مجلة جامعة بابل / العلوم الصرفة والتطبيقية / المجلد ١ / العدد ٣ : ١٩٩٦

A Proposed Solution to Polynomial Factorization over Prime Finite Field Public Key Cryptography

Sattar Bader Sadkhan
Military Research and Development Comitte

Abdul Sattar Salman
, University of Technology

Abstruct

One of the well known types of Public Key Cryptosystem is the type using reciprocal Number, that depends mainly in Decryption Process on using of polynomial factorization over Prime Finite Field and Legendre symbol. The publications showed that there is aproblem in determining this symbol, that depends on the reducibility idea. This paper suggest a solution to overcome such problem, by using the Greatest Common Divisor for polynomials, and overcome the limitations that appeared with Rabin,s method, that applied for such problem. A program was implemented in Turbo Pascal Version 5.5 and was with many examples. Such solution provide agreat gain in reducing the time and storage required for performing the Deciphering process of Reciprocal Public Key System.

Introduction

The revolutionary idea in cipher system is to make public the encipherment key as well as the enciphering algorithm. Such system is suggested in 1976 by Diffe and Hellman [6] and called *New Direction in Cryptography*". Such system is well known as Public Key Cryptosystem. They didn,t need for the encipherment procedure key to be the same as decipherement procedure.

For such system, given the encipherement procedure, the key, and perhaps the deduce the decipherement key. One we have such system, any one wishing to use it will be assigned an encipherement key which will be published in a dictionary. Any one wishing to send a message to one of the users merely consults the dictionary to see which encipherement key he should use. In this way a user, who will have his own secret decipheremeny key, will be able to decipher any cryptogram sent to him without even needing to know the identity of the sender.

Section 2 will discuss brifely the idea of public key cryptography using reciprocal number and gives the Legender and Jacobi symbols. Section 3 shows the Berlkamp's Algorithm for factorization of polynomial over finite field and gives the Division Algorithm with the runnig of the program for two examples. Aconclusion is mentioned in section 4.

Public Key Crypyosystem Using Reciprocal Number

This cryptosystem is proven to be as difficult as factoring a large number. The following symbol is called legenders symbol:

$$(a/p) = \begin{cases} 1 & \text{if } X^2 = a \bmod p \text{ has a solution} \\ -1 & \text{otherwise} \end{cases}$$

where p is aprime number other than two, while the Jacobis symbol is:-

$(a/R) = (a/p)(a/q)$, where $R=pq$.

Secret key : Two large prime numbers p and q

Public key : {R (=pq) , c} where $(c/p)n = (c/q)=-1$

Plain Text : M, where $0<M<R$ and GCD $(M,R)=1$

Cipher Text : (E, S, t,) , where

$$E = M+(c/M \bmod R) \qquad (1)$$

$$S = \begin{cases} 0 & \text{if } (M/R) = 1 \\ 1 & \text{if } (M/R)=-1 \end{cases}$$

$$t = \begin{cases} 0 & \text{if } (c/M \bmod) > M \\ 1 & \text{if } (c/M \bmod R) < M \end{cases}$$

Decryption

From eq. (1) , we obtain

$$M^2 - E M + c = 0 \qquad (2)$$

Let a_1 and a_2 be the roots {Eq. (2) mod p}, while b_1 and b_2 be the roots of {Eq. (2) mod q}. Eq. (2) mod R, has the following four roots:-

$M1 = [a_1 , b_1]$
$M2 = [a_1, b_2]$
$M3 = [a_2 , b_1]$
$M4 = [a_2 , b_1]$

Now we have the four messahe and one of them is the original plaintext which will be determined by using the value of (S and t).

When S=0, then

$$M = \begin{cases} \text{Min } (M_1 , M_2) & \text{if } t=0 \\ \text{Max } (M_1 , M_2) & \text{if } t=1 \end{cases}$$

When S=1, then

$$M = \begin{cases} \text{Min } (M_3, M_4) & \text{if } t=0 \\ \text{Max } (M_3, M_4) & \text{if } t=1 \end{cases}$$

Factorization of Polynomials over Finite field

All published algorithms were applied on asquare free polynomials [2], [3], [5].

Berlkam's Algorithm

This algorithm used to test the reducibility of the ploynomials and to factorize over small finite field [2]. Let u(x) be the polynomial to be factorized

Step 1:- Ensure that u(x) is squre free

Step 2 :- Construct the [n n] matrix Q, where n is the degree of u(x).

Step 3 :- Triangularize the matrix Q-

I, where I is the [n n] identity matrix, represente the number of irreducible factors of u(x), where r= , this means that u(x) is irreducible.

Find $v^{(1)},\ldots,v^{(r)}$ linearly independent vectors such that

$$v^{(j)}(Q-I)=(0,0,\ldots,0)$$

Step 4:- Calculation of GCD (u(x), $v^{(2)}$ (x)-S) for 0<S<p will give us anon-trivial factorization of u(x) and so on.

Lemma (1) :-

Let l_1, ..., l_k be all the prime divisors of n and n/li = mi Apolynomial g(x) Zp[x] if:-

a) g(x) (xp) - x)
b) (g(x) , x - x) = 1 1<i<k

Example :-

Find the value of (5/7), i.e. test the reducibility of the piolynomial x=5 over the field of residues modulo 7.

Solution

GCD (x - 5 , 5 - 1) = 5
this means that x - 5 is irreducible over our field.

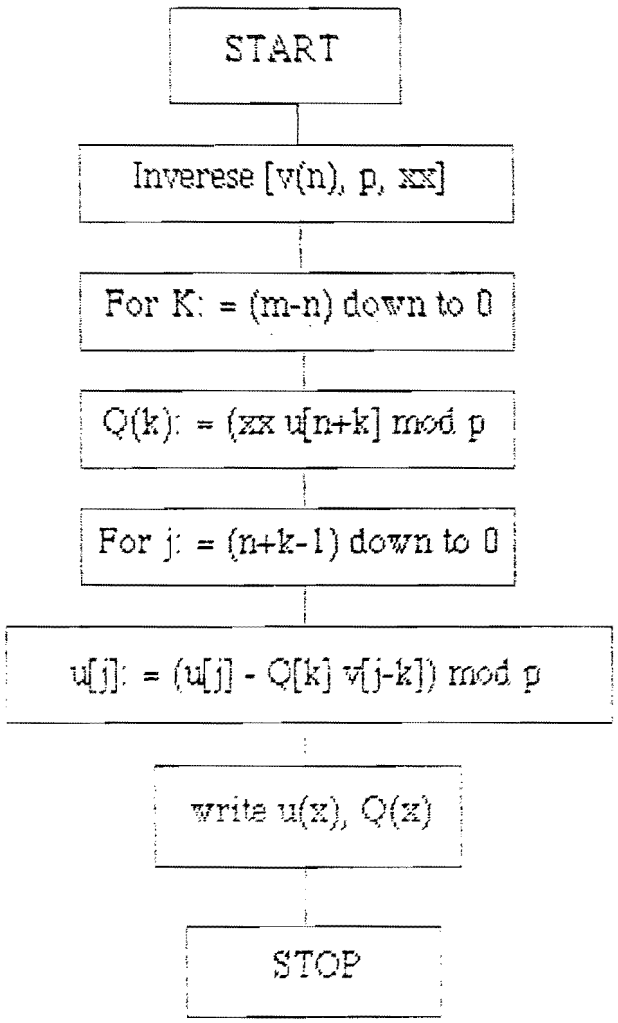
Let us find the following :-

GCD (x - 5 , x + 6) = -4
GCD (x - 5 , x + 5) = -1
GCD (x - 5 , x + 4) = -3
GCD (x - 5 , x + 3) = -3
GCD (x - 5 , x + 2) = -1
GCD (x - 5 , x + 1) = -4

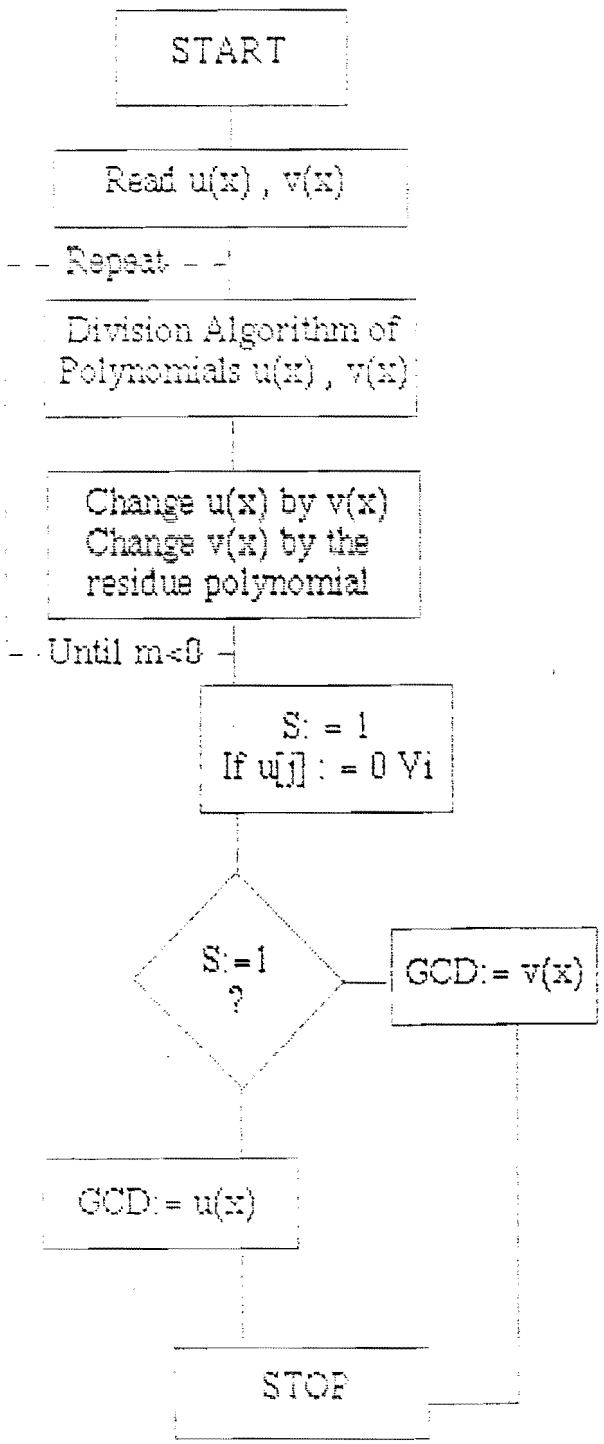
This mean that no one of the roots (x+1), ..., (x+6) is afactor of x - 5 , which insure that the polynomial is irreducible.

Division Algorithm used in the main Procedure

The Algorithm of division of polynomial u(x) of degree m over the polynomial v(x) of degree n over GF(p), is described by the following flow chart:-



The greatest Common Divisor Algorithm of Two Polynomials u(x) and v(x) by the flow chart below:-



Conclusion

a) We know that the Berlkamp Algorithm used to check the reducibility of polynomials over finite field, and to factorize the polynomial over such field, but it can not be applied for polynomials of degree (2). Because the Q-Matrix will be (2*2). And after Triangularization, and Subtracting the identity matrix of the same dimension will result in a matrix with zero elements row. Which alawys indicates that the polynomial is irreducible according to Berlkamp Algorithm, although it is reducible (actually).

b) We proposed a method to identify wether the polynomial is reducible or irreducible including that it will be either square free or not square free over that field according the degree of the resulted GCD of the given polynomial f(x) with the originating polynomial of that prime field (x-1) , and such result considered as a good result for the Legendre symbol .

References

1- Electronic Letters, 1987, vol. 23, No. 15.

2- Algebric Coding Theory, Elwyn R. Berlkamp.

3- Probabilisic Algorithm in finite field, SIAM J. on Computing vol. 9, No. 2, 1980.

4- The art of computing programming, vol. 2, Donald E. Knuth.