An Algorithm to Find the Irreducible Polynomials Over Galois Field GF(pm)

Article *in* International Journal of Computer Applications · January 2015

DOI: 10.5120/19266-1012

3 authors, including:

Sankhanil Dey
University of Calcutta
33 PUBLICATIONS **26** CITATIONS
SEE PROFILE

Ranjan Ghosh
University of Calcutta
76 PUBLICATIONS **194** CITATIONS
SEE PROFILE

An Algorithm to find the Irreducible Polynomials over Galois Field GF(p^m)

J K M Sadique Uz Zaman
Department of Radio Physics and Electronics,
University of Calcutta,
Kolkata – 700009, India

Sankhanil Dey
Department of Radio Physics and Electronics,
University of Calcutta,
Kolkata – 700009, India

Ranjan Ghosh
Department of Radio Physics and Electronics,
University of Calcutta,
Kolkata – 700009, India

ABSTRACT
Irreducible Polynomials over GF(p^m) and the multiplicative inverses under it are important in cryptography. Presently the method of deriving irreducible polynomials of a particular prime modulus is very primitive and time consuming. In this paper, in order to find all irreducible polynomials, be it monic or non-monic, of all prime moduli p with all its order m, a fast deterministic computer algorithm based on an algebraic method producing a (m×m) matrix is proposed. The maximum number of terms in each column of the matrix is 2^j where j is the column index.

General Terms
Algorithms, Irreducible polynomial.

Keywords
Extended Finite field, Finite field, Galois field, GF(7^3), Irreducible polynomial, Multiplicative inverse.

1. INTRODUCTION
A basic polynomial B(x) over finite field or Galois Field GF(p^m) is expressed as,

$$B(x) = a_m x^m + a_{m-1}x^{m-1} + - - - + a_1x + a_0$$

B(x) has (m+1) terms, where a_m is non-zero and is termed as the leading coefficient [1]. A polynomial is monic if a_m is unity, else it is non-monic. A finite field GF(p^m) is called Extension field if m>1. The algorithm presented in this paper is true for Extension field.

The GF(p^m) have (p^m – p) elemental polynomials, b(x) ranging from p to (p^m – 1) each of whose representation involves m terms with leading coefficient a_{m-1}. The expression of b(x) is written as,

$$b(x) = a_{m-1}x^{m-1} + - - - + a_1x + a_0$$

where a_1 to a_{m-1} are not simultaneously zero.

Many of the B(x), which has an elemental polynomial, b(x) as a factor under GF(p^m), are termed as reducible. Those of the B(x) that have no factors are termed as irreducible polynomials I(x) and is expressed as [1], [2],

$$I(x) = a_m x^m + a_{m-1}x^{m-1} + - - - + a_1x + a_0 \text{ , where } a_m \neq 0.$$

Under GF(p^m), the basic polynomials of degree m vary from p^m to (p^{m+1} – 1) while the elemental polynomials are those varying from p to (p^m – 1). Some of the basic polynomials are irreducible, since it has no elemental polynomial as a factor. The conventional method to look for an irreducible polynomial is to systematically multiply two or more elemental polynomials under GF(p^m) and the composite product polynomials belonging to the list of basic polynomials are cancelled leaving behind the irreducible polynomials [1]. The task involves a tedious effort, happens to be severely time consuming and becomes herculean in nature with increasing values of p and m. Following the said method the monic irreducible polynomials for few values of p = 2, 3, 5 and 7 are listed in literatures [1], [2] where maximum values of m are taken respectively as 11, 7, 5 and 4.

It is mentioned in [3] that following Inclusion-Exclusion principle of Galois Field, a non-monic irreducible polynomial is computed by multiplying a monic irreducible polynomial by α 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(p^m) with a view to get irreducible polynomials, many of them are probabilistic [4], [5], [6], [7] in nature and few of them are deterministic [8], [9]. 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. However, the composite polynomial approach is a straightforward deterministic method, although time-consuming.

The irreducible polynomial over GF(2^8) was first used in cryptography for designing an invertible S-Box of AES [10], [11], [12]. The technique involves finding all multiplicative inverses under an irreducible polynomial is available in [13], [14], [15], [16].

In this paper we propose a computer algorithm based on an algebraic method which searches irreducible polynomials among basic polynomials over GF(p^m). The algorithm is deterministic since it is able to find all the irreducible polynomials over GF(p^m) in a short time.

For convenient understanding, the proposed algebraic method is presented in Sec. 2 for any value of p with m=3. The method can find all monic and non-monic irreducible polynomials I(x) of all B(x) over GF(p^m). In Sec. 3 it is demonstrated that the proposed searching algorithm actually searches much less number of elemental polynomials to find all the irreducible polynomials over GF(p^m). The conclusion is in Sec. 4.

2. ALGEBRAIC METHOD TO FIND IRREDUCIBLE POLYNOMIALS OVER GF(p^m)
The basic idea of the algebraic method is to form a k-matrix of order (m×m) involving coefficients of b(x) and B(x) based on an assumption that the multiplicative inverses of an elemental polynomial b(x) under a basic polynomial B(x) over GF(p^m) exists. If the determinant of the k-matrix, i.e. det(k), is non-zero for all the b(x), one can conclude that the polynomial B(x) is an irreducible polynomial I(x). In the

event the det(k) is zero at least for one b(x), the concerned B(x) is reducible. For better clarity of understanding, the generalized algebraic method for any value of p is worked out in Sec. 2.1 with m=3. The formation of k-matrix of order (3×3) is presented in Sec. 2.2 for m=3. One can also refer [17] for understanding of k-matrix. It is interesting to note that column-wise elements of the k-matrix have a generalized similar pattern for m – the patterns are presented in Sec.2.3 for $2 \leq m \leq 5$.

2.1 Algebraic Method to find Irreducible Polynomials over GF(p^m) with m=3

Here $B(x) = (a_3x^3 + a_2x^2 + a_1x + a_0)$ is a polynomial over $GF(7^3)$ and $b(x) = (b_2x^2 + b_1x + b_0)$ is an elemental polynomial under B(x). If $c(x) = (c_2x^2 + c_1x + c_0)$ is the multiplicative inverse of the polynomial b(x), one can write,

$$[b(x)\, c(x)] \bmod B(x) = 1$$

$$\text{or, } [(b_2x^2 + b_1x + b_0)(c_2x^2 + c_1x + c_0)] \bmod (a_3x^3 + a_2x^2 + a_1x + a_0) = 1 \quad (1)$$

Here, one can get the values for c_0, c_1 and c_2 by solving eq.(1) as follows:

$$[b_2c_2x^4 + (b_1c_2 + b_2c_1)x^3 + (b_0c_2 + b_1c_1 + b_2c_0)x^2 + (b_0c_1 + b_1c_0)x + b_0c_0] \bmod (a_3x^3 + a_2x^2 + a_1x + a_0) = 1$$

$$\text{or, } [a_3^{-1}b_2c_2x(a_3x^3 + a_2x^2 + a_1x + a_0) + (b_1c_2 + b_2c_1 - a_3^{-1}a_2b_2c_2)x^3 + (b_0c_2 + b_1c_1 + b_2c_0 - a_3^{-1}a_1b_2c_2)x^2 + (b_0c_1 + b_1c_0 - a_3^{-1}a_0b_2c_2)x + b_0c_0] \bmod (a_3x^3 + a_2x^2 + a_1x + a_0) = 1$$

$$\text{or, } [a_3^{-1}(b_1c_2 + b_2c_1 - a_3^{-1}a_2b_2c_2)(a_3x^3 + a_2x^2 + a_1x + a_0) + (b_0c_2 + b_1c_1 + b_2c_0 - a_3^{-1}a_1b_2c_2 - a_3^{-1}a_2b_1c_2 - a_3^{-1}a_2b_2c_1 + a_3^{-2}a_2^2b_2c_2)x^2 + (b_0c_1 + b_1c_0 - a_3^{-1}a_0b_2c_2 - a_3^{-1}a_1b_1c_2 - a_3^{-1}a_1b_2c_1 + a_3^{-2}a_1a_2b_2c_2)x + (b_0c_0 - a_3^{-1}a_0b_1c_2 - a_3^{-1}a_0b_2c_1 + a_3^{-2}a_0a_2b_2c_2)] \bmod (a_3x^3 + a_2x^2 + a_1x + a_0) = 1$$

$$\text{or, } [\{(a_3^{-2}a_2^2b_2 - a_3^{-1}a_1b_2 - a_3^{-1}a_2b_1 + b_0)c_2 + (b_1 - a_3^{-1}a_2b_2)c_1 + b_2c_0\}x^2 + \{(a_3^{-2}a_1a_2b_2 - a_3^{-1}a_0b_2 - a_3^{-1}a_1b_1)c_2 + (b_0 - a_3^{-1}a_1b_2)c_1 + b_1c_0\}x + \{(a_3^{-2}a_0a_2b_2 - a_3^{-1}a_0b_1)c_2 - a_3^{-1}a_0b_2c_1 + b_0c_0\}] \bmod (a_3x^3 + a_2x^2 + a_1x + a_0) = 1 \quad (2)$$

From eq.(2) it is evident that the dividend is smaller than the divisor. Hence to satisfy the required condition, i.e., the remainder = 1, in this equation the following properties must hold.

(i) The constant part $\equiv 1 \bmod p$.

(ii) The coefficients of $x \equiv 0 \bmod p$.

(iii) The coefficients of $x^2 \equiv 0 \bmod p$.

Therefore,

$$\{(a_3^{-2}a_0a_2b_2 - a_3^{-1}a_0b_1)c_2 - a_3^{-1}a_0b_2c_1 + b_0c_0\} \bmod p = 1 \quad (3a)$$

$$\{(a_3^{-2}a_1a_2b_2 - a_3^{-1}a_0b_2 - a_3^{-1}a_1b_1)c_2 + (b_0 - a_3^{-1}a_1b_2)c_1 + b_1c_0\} \bmod p = 0 \quad (3b)$$

$$\{(a_3^{-2}a_2^2b_2 - a_3^{-1}a_1b_2 - a_3^{-1}a_2b_1 + b_0)c_2 + (b_1 - a_3^{-1}a_2b_2)c_1 + b_2c_0\} \bmod p = 0 \quad (3c)$$

Rearranging terms as coefficients of c_0, c_1 and c_2, the eq. (3) becomes as follows after considering the fact that –1 is equivalent to (p – 1) in modular arithmetic with modulus p, since the algebra is being worked out in $GF(p^3)$:

$$[b_0c_0 + \{0 + (p-1)a_3^{-1}a_0b_2\}c_1 + \{0 + 0 + (p-1)a_3^{-1}a_0b_1 + a_3^{-2}a_0a_2b_2\}c_2] \bmod p = 1 \quad (4a)$$

$$[b_1c_0 + \{b_0 + (p-1)a_3^{-1}a_1b_2\}c_1 + \{0 + (p-1)a_3^{-1}a_0b_2 + (p-1)a_3^{-1}a_1b_1 + a_3^{-2}a_1a_2b_2\}c_2] \bmod p = 0 \quad (4b)$$

$$[b_2c_0 + \{b_1 + (p-1)a_3^{-1}a_2b_2\}c_1 + \{b_0 + (p-1)a_3^{-1}a_1b_2 + (p-1)a_3^{-1}a_2b_1 + a_3^{-2}a_2a_2b_2\}c_2] \bmod p = 0 \quad (4c)$$

2.2 Formation of (m×m) K-Matrix for m=3

In order to form k-matrix, the above eq.(4) can be written as,

$$(k_{00}c_0 + k_{01}c_1 + k_{02}c_2) \bmod p = 1 \quad (5a)$$

$$(k_{10}c_0 + k_{11}c_1 + k_{12}c_2) \bmod p = 0 \quad (5b)$$

$$(k_{20}c_0 + k_{21}c_1 + k_{22}c_2) \bmod p = 0 \quad (5c)$$

where k-values are known and these are equal to,

$$\left.\begin{aligned} k_{00} &= (b_0) \bmod p \\ k_{01} &= ((p-1)a_3^{-1}a_0b_2) \bmod p \\ k_{02} &= ((p-1)a_3^{-1}a_0b_1 + a_3^{-2}a_0a_2b_2) \bmod p \end{aligned}\right\} \quad (6a)$$

$$\left.\begin{aligned} k_{10} &= (b_1) \bmod p \\ k_{11} &= (b_0 + (p-1)a_3^{-1}a_1b_2) \bmod p \\ k_{12} &= ((p-1)a_3^{-1}a_0b_2 + (p-1)a_3^{-1}a_1b_1 + a_3^{-2}a_1a_2b_2) \bmod p \end{aligned}\right\} \quad (6b)$$

$$\left.\begin{aligned} k_{20} &= (b_2) \bmod p \\ k_{21} &= (b_1 + (p-1)a_3^{-1}a_2b_2) \bmod p \\ k_{22} &= (b_0 + (p-1)a_3^{-1}a_1b_2 + (p-1)a_3^{-1}a_2b_1 + a_3^{-2}a_2a_2b_2) \bmod p \end{aligned}\right\} \quad (6c)$$

The eq.(5) , i.e., $(k \times c) \bmod p = V$ can be solved by using matrix method as,

$$c = (k^{-1} \times V) \bmod p \quad (7)$$

where,

$$V = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad k = \begin{pmatrix} k_{00} & k_{01} & k_{02} \\ k_{10} & k_{11} & k_{12} \\ k_{20} & k_{21} & k_{22} \end{pmatrix} \quad (8a)$$

$$k^{-1} = \begin{pmatrix} ik_{00} & ik_{01} & ik_{02} \\ ik_{10} & ik_{11} & ik_{12} \\ ik_{20} & ik_{21} & ik_{22} \end{pmatrix}, \quad c = \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} ik_{00} \\ ik_{10} \\ ik_{20} \end{pmatrix} \quad (8b)$$

While calculating k^{-1} from k-matrix, one has to ensure that the determinant det(k) is non-zero. In the event det(k) = 0, the B(x) is a reducible polynomial and the multiplicative inverses of its elements does not exist. If det(k) is non-zero for all the elements, the B(x) is irreducible and the multiplicative inverses of elements exist. By calculating k^{-1} from k-matrix

given in eq.(8), one can get solution for c_0, c_1 and c_2. In such a case one can write,

$$(b_2 x^2 + b_1 x + b_0)^{-1} = (c_2 x^2 + c_1 x + c_0) \bmod (a_3 x^3 + a_2 x^2 + a_1 x + a_0)$$

2.3 Generalized Column-Wise Patterns of K-Matrix Elements

Following the workouts of the algebraic method for $2 \le m \le 5$ for the purpose of forming (m×m) k-matrix, if k_{ij} terms are organized in m columns with $0 \le \text{both}(i,j) \le (m-1)$, one notices algebraic similarities up to $(m-1)^{th}$ columns and a new term emerges in the m^{th} column. The k_{ij} terms for m = 5 are shown below,

1^{st} column (j=0):

$k_{ij} = b_{i-0.}$

2^{nd} column (j=1):

$k_{ij} = b_{i-1} + (-a_m^{-1}) [a_{i-0} b_{m-1}]$.

3^{rd} column (j=2):

$k_{ij} = b_{i-2} + (-a_m^{-1}) [a_{i-1} b_{m-1} + a_{i-0} b_{m-2}] + (-a_m^{-1})^2 [a_{i-0} a_{m-1} b_{m-1}]$.

4^{th} column (j=3):

$k_{ij} = b_{i-3} + (-a_m^{-1})[a_{i-2} b_{m-1} + a_{i-1} b_{m-2} + a_{i-0} b_{m-3}] + (-a_m^{-1})^2 [b_{m-1}\{a_{i-1} a_{m-1} + a_{i-0} a_{m-2}\} + a_{i-0} a_{m-1} b_{m-2}] + (-a_m^{-1})^3 [a_{i-0} a_{m-1} a_{m-1} b_{m-1}]$.

5^{th} column (j=4):

$k_{i4} = b_{i-4} + (-a_m^{-1}) [a_{i-3} b_{m-1} + a_{i-2} b_{m-2} + a_{i-1} b_{m-3} + a_{i-0} b_{m-4}] + (-a_m^{-1})^2 [b_{m-1}(a_{i-2} a_{m-1} + a_{i-1} a_{m-2} + a_{i-0} a_{m-3}) + b_{m-2}(a_{i-1} a_{m-1} + a_{i-0} a_{m-2}) + a_i a_{m-1} b_{m-3}] + (-a_m^{-1})^3 [a_{m-1} b_{m-1}(a_{i-1} a_{m-1} + a_{i-0} a_{m-2}) + a_i a_{m-1}(a_{m-2} b_{m-1} + a_{m-1} b_{m-2})] + (-a_m^{-1})^4 [a_{i-0}\, a_{m-1} a_{m-1} a_{m-1} b_{m-1}]$.

The similarities of k_{ij} expressions indicate, (1) First and second columns are respectively for 1^{st} and 2^{nd} columns for $2 \le m \le 5$, (2) Third column is the same for $3 \le m \le 5$, (3) Fourth column is also the same for $4 \le m \le 5$ and (4) Fifth column is for m = 5 only.

Notes:

(1) If suffix of any term in j^{th} column is negative, the concerned term is zero.

(2) In k-matrix, maximum number of terms in j^{th} column of $(m-1)^{th}$ row is 2^j.

3. IRREDUCIBLE POLYNOMIALS OVER GF(p^m): A SEARCHING ALGORITHM

From the algebraic method presented in Sec. 2, it is evident that one has to check the det(k) of the k-matrix for all the elemental polynomials b(x) for a particular B(x). It is interesting to note that in actual computation, one can serve the purpose by having necessary checks much lesser in number. The rationality of adopting reduced number of checks is presented in Sec. 3.1. The related pseudo-code of the program algorithm is described in Sec. 3.2.The results of computation of irreducible polynomials for first six prime moduli are given in Sec. 3.3.

3.1 Reduced Number of Checks over Elemental Polynomials

For B(x) over GF(7^3), there are 336 elemental polynomials from 7 to 342 out of which 7 to ($7^2 - 1$), i.e. 42 are linear and 7^2 to ($7^3 - 1$), i.e. 294 are quadratic, while the basic polynomials have 7^3 to (7^4 - 1), i.e. there are 2058 cubic polynomials. The reducible B(x) of degree 3 must be composed either of a product of a linear and a quadratic polynomial or of a product of three linear polynomials. Hence, it is sufficient if det(k) is checked for 42 times over linear elemental polynomials only. The B(x) over GF(7^4) are 4-degree polynomials and reducible B(x) must be composed of a product either of a linear and a cubic polynomials or of two quadratic polynomials or of four linear polynomials. Hence its reducibility checks can be limited only to linear and quadratic elemental polynomials. Considering the said feature, one can define a parameter r as,

$$r = \left\lfloor \frac{m}{2} \right\rfloor + 1$$

and keep the checks from p to ($p^r - 1$). It may be noted that for a particular B(x), b(x) is searched ($p^r - p$) number of times, instead of ($p^m - p$) and that the maximum degree of the factoring elemental polynomial b(x) to be checked is $\left\lfloor \frac{m}{2} \right\rfloor$.

3.2 Pseudo-Code of the Program Algorithm

A new algorithm is proposed in this paper to find the irreducible polynomials over GF(p^m) where p is a prime modulus and index m is an integer. The pseudo-code of the algorithm is given below.

Pseudo-code of proposed algorithm:

Inputs: p and m.

$$r = \left\lfloor \frac{m}{2} \right\rfloor + 1$$

For Bx = p^m to $p^{m+1} - 1$

Convert Bx into its equivalent p-base number and store them in an array a[ ] defined in eq.(1) where a_0 is the least significant digit.

For bx = p to $p^r - 1$

Convert the bx into its equivalent p-base number and store them in an array b[ ] defined in eq.(1) where b_0 is the least significant digit.

From arrays a[ ] and b[ ] form the (m×m) k-matrix described in eq.(8).

Calculate determinant of the k-matrix det(k).

If det(k) = 0

Current Bx is reducible.

Break.

Else

If bx = $p^r - 1$

Current Bx is irreducible.

End of bx

End of Bx

3.3 Results of Computation

The computation is undertaken for monic as well as non-monic irreducible polynomials for the first six prime moduli with m = 2, 3 and 4. It is observed that the results of monic irreducible polynomials for first four prime moduli are identical to what is given in [1], [2]. It is also observed that all the non-monic polynomials are in conformity with what is stated in [3]. For prime moduli 11 and 13, there is no mention of irreducible polynomials in literatures. The monic irreducible polynomials for p = 11 and 13 with m = 2, 3 and 4 are obtained and their results for p = 11 and 13 with m = 2 and 3 are given in Appendix A while the whole list are uploaded in [18]. Their non-monic polynomials are also found to be in conformity with what is stated in [3].

4. CONCLUSION

The proposed computer algorithm searching all irreducible polynomials over GF(p^m) is fast. The computation of 7098 monic irreducible polynomials from among 28561 basic monic polynomials over GF(13^4) is undertaken practically in no time in the computing system available to the authors (Pentium(R) 4 CPU, 2.00GHz, 768 MB of RAM, Windows XP Service Pack 2, Compiler Turbo C 3.0).

At present, for all irreducible polynomials with p=2, one can find multiplicative inverses of all elemental polynomials for all values of m following Extended Euclidean Algorithm (EEA). It is observed that for irreducible polynomials with p>2 one cannot find multiplicative inverses of all elemental polynomials using EEA [17]. With little modification, the proposed algorithm can find multiplicative inverses of all irreducible polynomials for p > 2 with any value of m.

In Sec. 2.3 the k_{ij} expressions are presented in five columns for m=5. Looking at the algebraic expression of the m^{th} column of a particular m and comparing it with that of the $(m-1)^{th}$ column of the previous m, it might be possible to predict the algebraic expression of the $(m+1)^{th}$ column for the next m, based on some induction rule. This requires further futuristic initiatives.

5. ACKNOWLEDGMENTS

We express our gratitude towards the DST, New Delhi and the TEQIP (Phase-II), University of Calcutta for providing financial support respectively to the first author and the second author. We are also indeed thankful to the Head of the Department of Radio Physics and Electronics, University of Calcutta for providing necessary infrastructural facilities to undertake research activities.

6. REFERENCES

[1] Lidl R., Niederreiter H., Finite Fields, Encyclopedia of Mathematics and its Applications, Vol. 20, Addison-Wesley Publishing Company, 1983.

[2] Church R., "Tables of Irreducible Polynomials for the first four Prime Moduli", Annals of Mathematics, Vol. 36(1), pp. 198 – 209, January, 1935.

[3] 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.

[4] Berlekamp E. R., "Factoring Polynomial over finite fileds", Bell Syst. Tech. J., Vol. 46, pp. 1853 – 1859, 1967.

[5] 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.

[6] Cantor D.G., "On Arithmetical Algorithms over Finite Fields" J. Combinatorial Theory Series A 9, pp. 285 – 300 (1989).

[7] Bach E. and Shoup V., "Factoring Polynomials using Random Bits", J. Symbolic Computation, Vol 9, pp. 229 – 239, 1990.

[8] Berlekamp E. R., "Factoring Polynomial over large finite fileds", Math. Comput. Vol. 24 (11), pp. 713 – 735, 1970.

[9] Shoup, V., "New algorithms for finding irreducible polynomials in finite fields", Math. Comput. Vol. 54, pp. 435 – 447, 1990.

[10] Daemen J., Rijmen V., AES Proposal: Rijndael, AES Algorithm Submission, September 3, 1999.

[11] FIPS Pub. 197, Announcing the Advanced Encryption Standard (AES), November 26, 2001.

[12] Stinson D.R., Cryptography Theory and Practice (Boca Raton, Chapman & Hall, CRC, 3rd Edition, 2006).

[13] Stallings W., Cryptography and Network Security Principles and Practices, Delhi, Pearson Education, 4th Edition, 2008.

[14] Forouzan B.A., Mukhopadhyay D., Cryptography and Network Security, New Delhi, TMH, 2nd Edition, 2011.

[15] Hasan M.A., "Double-Basis Multiplicative Inversion Over GF(2^m)", IEEE Trans. Comp., Vol. 47,(9), pp. 960 – 970, 1998.

[16] Arguello F., "Lehmer-based algorithm for computing inverses in Galois fields GF(2^m)", Electronics Letters, Vol. 42(5), 2006.

[17] Zaman JKM. S. and Ghosh R., "Multiplicative Polynomial Inverse over GF(7^3): Crisis of EEA and its Solution", Applied Computation and Security Systems, Advances in Intelligent Systems and Computing, Volume 305, pp. 87 – 107, DOI: 10.1007/978-81-322-1988-0_6.

[18] https://www.academia.edu/attachments/34220711/download_file

Appendix A
Irreducible polynomials over GF(11^2), GF(11^3), GF(13^2) and GF(13^3)

1. In GF(11^2): Total number of irreducible polynomial is 55

101, 103, 104, 105, 109, 111, 114, 116, 117, 118, 122, 124, 125, 126, 12A, 133, 136, 138, 139, 13A, 142, 145, 147, 148, 149, 151, 152, 153, 157, 15A, 161, 162, 163, 167, 16A, 172, 175, 177, 178, 179, 183, 186, 188, 189, 18A, 192, 194, 195, 196, 19A, 1A1, 1A4, 1A6, 1A7, 1A8.

2. In GF(11^3): Total number of irreducible polynomial is 440

1014, 1015, 1016, 1017, 1022, 1024, 1027, 1029, 1032, 1035, 1036, 1039, 1041, 1044, 1047, 104A, 1051, 1053, 1058, 105A, 1063, 1065, 1066, 1068, 1071, 1072, 1079, 107A, 1081, 1085, 1086, 108A, 1092, 1093, 1098, 1099, 10A3, 10A4, 10A7, 10A8, 1102, 1103, 1105, 1106, 1112, 1113, 1117, 1119, 1123, 1124, 1129, 112A, 1131, 1132, 1138, 1139, 1156, 1157, 1158, 1159, 1162, 1164, 1168, 116A, 1171, 1174, 1175, 1178, 1182, 1184, 1187, 118A, 1194, 1196, 1198, 119A, 11A3, 11A5, 11A6, 11A8, 1202, 1204, 1205, 1207, 1215, 1216, 1218, 1219, 1223, 1225, 1229, 122A, 1233, 1234, 1239, 123A, 1241, 1242, 1245, 1246, 1267, 1268, 1269, 126A, 1272, 1274, 1277, 1279, 1282, 1283, 1286, 128A, 1291, 1294, 1296, 1299, 12A1, 12A3, 12A5, 12AA, 1303, 1304, 1308, 130A, 1311, 1312, 1317, 1318, 1323, 1324, 1327, 1328, 1346, 1347, 1348, 1349, 1351, 1355, 1357, 135A, 1362, 1366, 1369, 136A, 1371, 1374, 1376, 1379, 1383, 1385, 1387, 1389, 1391, 1392, 1394, 139A, 13A6, 13A7, 13A9, 13AA, 1401, 1405, 1407, 140A, 1412, 1413, 1416, 141A, 1421, 1423, 1426, 1429, 1434, 1436, 1438, 143A, 1444, 1446, 1447, 1449, 1454, 1455, 1457, 1458, 1461, 1465, 1466, 146A, 1472, 1473, 1477, 1478, 1482, 1483, 1486, 1487, 14A2, 14A3, 14A4, 14A5, 1501, 1502, 1508, 1509, 1525, 1526, 1527, 1528, 1531, 1533, 1536, 1538, 1542, 1543, 1546, 154A, 1552, 1555, 1557, 155A, 1561, 1563, 1565, 1567, 1575, 1577, 1578, 157A, 1581, 1582, 1589, 158A, 1593, 1594, 1598, 159A, 15A4, 15A5, 15A9, 15AA, 1602, 1603, 1609, 160A, 1623, 1624, 1625, 1626, 1633, 1635, 1638, 163A, 1641, 1645, 1648, 1649, 1651, 1654, 1656, 1659, 1664, 1666, 1668, 166A, 1671, 1673, 1674, 1676, 1681, 1682, 1689, 168A, 1691, 1693, 1697, 1698, 16A1, 16A2, 16A6, 16A7, 1701, 1704, 1706, 170A, 1711, 1715, 1718, 1719, 1722, 1725, 1728, 172A, 1731, 1733, 1735, 1737, 1742, 1744, 1745, 1747, 1753, 1754, 1756, 1757, 1761, 1765, 1766, 176A, 1773, 1774, 1778, 1779, 1784, 1785, 1788, 1789, 17A6, 17A7, 17A8, 17A9, 1801, 1803, 1807, 1808, 1813, 1814, 1819, 181A, 1823, 1824, 1827, 1828, 1842, 1843, 1844, 1845, 1851, 1854, 1856, 185A, 1861, 1862, 1865, 1869, 1872, 1875, 1877, 187A, 1882, 1884, 1886, 1888, 1891, 1897, 1899, 189A, 18A1, 18A2, 18A4, 18A5, 1904, 1906, 1907, 1909, 1912, 1913, 1915, 1916, 1921, 1922, 1926, 1928, 1931, 1932, 1937, 1938, 1945, 1946, 1949, 194A, 1961, 1962, 1963, 1964, 1972, 1974, 1977, 1979, 1981, 1985, 1988, 1989, 1992, 1995, 1997, 199A, 19A1, 19A6, 19A8, 19AA, 1A05, 1A06, 1A08, 1A09, 1A12, 1A14, 1A18, 1A19, 1A21, 1A22, 1A27, 1A28, 1A32, 1A33, 1A39, 1A3A, 1A52, 1A53, 1A54, 1A55, 1A61, 1A63, 1A67, 1A69, 1A73, 1A76, 1A77, 1A7A, 1A81, 1A84, 1A87, 1A89, 1A91, 1A93, 1A95, 1A97, 1AA3, 1AA5, 1AA6, 1AA8.

3. In GF(13^2): Total number of irreducible polynomial is 78

102, 105, 106, 107, 108, 10B, 112, 113, 114, 115, 118, 11C, 123, 126, 127, 128, 129, 12C, 131, 134, 135, 136, 137, 13A, 142, 146, 149, 14A, 14B, 14C, 151, 155, 158, 159, 15A, 15B, 161, 162, 163, 164, 167, 16B, 171, 172, 173, 174, 177, 17B, 181, 185, 188, 189, 18A, 18B, 192, 196, 199, 19A, 19B, 19C, 1A1, 1A4, 1A5, 1A6, 1A7, 1AA, 1B3, 1B6, 1B7, 1B8, 1B9, 1BC, 1C2, 1C3, 1C4, 1C5, 1C8, 1CC.

4. In GF(13^3): Total number of irreducible polynomial is 728

1002, 1003, 1004, 1006, 1007, 1009, 100A, 100B, 1015, 1016, 1017, 1018, 1022, 1024, 1029, 102B, 1035, 1036, 1037, 1038, 1041, 1044, 1049, 104C, 1052, 1054, 1059, 105B, 1062, 1064, 1069, 106B, 1073, 1076, 1077, 107A, 1083, 1086, 1087, 108A, 1095, 1096, 1097, 1098, 10A1, 10A4, 10A9, 10AC, 10B3, 10B6, 10B7, 10BA, 10C1, 10C4, 10C9, 10CC, 1102, 1107, 110A, 110C, 1113, 1115, 1119, 111B, 1121, 1125, 1127, 112C, 1132, 1135, 1136, 1139, 1141, 1142, 1145, 114B, 1159, 115A, 115B, 115C, 1161, 1164, 1169, 116C, 1172, 1173, 1176, 117C, 1181, 1184, 1186, 1189, 1193, 1194, 1195, 1197, 1198, 119A, 119B, 119C, 11A2, 11A3, 11A4, 11A5, 11B2, 11B4, 11B8, 11BA, 11C7, 11C8, 11C9, 11CA, 1202, 1203, 1204, 1205, 1211, 1213, 1216, 121B, 1223, 1225, 1229, 122B, 1231, 1233, 1238, 123A, 1241, 1247, 124A, 124B, 1252, 1253, 1256, 125C, 1266, 1267, 1268, 1269, 1272, 1275, 1277, 127A, 1281, 1284, 1285, 1288, 1292, 1294, 1297, 129C, 12A1, 12A2, 12A4, 12A5, 12A6, 12AA, 12AB, 12AC, 12B5, 12B6, 12B7, 12B8, 12C1, 12C3, 12C7, 12C9, 1302, 1307, 130A, 130C, 1312, 1315, 1316, 1319, 1321, 1324, 1329, 132C, 1333, 1334, 1335, 1337, 1338, 133A, 133B, 133C, 1347, 1348, 1349, 134A, 1351, 1355, 1357, 135C, 1369, 136A, 136B, 136C, 1371, 1374, 1376, 1379, 1382, 1384, 1388, 138A, 1393, 1395, 1399, 139B, 13A1, 13A2, 13A5, 13AB, 13B2, 13B3, 13B6, 13BC, 13C2, 13C3, 13C4, 13C5, 1401, 1403, 1406, 140B, 1411, 1412, 1413, 1415, 1416, 1418, 1419, 141A, 1421, 1422, 1423, 1424, 1432, 1434, 1438, 143A, 1448, 1449, 144A, 144B, 1451, 1454, 1459, 145C, 1461, 1466, 1468, 146C, 1473, 1475, 1479, 147B, 1481, 1487, 148A, 148B, 1494, 1497, 1498, 149B, 14A3, 14A4, 14A5, 14A6, 14B4, 14B7, 14B9, 14BC, 14C2, 14C8, 14CB, 14CC, 1502, 1503, 1504, 1505, 1512, 1514, 1517, 151C, 1522, 1523, 1526, 152C, 1531, 1533, 1536, 153B, 1541, 1542, 1544, 1545, 1546, 154A, 154B, 154C, 1556, 1557, 1558, 1559, 1563, 1565, 1569, 156B, 1575, 1576, 1577, 1578, 1582, 1585, 1587, 158A, 1591, 1593, 1598, 159A, 15A1, 15A3, 15A7, 15A9, 15B1, 15B4, 15B5, 15B8, 15C1, 15C7, 15CA, 15CB, 1602, 1603, 1604, 1605, 1611, 1613, 1618, 161A, 1626, 1627, 1628, 1629, 1632, 1634, 1637, 163C, 1641, 1643, 1647, 1649, 1653, 1655, 1659, 165B, 1662, 1663, 1666, 166C, 1671, 1674, 1675, 1678, 1685, 1686, 1687, 1688, 1691, 1693, 1696, 169B, 16A1, 16A7, 16AA, 16AB, 16B2, 16B5, 16B7, 16BA, 16C1, 16C2, 16C4, 16C5, 16C6, 16CA, 16CB, 16CC, 1708, 1709, 170A, 170B, 1713, 1715, 171A, 171C, 1724, 1725, 1726, 1727, 1731, 1736, 1739, 173B, 1744, 1746, 174A, 174C, 1752, 1754, 1758, 175A, 1761, 1767, 176A, 176B, 1775, 1778, 1779, 177C, 1785, 1786, 1787, 1788, 1792, 1797, 179A, 179C, 17A2, 17A3, 17A6, 17AC, 17B3, 17B6, 17B8, 17BB, 17C1, 17C2, 17C3, 17C7, 17C8, 17C9, 17CB, 17CC, 1808, 1809, 180A, 180B, 1811, 1816, 1819, 181B, 1821, 1827, 182A, 182B, 1832, 1837, 183A, 183C, 1841, 1842, 1843, 1847, 1848, 1849, 184B, 184C, 1854, 1855, 1856, 1857, 1862, 1864, 1868, 186A, 1875, 1876, 1877, 1878, 1883, 1886, 1888, 188B, 1893, 1895, 189A, 189C, 18A4, 18A6, 18AA, 18AC, 18B5, 18B8, 18B9, 18BC, 18C2, 18C3, 18C6, 18CC, 1902, 1907, 190A, 190C, 1913, 1914, 1915, 1917, 1918, 191A, 191B, 191C, 1929, 192A, 192B, 192C, 1933, 1935, 1939, 193B, 1942, 1943, 1944, 1945, 1951, 1954, 1959, 195C, 1961, 1965, 1967, 196C, 1972, 1974, 1978, 197A, 1982, 1983, 1986, 198C, 1992, 1995, 1996, 1999, 19A7, 19A8, 19A9, 19AA, 19B1, 19B4, 19B6, 19B9, 19C1, 19C2, 19C5, 19CB, 1A01, 1A03, 1A06, 1A0B, 1A14, 1A17, 1A18,

1A1B, 1A21, 1A24, 1A29, 1A2C, 1A31, 1A32, 1A33, 1A35, 1A36, 1A38, 1A39, 1A3A, 1A43, 1A44, 1A45, 1A46, 1A51, 1A56, 1A58, 1A5C, 1A61, 1A62, 1A63, 1A64, 1A74, 1A77, 1A79, 1A7C, 1A83, 1A85, 1A89, 1A8B, 1A92, 1A94, 1A98, 1A9A, 1AA2, 1AA8, 1AAB, 1AAC, 1AB1, 1AB7, 1ABA, 1ABB, 1AC8, 1AC9, 1ACA, 1ACB, 1B08, 1B09, 1B0A, 1B0B, 1B12, 1B17, 1B1A, 1B1C, 1B22, 1B24, 1B28, 1B2A, 1B33, 1B35, 1B3A, 1B3C, 1B42, 1B43, 1B46, 1B4C, 1B51, 1B57, 1B5A, 1B5B, 1B64, 1B65, 1B66, 1B67, 1B73, 1B76, 1B78, 1B7B, 1B85, 1B88, 1B89, 1B8C, 1B91, 1B96, 1B99, 1B9B, 1BA1, 1BA2, 1BA3, 1BA7, 1BA8, 1BA9, 1BAB, 1BAC, 1BB5, 1BB6, 1BB7, 1BB8, 1BC4, 1BC6, 1BCA, 1BCC, 1C01, 1C03, 1C06, 1C0B, 1C12, 1C14, 1C18, 1C1A, 1C21, 1C26, 1C28, 1C2C, 1C34, 1C37, 1C38, 1C3B, 1C42, 1C48, 1C4B, 1C4C, 1C51, 1C52, 1C53, 1C54, 1C61, 1C64, 1C69, 1C6C, 1C71, 1C77, 1C7A, 1C7B, 1C84, 1C87, 1C89, 1C8C, 1C91, 1C92, 1C93, 1C95, 1C96, 1C98, 1C99, 1C9A, 1CA8, 1CA9, 1CAA, 1CAB, 1CB3, 1CB5, 1CB9, 1CBB, 1CC3, 1CC4, 1CC5, 1CC6.