A New Algebraic Method to Search Irreducible Polynomials Using
Decimal Equivalents of Polynomials over Galois Field GF(p^q)

Sankhanil Dey¹ and Ranjan Ghosh²
Institute of Radio Physics and Electronics
University of Calcutta, 92 A. P. C. Road, Kolkata – 700 009
¹ sankhanil12009@gmail.com, ²rghosh47@yahoo.co.in

Abstract. Irreducible polynomials play an important role till now, in construction of 8-bit S-Boxes in ciphers. The 8-bit S-Box of Advanced Encryption Standard is a list of decimal equivalents of Multiplicative Inverses (MI) of all the elemental polynomials of a monic irreducible polynomial over Galois Field GF(2^8) [1]. In this paper a new method to search monic Irreducible Polynomials (IPs) over Galois fields GF(p^q) has been introduced. Here the decimal equivalents of each monic elemental polynomial (ep), two at a time, are split into the p-nary coefficients of each term, of those two monic elemental polynomials. From those coefficients the p-nary coefficients of the resultant monic basic polynomials (BP) have been obtained. The decimal equivalents of resultant basic polynomials with p-nary coefficients are treated as decimal equivalents of the monic reducible polynomials, since monic reducible polynomials must have two monic elemental polynomials as its factor. The decimal equivalents of polynomials belonging to the list of reducible polynomials are cancelled leaving behind the monic irreducible polynomials. A non-monic irreducible polynomial is computed by multiplying a monic irreducible polynomial by \( \alpha \) where \( \alpha \in GF(p^q) \) and assumes values from 2 to (p-1).

General Terms: Algorithms, Irreducible polynomial.
Keywords: Finite field, Galois field, Irreducible polynomials, Decimal Equivalents.

1. Introduction:

A basic polynomial BP(x) over finite field or Galois Field GF(p^q) is expressed as,

\[ BP(x) = a_q x^q + a_{q-1} x^{q-1} + \ldots + a_1 x + a_0 \]

B(x) has (q+1) terms, where \( a_q \) is non-zero and is termed as the leading coefficient [2]. A polynomial is monic if \( a_q \) is unity, else it is non-monic. The GF(p^q) have \( (p^q - p) \) elemental polynomials ep(x) ranging from p to \( (p^q - 1) \) each of whose representation involves q terms with leading coefficient \( a_{q-1} \). The expression of ep(x) is written as,

\[ ep(x) = a_{q-1} x^{q-1} + \ldots + a_1 x + a_0 , \text{ where } a_1 \text{ to } a_{q-1} \text{ are not simultaneously zero.} \]

Many of BP(x), which has an elemental polynomial as a factor under GF(p^q), are termed as reducible. Those of the BP(x) that have no factors are termed as irreducible polynomials IP(x) [3][4] and is expressed as,

\[ IP(x) = a_q x^q + a_{q-1} x^{q-1} + \ldots + a_1 x + a_0 , \text{ where } a_q \neq 0. \]

In Galois field GF(p^q), the decimal equivalents of the basic polynomials of extension q vary from p^q to \( (p^{q+1} - 1) \) while the elemental polynomials are those with decimal equivalents varying from p to \( (p^q - 1) \). Some of the monic basic polynomials are irreducible, since it has no monic elemental polynomial as a factor. The method in this paper is to look for the decimal equivalents of the reducible polynomials with multiplication, addition and modulus, of the p-nary coefficients of each term of each two monic elemental polynomials to obtain the decimal equivalent of the p-nary coefficients of each term of the resultant monic basic polynomial. The resultant monic basic polynomials are termed as reducible polynomials, since it is the product of two monic elemental polynomials. The polynomials belonging to the list of reducible polynomials are cancelled leaving behind the monic irreducible polynomials. A non-monic irreducible polynomial is computed by multiplying a monic irreducible polynomial by \( \alpha \) where \( \alpha \in GF(p) \) and assumes values from 2 to (p-1). In literatures, to the best knowledge of the present authors, there is no
mention of a paper in which the composite polynomial method is translated into an algorithm and in turn into a
computer program.

Since 1967 researchers took algorithmic initiatives, followed by computational time-complexity analysis, to
factorize basic polynomials on GF(p⁹) with a view to get irreducible polynomials, many of them are probabilistic
[3][6][7][8] in nature and few of them are deterministic [9][10]. One may note that the deterministic algorithms are
able to find all irreducible polynomials, while the probabilistic ones are able to find many, but not all. The
irreducible polynomial over GF(2⁸) was first used in cryptography for designing an invertible 8-bit S-Box of AES
[11][12][13]. The technique involves finding all multiplicative inverses under an irreducible polynomial is available
in [14][15][16][17].

For convenient understanding, the proposed algebraic method is presented in Sec. 2 for p=7 with q=7. The
method can find all monic and non-monic irreducible polynomials IP(x) over GF(7⁷). Sec. 3 is demonstrates the
obtained results to show that the proposed searching algorithm is actually able to search for any extension of the
Galois field with any prime of GF(p⁹), where p= 3, 5, 7,...,101,...p and q= 2, 3, 5, 7,...,101,...,q. In Sec.4 and 5, the
conclusion of the paper and the references are illustrated. A sample list of the decimal equivalents of the monic
irreducible polynomials over Galois Field GF(7⁷) is given in Appendix.

2 Algebraic method to find Irreducible Polynomials over GF(p⁹)

The basic idea of the algebraic method is to split the decimal equivalents of each monic elemental polynomial of a
monic Basic Polynomial, any two at a time, into p-nary coefficients of each term of those monic elemental
polynomials. Then multiply the p-nary coefficients to obtain each coefficients of the term with equal degree of each
term of monic basic polynomials. All the multiplied results are then added to obtain the decimal coefficients of each
term of the resultant monic basic polynomial. The decimal coefficients of each term of resultant monic basic
polynomial are then reduced to p-nary coefficients of each term of that polynomial. The decimal equivalents of
resultant monic basic polynomials with p-nary coefficients of each term are the decimal equivalents of the monic
reducible polynomials since it has two monic elemental polynomials as its factor. The polynomials belonging to the
list of monic reducible polynomials are cancelled leaving behind the monic irreducible polynomials. A non-monic
irreducible polynomial is computed by multiplying a monic irreducible polynomial by \( \alpha \) where \( \alpha \in \text{GF}(p) \) and
assumes values from 2 to (p-1). The algebraic method to find the monic Irreducible polynomial over GF(7⁷) is
demonstrated in section 2.2 and the extension to any Galois Field GF(p⁹) is described in section 2.2. The general
method to develop each block of the algorithm of the algebraic method is demonstrated in section 2.3. The pseudo
code for the above algebraic method is described in section 2.4.

2.1 Algebraic method to find Irreducible Polynomials over Galois Field GF(7⁷).

Here the interest is to find the monic irreducible polynomials over Galois Field or GF(7⁷).where p=7 is the
prime field and q=7 is the extension of that prime field. Since the indices of multiplicand and multiplier are added to
obtain the product. The extension q=7 can be demonstrated as a sum of two integers \( d_1 \) and \( d_2 \). The degree of highest
degree term present in elemental polynomials of GF(7⁷) is (q-1) = 6 to 1, since the polynomials with highest degree
term 0, are constant polynomials and they do not play any significant role here, so they are neglected. Hence the
two set of monic elemental polynomials for which the multiplication is a monic basic polynomial where p=7, q=7,
have the degree of highest degree terms \( d_1, d_2 \) where, \( d_1=1,2,3 \), and the corresponding values of \( d_2 \) are, 6,5,4.
Number of coefficients in the monic basic polynomial \( BP = (q+1)= (7+1) =8 \); they are defined as \( BP_0, BP_1, BP_2, BP_3, BP_4, BP_5, BP_6, BP_7 \); the value of the suffix also indicates the degree of the term of the monic basic polynomial. For
monic polynomials \( BP_7= 1 \). Total number of blocks is the number of integers in \( d_1 \) or \( d_2 \), i.e. 3 for this case.
Coefficients of each term in the 1st monic elemental polynomial $EP^0$ where, $d_1=1$; are defined as $EP^0_0$, $EP^0_1$. Coefficients of each term in the 2nd monic elemental polynomial $EP^1$ where $d_2=6$; are defined as $EP^0_1$, $EP^1_1$, $EP^2_1$, $EP^3_1$, $EP^4_1$, $EP^5_1$. The value in suffix also gives the degree of the term of the monic elemental polynomials.

Now, the algebraic method is as follows,

1st block:

$$BP_0 = (EP^0_0 \times EP^0_1) \% 7.$$  
$$BP_1 = (EP^0_0 \times EP^1_1 + EP^1_0 \times EP^0_1) \% 7.$$  
$$BP_2 = (EP^0_0 \times EP^2_1 + EP^1_0 \times EP^1_1) \% 7.$$  
$$BP_3 = (EP^0_0 \times EP^3_1 + EP^1_0 \times EP^2_1) \% 7.$$  
$$BP_4 = (EP^0_0 \times EP^4_1 + EP^1_0 \times EP^3_1) \% 7.$$  
$$BP_5 = (EP^0_0 \times EP^5_1 + EP^1_0 \times EP^4_1 + EP^2_0 \times EP^3_1) \% 7.$$  
$$BP_6 = (EP^0_0 \times EP^6_1 + EP^1_0 \times EP^5_1 + EP^2_0 \times EP^4_1 + EP^3_0 \times EP^3_1 + EP^4_0 \times EP^2_1 + EP^5_0 \times EP^1_1 + EP^6_0 \times EP^0_1) \% 7.$$  
$$BP_7 = (EP^1_0 \times EP^6_1) \% 7 = 1.$$  

Now the given basic monic polynomial is,

$$BP(x) = BP_7 x^7 + BP_6 x^6 + BP_5 x^5 + BP_4 x^4 + BP_3 x^3 + BP_2 x^2 + BP_1 x^1 + BP_0 x^0.$$  

Decm_eqv(BP(x)) = $BP_7 \times 7^7 + BP_6 \times 7^6 + BP_5 \times 7^5 + BP_4 \times 7^4 + BP_3 \times 7^3 + BP_2 \times 7^2 + BP_1 \times 7^1 + BP_0 \times 7^0.$

Coefficients of each term in the 1st monic elemental polynomial $EP^0$ where, $d_1=2$; are defined as $EP^0_0$, $EP^0_1$, $EP^1_0$. Coefficients of each term in the 2nd monic elemental polynomial $EP^1$ where $d_2=5$; are defined as $EP^0_1$, $EP^1_1$, $EP^2_1$, $EP^3_1$, $EP^4_1$, $EP^5_1$. The value in suffix also gives the degree of the term of the monic elemental polynomials.

Now, the algebraic method is as follows,

2nd block:

$$BP_0 = (EP^0_0 \times EP^0_1) \% 7.$$  
$$BP_1 = (EP^0_0 \times EP^1_1 + EP^1_0 \times EP^0_1) \% 7.$$  
$$BP_2 = (EP^0_0 \times EP^2_1 + EP^1_0 \times EP^1_1) \% 7.$$  
$$BP_3 = (EP^0_0 \times EP^3_1 + EP^1_0 \times EP^2_1 + EP^2_0 \times EP^3_1) \% 7.$$  
$$BP_4 = (EP^0_0 \times EP^4_1 + EP^1_0 \times EP^3_1 + EP^2_0 \times EP^4_1) \% 7.$$  
$$BP_5 = (EP^0_0 \times EP^5_1 + EP^1_0 \times EP^4_1 + EP^2_0 \times EP^5_1) \% 7.$$  
$$BP_6 = (EP^0_0 \times EP^6_1 + EP^1_0 \times EP^5_1 + EP^2_0 \times EP^6_1 + EP^3_0 \times EP^6_1 + EP^4_0 \times EP^5_1 + EP^5_0 \times EP^3_1 + EP^6_0 \times EP^2_1 + EP^7_0 \times EP^0_1) \% 7.$$  
$$BP_7 = (EP^1_0 \times EP^6_1 + EP^2_0 \times EP^5_1 + EP^3_0 \times EP^4_1 + EP^4_0 \times EP^3_1 + EP^5_0 \times EP^2_1 + EP^6_0 \times EP^1_1 + EP^7_0 \times EP^0_1) \% 7 = 1.$$  

Now the given basic monic polynomial is,

$$BP(x) = BP_7 x^7 + BP_6 x^6 + BP_5 x^5 + BP_4 x^4 + BP_3 x^3 + BP_2 x^2 + BP_1 x^1 + BP_0 x^0.$$  

Decm_eqv(BP(x)) = $BP_7 \times 7^7 + BP_6 \times 7^6 + BP_5 \times 7^5 + BP_4 \times 7^4 + BP_3 \times 7^3 + BP_2 \times 7^2 + BP_1 \times 7^1 + BP_0 \times 7^0.$

Coefficients of each term in the 1st monic elemental polynomial $EP^0$ where, $d_1=3$; are defined as $EP^0_0$, $EP^0_1$, $EP^1_0$. Coefficients of each term in the 2nd monic elemental polynomial $EP^1$ where $d_2=4$; are defined as $EP^0_1$, $EP^1_1$, $EP^2_1$, $EP^3_1$, $EP^4_1$. The value in suffix also gives the degree of the term of the monic elemental polynomials.

Now, the algebraic method is as follows,

3rd block:

$$BP_0 = (EP^0_0 \times EP^0_1) \% 7.$$  
$$BP_1 = (EP^0_0 \times EP^1_1 + EP^1_0 \times EP^0_1) \% 7.$$  
$$BP_2 = (EP^0_0 \times EP^2_1 + EP^1_0 \times EP^1_1) \% 7.$$  
$$BP_3 = (EP^0_0 \times EP^3_1 + EP^1_0 \times EP^2_1 + EP^2_0 \times EP^3_1 + EP^3_0 \times EP^0_1) \% 7.$$  
$$BP_4 = (EP^0_0 \times EP^4_1 + EP^1_0 \times EP^3_1 + EP^3_0 \times EP^1_1 + EP^4_0 \times EP^0_1) \% 7.$$  
$$BP_5 = (EP^0_0 \times EP^5_1 + EP^1_0 \times EP^4_1 + EP^3_0 \times EP^3_1) \% 7.$$  
$$BP_6 = (EP^0_0 \times EP^6_1 + EP^1_0 \times EP^5_1 + EP^3_0 \times EP^4_1) \% 7.$$  
$$BP_7 = (EP^1_0 \times EP^6_1) \% 7 = 1.$$  

Now the given basic monic polynomial is,
In this way the decimal equivalents of all the monic basic polynomials or monic reducible polynomials are pointed out. The polynomials belonging to the list of reducible polynomials are cancelled leaving behind the irreducible polynomials. Non-monic irreducible polynomials are computed by multiplying a monic irreducible polynomial by $\alpha$ where $\alpha \in \text{GF}(p)$ and assumes values from 2 to 6.

2.2 General Algebraic method to find Irreducible Polynomials over Galois Field $\text{GF}(p^q)$.

Here the interest is to find the monic irreducible polynomials over Galois Field $\text{GF}(p^q)$, where $p$ is the prime field and $q$ is the extension of the field. Since the indices of multiplicand and multiplier are added to obtain the product. The extension $q$ can be demonstrated as a sum of two integers, $d_1$ and $d_2$. The degree of highest degree term present in elemental polynomials of $\text{GF}(p^q)$ is $(q-1)$ to 1, since the polynomials with highest degree of term 0, are constant polynomials and they do not play any significant role here, so they are neglected. Hence the two set of monic elemental polynomials for which the multiplication is a monic basic polynomial, have the degree of highest degree terms $d_1$, $d_2$ where, $d_1=1,2,3,...,(q/2-1)$ and the corresponding values of $d_2$ are, $(q-1), (q-2), (q-3),...,q-(q/2-1)$. Number of coefficients in the monic basic polynomial $BP = (q+1)$; they are defined as $BP_0, BP_1, BP_2, BP_3, BP_4, BP_5, BP_6, BP_7,......, BP_q$, the value of the suffix also indicates the degree of the term of the monic basic polynomial. For monic polynomials $BP_0 = 1$.

Coefficients of each term in the 1st monic elemental polynomial $EP_i^0$, where, $d_1=1,2,3,...,(q/2-1)$; are defined as $EP_i^0, EP_i^{0-1}, EP_i^{0-2}, EP_i^{0-3}, EP_i^{0-4}, EP_i^{0-5}$. Coefficients of each term in the 2nd monic elemental polynomial $EP_i^1$ where $d_2= (q-1), (q-2), (q-3),...,q-(q/2-1)$; are defined as $EP_i^1, EP_i^{1-1}, EP_i^{1-2}, EP_i^{1-3}, EP_i^{1-4}, EP_i^{1-5}$. The value in suffix also gives the degree of the term of the monic elemental polynomials. Total number of blocks is the number of integers in $d_1$ or $d_2$, i.e. $(q/2-1)$ for this example.

Now, the algebraic method for $(q/2-1)^{th}$ block is as follows,

(q/2-1)th block:

\[
\begin{align*}
BP_0 &= (EP_0^0 \cdot EP_0^1) \mod p. \\
BP_1 &= (EP_1^0 \cdot EP_1^1 + EP_1^0 \cdot EP_0^1) \mod p. \\
BP_2 &= (EP_2^0 \cdot EP_2^1 + EP_2^0 \cdot EP_1^1 + EP_2^0 \cdot EP_0^1) \mod p. \\
BP_3 &= (EP_3^0 \cdot EP_3^1 + EP_3^0 \cdot EP_2^1 + EP_3^0 \cdot EP_1^1 + EP_3^0 \cdot EP_0^1) \mod p. \\
\vdots & \vdots \\
BP_{q-1} &= (EP_{(q/2-1)}^0 \cdot EP_{(q/2-1)}^1 + EP_{(q/2-1)}^0 \cdot EP_{(q/2-1)}^2 + \ldots + EP_{(q/2-1)}^0 \cdot EP_{(q/2-1)}^{q-(q/2-1)}) \mod p. \\
BP_q &= (EP_{q-(q/2-1)}^0 \cdot EP_{q-(q/2-1)}^1) \mod p.
\end{align*}
\]

Now the given basic monic polynomial is,

\[
BP(x) = BP_q x^q + BP_{q-1} x^{q-1} + \ldots + BP_5 x^5 + BP_4 x^4 + BP_3 x^3 + BP_2 x^2 + BP_1 x + BP_0 = 0.
\]

Decm_eqv(BP(x)) = $BP_q \cdot p^q + BP_{q-1} \cdot p^{q-1} + \ldots + BP_5 \cdot p^5 + BP_4 \cdot p^4 + BP_3 \cdot p^3 + BP_2 \cdot p^2 + BP_1 \cdot p + BP_0 \cdot p^0$.

Similarly all the decimal equivalents of all the resultant basic polynomials or reducible polynomials for all $a$ and its corresponding $b$ values are calculated. The polynomials belonging to the list of reducible polynomials are cancelled leaving behind the irreducible polynomials. Non-monic irreducible polynomials are computed by multiplying a monic irreducible polynomial by $\alpha$ where $\alpha \in \text{GF}(p)$ and assumes values from 2 to $(p-1)$.

2.3 General Method to develop each block of the Algorithm of the New Algebraic Method.

Prime field: $p$
Extension of the field: $q$.
d_1 = 1,2,3,...,(q/2-1).
d_2 = (q-1), (q-2), (q-3),...,q-(q/2-1).
Number of terms in 1st elemental polynomial: \( N(d_1) \).
Number of terms in 2nd elemental polynomial: \( N(d_2) \).
Number of terms in Basic Polynomial: \( p \).
Coefficients of Basic polynomial: \( BP_{\text{indx}} \), where \( 1 < \text{indx} < p \)
Coefficients of Elemental polynomials: \( EP_{\text{indx}_i} \), where \( 1 < i < 2 \).

Here,

\[
N(d_1) = N(d_2) = \text{Total number of blocks.}
\]

Each coefficient of basic polynomial can be derived as follows,

\[
BP_{\text{indx}} = (\Sigma EP_{\text{indx}_1} \cdot p^1 + EP_{\text{indx}_2} \cdot p^2) \mod p \quad \text{(i)}
\]

where \( 1 < \text{indx} < p, 1 < \text{indx}_1 < (q/2-1), (q-1) > \text{indx}_2 > q-(q/2-1) \).

\( 0 < p \cdot N(d_1) - 1, 0 < p \cdot N(d_2) - 1, \) and \( \text{indx} = \text{indx}_1 + \text{indx}_2 \).

2.4. Pseudo code:

The pseudo code of the \((q/2-1)\)th block of above algebraic code for Galois Field \( GF(p^q) \) is described as follows, where \( \text{ep}[0] \) and \( \text{ep}[1] \) are the arrays of all possible decimal equivalents of 1st and 2nd monic elemental polynomials respectively. \( EP^0, EP^1 \) are the arrays consists of \( p \)-ary coefficients of 1st and 2nd monic elemental polynomials respectively. \( BP \) is the array consists of \( p \)-ary coefficients of the resultant monic basic polynomial. \( \text{Decm}_{eqv}(BP(x)) \) is the decimal equivalent of the resultant monic basic polynomial.

```plaintext
for (\text{ep}[0]=p..p^{q/2-1}, \text{ep}[1]=p^{q-1}..p^{q-(q/2-1)}; \text{ep}[0]<2\cdot p..p^{q/2-1}, \text{ep}[0]<2\cdot p^{q-1}..p^{q-(q/2-1)}; \text{ep}[0]++, \text{ep}[1]++) {
    for (\text{indx}[0]=\text{ep}[0]; \text{indx}[0]<2\cdot \text{ep}[0]; \text{indx}[0]++) {
        coeff_conv_1st_deg (\text{indx}[0], EP^0);
    }
    for (\text{indx}[1]=\text{ep}[1]; \text{indx}[1]<2\cdot \text{ep}[1]; \text{indx}[1]++) {
        coeff_conv_2nd_deg (\text{indx}[1], EP^1);
        BP_0 = (EP^0_0 \cdot EP^0_1) \mod p;
        BP_1 = (EP^0_0 \cdot EP^1_1 + EP^1_0 \cdot EP^0_1) \mod p;
        BP_2 = (EP^0_0 \cdot EP^2_1 + EP^2_0 \cdot EP^1_1 + EP^1_0 \cdot EP^2_1) \mod p;
        BP_3 = (EP^0_0 \cdot EP^3_1 + EP^3_0 \cdot EP^2_1 + EP^2_0 \cdot EP^3_1 + EP^3_0 \cdot EP^2_1) \mod p;
        ... 
        BP_{q-1} = (EP^0_{q-1} \cdot EP^1_{q-1} + EP^1_{q-1} \cdot EP^2_{q-1} + ... + EP^2_{q-1} \cdot EP^3_{q-1} + ... + EP^3_{q-1} \cdot EP^q_{q-1}) \mod p;
        BP_q = (EP^0_{q/2-1} \cdot EP^1_{q/2-1} + EP^1_{q/2-1} \cdot EP^2_{q/2-1} + ... + EP^2_{q/2-1} \cdot EP^3_{q/2-1} + ... + EP^3_{q/2-1} \cdot EP^q_{q/2-1}) \mod p;
        \text{BF}(x) = BP_0 \cdot x^p + BP_1 \cdot x^{p^2} + BP_2 \cdot x^{p^3} + ... + BP_q \cdot x^{p^q};
        \text{Decm}_{eqv}(\text{BF}(x)) = BP_0 \cdot p^0 + BP_1 \cdot p^1 + BP_2 \cdot p^2 + BP_3 \cdot p^3 + BP_4 \cdot p^4 + BP_5 \cdot p^5 + ... + BP_q \cdot p^q;
        \text{indx}[2]++;
    }
}
End for.
End for.
```

3. Results.

The algebraic method or the above pseudo code has been tested on \( GF(7^3), GF(11^3), GF(1013) \) and \( GF(7^5) \). Numbers of monic Irreducible polynomials are same as in hands on as well as previous calculations [18]. The list of Numbers of monic irreducible polynomials are given below for the above four Extended Galois Fields. The list of all Irreducible monic basic polynomials of four extended Galois fields are available in reference [19][20][21][22]. The Sample list of monic Irreducible Polynomial over \( GF(7^3) \) is given in Appendix and also available in the link given[23].

| GF    | GF(7^3) | GF(11^3) | GF(1013) | GF(7^5) |
|-------|---------|----------|----------|---------|
| Number of IP | 112     | 440      | 343400   | 5712    |
4. Conclusion.

To the best knowledge of the present authors, there is no mention of a paper in which the composite polynomial method is translated into an algorithm and turn into a computer program. The new algebraic method is a much simpler method similar to composite polynomial method to find monic irreducible polynomials over Galois Field GF(p^2). It is able to determine decimal equivalents of the monic irreducible polynomials over Galois Field with large value of prime, also with large extensions. So this method can reduce the complexity to find monic Irreducible Polynomials over Galois Field with large value of prime and also with large extensions of the prime field. So this would help the crypto community to build S-Boxes or ciphers using irreducible polynomials over Galois Fields with a large value of prime, also with the large extensions of the prime field.

5. References.

[1] Canright, D, “A very Compact S-box for AES”, Link: https://www.iacr.org/archive/ches2005/032.pdf.
[2] Lidl, R, Niederreiter, H, Finite Fields, Encyclopedia of Mathematics and its Applications, Vol. 20, Addison-Wesley Publishing Company, 1983.
[3] Church, R, “Tables of Irreducible Polynomials for the first four Prime Moduli”, Annals of Mathematics, Vol. 36(1), pp. 198 – 209, January, 1935.
[4] Chebolu, S.K, and Minac, J, “Counting Irreducible Polynomials over Finite Fields Using the Inclusion-Exclusion Principle”, Math. Mag., Vol. 84(5), pp. 369 – 371, 2011.
[5] Berlekamp, E, R, “Factoring Polynomials over finite fields”, Bell Syst. Tech. J., Vol. 46, pp. 1853 – 1859, 1967.
[6] Adleman, L M and Lenstra, H W, “Finding irreducible polynomials over finite fields”, Proc. 18th ACM Conf. on The Theory of Computing, Berkeley, CA, pp. 350 – 355, 1986.
[7] Cantor, D G, “On Arithmetical Algorithms over Finite Fields” J. Combinatorial Theory Series A 9, pp. 285 – 300 (1989).
[8] Bach, E and Shoup, V, “Factoring Polynomials using Random Bits”, J. Symbolic Computation, Vol 9, pp. 229 – 239, 1990.
[9] Berlekamp, E, R, “Factoring Polynomials over large finite fields”, Math. Comput. Vol. 24 (11), pp. 713 – 735, 1970.
[10] Shoup, V, “New algorithms for finding irreducible polynomials in finite fields”, Math. Comput. Vol. 54, pp. 435 – 447, 1990.
[11] Daemen, J, Rijmen, V, AES Proposal: Rijndael, AES Algorithm Submission, September 3, 1999.
[12] FIPS Pub. 197, “Announcing the Advanced Encryption Standard” (AES), November 26, 2001.
[13] Stinson, D.R, Cryptography Theory and Practice (Boca Raton, Chapman & Hall, CRC, 3rd Edition, 2006).
[14] Stallings, W, Cryptography and Network Security Principles and Practices, Delhi, Pearson Education, 4th Edition, 2008.
[15] Forouzan, B.A, Mukhopadhyay D., Cryptography and Network Security, New Delhi, TMH, 2nd Edition, 2011.
[16] Hasan, M.A, “Double-Basis Multiplicative Inversion Over GF(2^n)”, IEEE Trans. Comp., Vol. 47,(9), pp. 960 – 970, 1998.
[17] Arguello, F, “Lehmer-based algorithm for computing inverses in Galois fields GF(2^n)”, Electronics Letters, Vol. 42(5), 2006.
[18] Zaman, J, K, M, Sadique, Uz, Dey, Sankhanil, Ghosh, Ranjan, “An Algorithm to find the Irreducible Polynomials over Galois Field GF(p^n)”, International Journal of Computer Applications (0975 – 8887,) Volume 109 – No. 15, January 2015,pp-24-29.
[19] Dey, Sankhanil “The list of Decimal Equivalents of All the Monic Irreducible Polynomials over Galois Field GF(7^3)”, Link: https://www.academia.edu/15224792/The_list_of_Decimal_Equivalents_of_All_the_Monic_Irreducible_Polynomials_over_Galois_Field_GF_7_3_.
[20] Dey, Sankhanil “The list of Decimal Equivalents of All the Monic Irreducible Polynomials over Galois Field GF(11^3)”, Link: https://www.academia.edu/15224871/The_list_of_Decimal_Equivalents_of_All_the_Monic_Irreducible_Polynomials_over_Galois_Field_GF_11_3_.
[21] Dey, Sankhanil “The list of Decimal Equivalents of All the Monic Irreducible Polynomials over Galois Field GF(101^3)”, Link: https://www.academia.edu/15224878/The_list_of_Decimal_Equivalents_of_All_the_Monic_Irreducible_Polynomials_over_Galois_Field_GF_101_3_.
[22] Dey, Sankhanil “The list of Decimal Equivalents of All the Monic Irreducible Polynomials over Galois Field GF(7^5)”, Link: https://www.academia.edu/15224842/The_list_of_Decimal_Equivalents_of_All_the_Monic_Irreducible_Polynomials_over_Galois_Field_GF_7_5_.
[23] Dey, Sankhanil “The Sample list of Decimal Equivalents of the Monic Irreducible Polynomials over Galois Field GF(7^7)”, Link:https://www.academia.edu/15224866/A_sample_list_of_Decimal_Equivalents_of_the_Monic_Irreducible_Polynomials_over_Galois_Field_GF_7_7_.


A sample list of Decimal Equivalents of Monic Irreducible Polynomials over Galois Field GF(7^7) is given below.

| Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent | Decimal Equivalent |
|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|--------------------|
| 823586             | 823587             | 823588             | 823589             | 823590             | 823591             | 823592             | 823593             | 823594             | 823595             | 823596             | 823597             | 823598             | 823599             | 823600             | 823601             | 823602             | 823603             | 823604             | 823605             | 823606             | 823607             | 823608             | 823609             | 823610             | 823611             | 823612             | 823613             | 823614             | 823615             | 823616             | 823617             |
