, L_t, L_u are elements of the group $L(m)$ and L_v, L_w are elements of the group $L(2m)$. Let $\pi_1, \pi_2, \pi_3, \pi_4$ and π_5 random permutations of $0, 1, 2, \ldots, m-1$ and π_6, π_7 are random permutations of $0, 1, 2, \ldots, 2m-1$.

Now compute $T_1' = L_x \circ \pi_1$, $T_2' = L_y \circ \pi_2$, $T_3' = L_z \circ \pi_3$, $T_4' = L_t \circ \pi_4$, $T_5' = L_u \circ \pi_5$, $T_6' = L_m \circ \pi_6$ and $T_7' = L_v \circ \pi_7$ where $\circ$ denotes the composition of mappings.

Now, define the affine transformation $T_r(X) = T_r'(X) + \sigma_r$ for $1 \leq r \leq 7$, where σ_r for $1 \leq r \leq 5$ is an even weight element of $\mathbb{F}_{2^m}$ and σ_6, σ_7 are even weight element of $\mathbb{F}_{2^{2m}}$. And when X is an odd weight element of $\mathbb{F}_{2^m}$, then $T_r'(X)$ and $T_r(X)$ are odd weight element of $\mathbb{F}_{2^m}$, thus, $T_r(X)$ is a bijection of $O\mathbb{F}_{2^m}$

Now compute the following:

- $X' = T_1(X)$ and $X" = T_2(X)$
- $T_3((X')^2 * X")$ and $T_4(X' * X") + T_5((X')^2 * X")$

Suppose the quadratic polynomials f_i and f_{m+i} denote the i^{th} bits of $T_3((X')^2 * X")$ and $T_4(X' * X") + T_5((X')^2 * X")$ respectively in their normal basis representation.

Suppose θ' is the normal element of $\mathbb{F}_{2^{2m}}$ and $\mathbb{B}'$ denotes the normal basis of $\mathbb{F}_{2^{2m}}$ over $\mathbb{F}_2$ corresponding to θ'. And consider $(f_0, f_1, \ldots, f_{2m-1})$ as an element of $\mathbb{F}_{2^{2m}}$ corresponding to the basis $\mathbb{B}'$.

Let $Y = (y_0, y_1, \ldots, y_{2m-1})$ the ciphertext which is to be computed using the algorithm described above. Now let $Z = T_6(Y)$ and suppose λ and σ are elements of $\mathbb{F}_{2^{2m}}$ of even and odd weights respectively. Then by Lemma 4.2 the function $\lambda + \sigma * (Z)^{2m-1}$ is a bijection of $O\mathbb{F}_{2^{2m}}$. Hence the relation between the plaintext and the ciphertext is:

$$T_7(f_0, f_1, \ldots, f_{2m-1}) = \lambda + \sigma * (Z)^{2m-1} \tag{4.1}$$

4.2.2 Secret Key

The secret key consist in the following:

- The linear transformations $(T_1, T_2, T_3, T_4, T_5, T_6, T_7)$.
- Two finite fields elements λ and σ .

4.2.3 Encryption

In order to encrypt a message M we will transform it into a binary string $(x_0, x_1, \ldots, x_{m-2})$ and then adjoin an additional bit x_{m-1} so that $X = (x_0, x_1, \ldots, x_{m-1})$ is a binary string of odd weight. Now that is done, we will do the following:

1. Substitute the plaintext $(x_0, x_1, \ldots, x_{m-1})$ in the $2m$ equations in (4.1) and get $2m$ linear equations in ciphertext variables y_i, $0 \leq i \leq 2m-1$.
2. Solve the resulting system using Gaussian elimination to obtain the ciphertext $(y_0, \ldots, _{2m-1})$.

Thus, from equation (4.1), the plaintext variable X and the ciphertext Y satisfy the following relation:

$$E(X) = Y = T_6^{-1}(((F(X) + \lambda) * (\sigma)^{2m-1})^{2m-1})$$

where $F(X) = T_7(f_0, f_1, \ldots, f_{2m-1})$.

Theorem 4.1. *The encryption function E is a bijection from $O\mathbb{F}_{2^{2m}}$ to the set $E(O\mathbb{F}_{2^{2m}})$ of all valid ciphertexts in $O\mathbb{F}_{2^{2m}}$.*

4.2.4 Decryption

The decryption algorithm works as follow:

Input

A ciphertext $Y = (y_0, \ldots, y_{2m-1})$, secret parameters $(T_1, T_2, T_3, T_4, T_5, T_6, T_7)$, two finite fields elements λ and σ as well as an element $\alpha \in \mathbb{F}_{2^{2m}}$ such that $w(\alpha)$ is odd.

Output

1. $Z \leftarrow T_6(Y)$.
2. $(Z)^{2m-1} \leftarrow L_\alpha^{-1}(L_Z^{2m-1}(\alpha))$.
3. $Z \leftarrow \lambda + \sigma * (Z)^{2m-1}$.
4. $A \leftarrow T_7^{-1}(Z')$.
5. $(t_0, \ldots, t_{2m-1}) \leftarrow A$
6. $A_1 \leftarrow (t_0, \ldots, t_{m-1})$ and $A_2 \leftarrow (t_m, \ldots, t_{2m-1})$.

7. $A_3 \leftarrow T_3^{-1}(A_1)$
8. $A_4 \leftarrow T_5(A_3)$
9. $A_5 \leftarrow A_2 + A_4$
10. $A_6 \leftarrow T_4^{-1}(A_7)$
11. $A_7 \leftarrow L_{A_6}^{m-1}(A_3)$
12. $A_8 \leftarrow T_1^{-1}(A_7)$
13. $X \leftarrow T_6^{-1}(A_8)$
14. return X.

X can be proved to be the valid plaintext for the ciphertext Y.

4.3 The cryptosystem Poly-Dragon

4.3.1 Public key generation

In this section we will be introducing another public key cryptosystem using non linear permutation polynomials $g(x) = (x^{2^n} + x + \alpha)^{2^n+1} + x$ and $f(x) = (L_\beta(x) + \gamma)^{2n-1} + Tr(x)$, where α, β and γ are secret. Suppose s and t are two invertible transformations, and the relation between the plaintext x and the ciphertext y is given by $g(s(x)) = f(t(y))$. Let $u = s(x)$ and $v = t(y)$, we have:

$$\begin{aligned} g(u) &= f(v) \\ (u^{2^n} + u + \alpha)^{2^n-1} + u &= (L_\beta(v) + \gamma)^{2^n-1} + Tr(v) \\ \frac{(u^{2^n} + u + \alpha)^{2^n}}{(u^{2^n} + u + \alpha)} + u &= \frac{(L_\beta(v) + \gamma)^{2^n}}{(L_\beta(v) + \gamma)} + Tr(v) \end{aligned}$$

This gives, on the left hand side:

$$A = (u^{2^n} + u + \alpha)^{2^n}(L_\beta(v) + \gamma) + u(L_\beta(v) + \gamma)(u^{2^n} + u + \alpha)$$

and on the right hand side:

$$B = (L_\beta(v) + \gamma)^{2^n}(u^{2^n} + u + \alpha) + Tr(v)(u^{2^n} + u + \alpha)(L_\beta(v) + \gamma)$$

This then gives the relation below:

$$A + B = 0$$

We will now fix a basis $\mathbb{B} = \{v_0, \ldots, v_{m-1}\}$ of $\mathbb{F}_{2^n}$ and rewrite x and y as vectors which will give us m nonlinear polynomial equations of the form:

$$\sum a_{ijk}x_ix_jx_k + \sum b_{ij}x_ix_j + \sum(c_{ij} + Tr(v))x_iy_j + \sum(d_k + Tr(v))y_k + \sum(e_k + Tr(v))x_k + f_l = 0$$

where a_{ij}, b_{ij}, c_k, d_k, e_k and f_l are elements in $\mathbb{F}_2$ and $Tr(v) \in \{0,1\}$.

4.3.2 Secret Key

The invertible transformations (s,t) and the field elements α, β and γ are the secret keys.

4.3.3 Encryption

If Bob wants to send a message $x = (x_0, \ldots, x_{m-1})$ to Alice, he does the following:

1. Bob substitues the plaintext $x = (x_0, \ldots, x_{m-1})$ and $Tr(v) = 0$ in public key and gets n linear equations in ciphertext variables $y_0, \ldots, y_{m-1}$. Bob then solve those linear equations by Gaussian elimination and get $y' = (y'_0, \ldots, y'_{m-1})$.

2. Bob then repeats the same process letting $Tr(v) = 1$ this time and gets m linear equations that he will solve to get $y" = (y"_0, \ldots, y"_{m-1})$.

3. The ordered pair $(y', y")$ is the required ciphertext.

4.3.4 Decryption

Alice knows the ciphertext $(y', y")$ and the secret parameters $(s, t, \alpha, \beta, \gamma)$. In order to retrieve the original message, she will use the following algorithm:

1. $v_1 \leftarrow t(y')$ and $v_2 \leftarrow t(y")$.

2. $z_1 \leftarrow L_\beta(v_1) + \gamma$ and $z_2 \leftarrow L_\beta(v_2) + \gamma$

3. $z'_3 \leftarrow (z_1)^{2m-1}$ and $z'_4 \leftarrow (z_2)^{2^m-1}$

4. $z_3 \leftarrow z'_3 + Tr(v_1)$ and $z_4 \leftarrow z'_4 + Tr(v_2)$

5. $z_5 \leftarrow z_3^{2m} + z_3 + \alpha + 1$ and $z_6 \leftarrow z_4^{2m} + z_4 + \alpha + 1$

6. $z_7 \leftarrow z_5^{2m-1}$ and $z_8 \leftarrow z_6^{2m-1}$

7. $O_1 \leftarrow s^{-1}(z_3 + 1)$, $O_2 \leftarrow s^{-1}(z_4 + 1)$, $O_3 \leftarrow s^{-1}(z_3 + z_7 + 1)$ and $O_4 \leftarrow s^{-1}(z_4 + z_8 + 1)$

8. return (O_1, O_2, O_3, O_4)

Out of the four messages Alice retrieved one of them will be the correct message, which is easily identifiable.

Example 21. *Let's consider the finite field $\mathbb{F}_{2^3}$ where $n = 2$ and $m = 3$. Let $x^3 + x + 1$ the irreducible polynomial over $\mathbb{F}_2$. Suppose v is the root of the above polynomial in the extension field of $\mathbb{F}_2$. v is such $v^3 + v + 1 = 0$. Using the basis $\{1, v, v^2\}$ the element of the finite field $\mathbb{F}_{2^3}$ can be expressed as $\mathbb{F}_{2^3} = \{0, 1, v, v^2, 1+v, 1+v^2, v+v^2, 1+v+v^2\}$. Bob will now take $\alpha = \gamma = 1 + v + v^2$ and $\beta = 1 + v$. Corresponding to $\beta = 1 + v = (1, 1, 0)$, $L_\beta = x + x^2$. He will also take the invertible transformation $s(x) = A_1 x + c_1$ and $t(x) = A_2 x + c_2$, where:*

$$A_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, c_1 = (1,0,1)^T \, c_2 = (0,1,0)^T$$

Suppose $x \in \mathbb{F}_{2^3}$, then x can be expressed as $x = x_0 + x_1 v + x_2 v^2$, where $x_i \in \mathbb{F}_2$. Taking $x = (x_0, x_1, x_2)^T$, we have:

$$A_1 x + c_1 = (x_0 + x_1 + 1, x_1 + x_2, x_2 + 1)^T$$

and

$$A_2 x + c_2 = (x_0 + x_1 + x_2, x_1 + x_2 + 1, x_2)^T$$

For the plaintext variable $x = (x_0, x_1, x_2)$ the corresponding ciphertext variable is $y = (y_0, y_1, y_2)$. We have:

$$u = (x_0 + x_1 + 1) + (x_1 + x_2)v + (x_2 + 1)v^2$$

and

$$v = (y_0 + y_1 + y_2) + (y_1 + y_2 + 1)v + y_2 v^2$$

The relation between the plaintext and the ciphertext is:

$$(u^{2^n} + u + \alpha)^{2^n}(L_\beta(v) + \gamma) + u(u^{2^n} + u + \alpha)(L_\beta(v) + \gamma) + (u^{2^n} + u + \alpha)(L_\beta(v) + \gamma)^{2^n} +$$

$$Tr(v)(u^{2^n} + u + \alpha)(L_\beta(v) + \gamma) = 0$$

By substitution we get the following relation between the plaintext and thhe ciphertext:

$$1 + Tr(v) + (1 + Tr(v))x_2y_2 + (1 + Tr(v))x_2y_1 + Tr(v)x_1y_1 + x_0 + y_1 + x_1x_2 + x_0x_1y_1 + x_0x_2y_1 + x_0x_2y_2 = 0,$$

$$x_1 + (Tr(v) + 1)y_1 + y_2 + Tr(v)x_2 + Tr(v)x_2y_1 + (Tr(v) + 1)x_2y_2 + Tr(v)x_1y_2 + x_0x_2 + x_0y_1 +$$
$$x_0x_2y_2 + x_0x_1y_1 + x_1y_1 + x_1x_2y_2 = 0,$$
$$1 + x_2 + (Tr(v) + 1)y_2 + Tr(v)x_1 + Tr(v)y_1 + (Tr(v) + 1)x_1y_1 + Tr(v)x_1y_2 + (Tr(v) + 1)x_2y_1 +$$
$$x_2y_2 + x_0x_1 + x_0y_1 + x_0y_2 + x_0x_1y_1 + x_0x_1y_2 + x_0x_2y_1 + x_1x_2y_1 = 0.$$

The above equations represent the public key.

4.4 Key Exchange based on Dickson Polynomials

A key exchange is a protocol whereby a shared secret becomes available to two parties. A method used to share cryptographic keys between two or more parties to allow them to secure their communication.The security of such scheme relies on the difficulty of solving the discrete logarithm problem, in other words, given α and a non zero element g the difficulty of finding an integer k such that $\alpha^k = g$. We will, in this section, introduce two cryptosystems similar to the Diffie-Hellman key exchange algorithm based on Dickson polynomials.

4.4.1 Diffie-Hellman Key Exchange

It is one of the most important developments in public key cryptography and it is still used nowadays in various security protocols. It was first introduced by Diffie and Hellman in 1976 allowing two parties with no communication background to securely establish a key which they can use to secure their communications. This key-exchange process works as follow:

- Alice and Bob agree to use two public integers modulo a prime p and and a base g where g is a primitive root modulo p.
- Alice chooses a secret integer a and computes $A \equiv g^a \mod p$ and so does Bob with an integer b as he will be computing $B \equiv g^b \mod p$, and send it to each other.
- Alice will then compute $B^a \mod p$ and Bob computes $A^b \mod p$. They will then both share the same key.

This key can then be used to encrypt ongoing communications. ElGamal cryptosystem is one of the encryption based on the Diffie-Hellman key exchange.

4.4.2 New Version of the Diffie-Hellman Key Exchange

We will see the steps of an analogue of the Diffie-Hellman Key-exchange scheme, that works as follow:

1. Alice and Bob agree on a finite field $\mathbb{F}_q$, and a generator g in $\mathbb{F}_q$.
2. Alice picks a secret integer a in $[0, q^2-1]$ and Bob picks a secret integer b in $[0, q^2-1]$.
3. Alice computes $A_k = D_a(g,1)$ and publishes it and so does Bob with $B_k = D_b(g,1)$.
4. Alice will compute $C_k = D_a(B_k,1) = D_a(D_b(g,1),1) = D_{ab}(g,1)$ wich will be the common key as when Bob computes $D_b(A_k,1) = D_b(D_a(g,1),1) = D_{ba}(g,1) = D_{ab}(g,1)$ he gets the same value C_k.

The shared secret is then C_k.

4.4.3 Key Exchange Scheme

In this section, a scheme using Dickson polynomials and hashing functions will be introduce. We will first define hash functions, then state the steps of the cryptographic scheme.

A glimpse on hash functions

A hash function takes an arbitrary length input as a message or a file and produces a fixed length output. Note that hashing the same input will produce the same digest (hash). One major property of hash functions is that one can not revert the algorithm, in other words, we shouldn't be able to find the input from just the output, we say that they are one-way.

Hash function are usually used in applied cryptography to provide specific security properties such as pre-image resistance that was mentioned above, the second pre-image resistance that is if given an input and its digest one won't be able to find a different input that hashes to the same digest. And the collision-resistance which guarantees that no one should be able to produce two different inputs that hash to the same output.

Hash functions in practice a rarely used alone, as they are mostly combined with other elements to create a cryptographic protocol, which we will see below.

Scheme

Based on what seen above, we can now construct a key exchange protocol similarly to the on of Diffie-Hellman algorithm, where Alice and Bob try to share a common key, which will work as follow:

1. Alice and Bob agree on a Hash function H and share the hash value $h = H(id_A||id_B||\beta||\alpha)$ (the symbol $||$ refers to concatenation, the operation of joining two strings together) where id_A and id_B are Alice and Bob's identity numbers, α and β are Alice and Bob's private key respectively.

2. Alice chooses a random integer a and a nonce (random number only used once) n_A, and then computes $AK_1 = H(h||a||n_A||id_A)$ and sends AK_1, a, n_A along with id_A to Bob.

3. Bob computes $AK_1' = H(h||a||n_A||id_A)$, compares whether $AK_1 = AK_1'$, if not, Bob stops the exchange, otherwise Alice is authenticated and he moves to the next step.

4. Bob chooses a random integer b and a random nonce n_B and computes $BK_2 = H(h||b||n_B||id_B)$ and sends BK_2, b, n_B along with id_B to Alice.

5. Alice computes $BK_2' = H(h||b||n_B||id_B)$, compares whether $BK_2 = BK_2'$, if not, Alice stops the exchange, otherwise Bob is authenticated and she moves to the next step.

6. Alice computes $m = ab$, $x_0 = (a+b) \mod 2^n$ then chooses an odd integer o_A and computes $X_A = D_{0_A}(x_0, 1) \mod 2^n$ (a permutation polynomial by *Theorem* 2.6) along with $AK_3 = H(h||n_B)$ and sends them to Bob.

7. Bob computes $n = ab$, $x_0 = (a+b) \mod 2^n$ then chooses an odd integer o_B and computes $X_B = D_{0_B}(x_0, 1) \mod 2^n$, along with $BK_4 = H(h||n_A)$ and sends them to Alice.

8. Alice computes $AK_4' = H(h||n_A)$ and compares whether the $AK_4 = AK_4'$ if the relation holds Alice computes the secret key as $CK \equiv D_{o_A}(X_B, 1) \mod 2^n$.

9. Bob computes $AK_3' = H = (h||n_B)$ and compares whether the $AK_3 = AK_3'$ if the relation holds Alice computes the secret key as $CK \equiv D_{o_B}(X_A, 1) \mod 2^n$.

Bob and Alice now share a common key which will insure them to communicate securely, the algorithm above can also be used to secure transmission between a person and a server.

BIBLIOGRAPHY

[1] D. Q. Wan, Permutation polynomials over finite fields, Acta Math. Sinica (N.S) 3, 1987.

[2] L. Carlitz, J. A. Lutz, A characterization of permutation polynomials over a finite field, The American Math. Monthly 85, 1978.

[3] L. Wang, On permutation polynomials, Finite Fields Appl. 8, 2002.

[4] M. Ayad, K. Belghaba, O. Kihel, On permutation binomials over finite fields, Bull. Austral. Math. Soc 89 (1), 2014.

[5] M. Zieve, Some families of permutation polynomials over finite fields, Int. J. Number Theroty 4, 2008.

[6] N. Bourbaki, Elements de Mathematiques, Algèbre Commutative, Springer.

[7] P. Wei, X. Liao, K. Wong, Key Exchange based on Dickson Polynomials over Finite Field with 2^m, China, 2011.

[8] R. Lidlm G. L. Mullen, Does a polynomial permute the elements of the field ?, The American Math, Monthly 95, 1988.

[9] R.Lidl, H. Niederreiter, Finite Fields, second ed., Encyclopedia of Mathematics and Applications, vol.20, Cambridge University Press, Cambridge, 1997.

[10] R. Singh, Permutation Polynomials and Their Application in Cryptography, Indian Institute of Technology, India, 2010.

[11] Y. Laigle-Chapuy, Pôlynomes de permutations et application en cryptographie, Cryptanalyse de registre combinés, 2009.