P- ISSN 1991-8941 E-ISSN 2706-6703 *Journal of University of Anbar for Pure Science (JUAPS)* Open Access
2011,(5), (3) :45-49

Developed Protocol for Key Exchange Based on Irreducible Polynomial

Abdul Monem S. Rahma* **Rabah N. Farhan**** **Hussam J. Mohammad****

* University of Technology- Computer science Dept.
**University of Anbar - College of Computer.

ARTICLE INFO

Received: 4 / 6 /2011
Accepted: 6 / 9 /2011
Available online: 14/6/2012
DOI: 10.37652/juaps.2011.44312
Keywords:
key exchange,
Irreducible Polynomial,
Diffie-Hellman.

ABSTRACT

The Aim of this paper is to design a protocol for key exchanging to work on the available computers for different data security application. This paper proposed idea to modify the Diffie-Hellman key exchange by using truncated polynomial instead of discrete logarithm problem to overcome the problem of large prime numbers and non-full coverage of the finite set. The proposed method depends on the arithmetic polynomials. The Irreducible truncated polynomial mathematics is highly efficient and compatible with personal computers.

Introduction

Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted. Modern cryptographic systems include symmetric-key algorithms (such as DES and AES) and public-key algorithms (such as RSA)[12]. Symmetric-key algorithms use a single shared key; keeping data secret requires keeping this key secret. Public-key algorithms use a public key and a private key. The public key is made available to anyone (often by means of a digital certificate). A sender will encrypt data with the public key; only the holder of the private key can decrypt this data[11].

The key exchange problem is how to exchange whatever keys or other information are needed so that no one else can obtain a copy. With the advent of public key / private key cipher algorithms, the encrypting key (public key) could be made public, since (at least for high quality algorithms) no one without the decrypting key (the private key) could decrypt the message[1,13].

The key exchange protocols can be categorized in to two categories: unauthenticated and authenticated. In an unauthenticated key exchange, the parties involved in key exchange do not authenticate each other. As a result, the adversary can launch a man-in-middle attack to agree upon a different key with each of the party involved in key exchange.

* Corresponding author at: University of Technology- Computer science Dept, Iraq.E-mail address:

This situation is resolved by using authenticated key exchange. The protocol is authenticated if every party verifies the authenticity of all the other parties involved in the key exchange [6, 11].

Diffie-Hellman Key Exchange

The Diffie-Hellman key agreement was invented in 1976 during collaboration between Whitfield Diffie and Martin Hellman and was the first practical method for establishing a shared secret over an unprotected communications channel [7]. Diffie-Hellman depend on discrete logarithm problem and prime number .The Diffie-Hellman Key Exchange's security depends on the difficulty of solving the discrete log problem, since no fast algorithms have been discovered for these problems; the DH Key Exchange is still in use today and is thought to be one of the most secure methods available [8].

In the following review, different methods are modified of Diffie-Hellman:

Bhattacharya P., Debbabi M. and et al, (2005), proposed two modifications of Diffie-Hellman. The first modification is to change the domain to integer with n=2pt where Zn* is still cyclic and the second modification is to change the domain to Gaussian arithmetic Zn*[i]. After implementing the three

algorithms they found that the symmetric key size derived from the two modified algorithms is much greater than the classical one. Moreover, attacking the two modified algorithms using Pohlig-Hellman algorithm, using the same prime value p and private value a or b, needs much more time than the classical one [5].

Also Pathak H. K., Manju S. (2010) proposed a new public key cryptosystem and a Key Exchange Protocol based on the generalization of discrete logarithm problem using Non-abelian group of block upper triangular matrices of higher order. The proposed cryptosystem is efficient in producing keys of large sizes without the need of large primes. The security of both the systems relies on the difficulty of discrete logarithms over finite fields [10].

Irreducible polynomial

In mathematics, the adjective irreducible means that an object cannot be expressed as the product of two or more non-trivial factors in a given set [2]. For any field F, the ring of polynomials with coefficients in F is denoted by F[x]. A polynomial p(x) in F[x] is called irreducible over F if it is non-constant and cannot be represented as the product of two or more non-constant polynomials from F[x]. The property of irreducibility depends on the field F; a polynomial may be irreducible over some fields but reducible over others [3, 4].

Proposal method

This paper produce a modified Diffie-Hellman key exchange by using truncated polynomial instead of discrete logarithm problem and increases the complexity of this method over unsecured channel. There are many conditions before explaining the Proposal Method, these conditions are:

1. Each side (Alice and Bob) has database that contain the value of irreducible polynomial (g) and polynomial value (X).

2. Both sides must have same database and put their database in a very secret place.

3. The database consist of 360 rows according to the days for year, table (1) shows part from this database.

4. All operations performed to compute the key are applied in a polynomial operations (addition, subtraction, multiplication, and division).

Key generation

two sides want to exchange key (Alice and Bob) as following:

1. Alice selects two integer numbers (A1, B1) and sends the two values to Bob.

2. Bob receive (A1 ,B1) and select also two integer (A2 , B2) and send the two value to Alice .

3. Now each side has (A1, B1, A2, and B2) and converts these values to binary then to polynomial.

4. Alice and Bob return values of (X, g) from database based on the day and month for communication between them.

5. Each side applying function (1) and (2) to compute (Y1, Y2):

$Y1 = (A1 \square\square X \square B1) \bmod g \ldots. (1)$

$Y2 = (A2 \square X \square B2) \bmod g \ldots. (2)$

6. Now the two sides have two values (Y1, Y2), each one apply the same function on these values to compute secret key (Sk) as:

$Sk = (Y1 \square X \square Y2) \bmod g \ldots. (3)$

Figure (1) that represents the steps of proposed method.

Example 1: Let us take simple example for apply the method when Alice key exchange with Bob in date (1- January):

1. Alice generate two integer values and sends the two values to Bob

A1 = 6, B2 = 4.

2. Bob generate two integer values and sends the two values to Alice

A2 = 9, B2 = 7.

3. Alice and Bob convert each values to binary then polynomials.

A1 = 110 = $x^2 + x$

B1 = 100 = x^2

A2 = 1001 = $x^3 + 1$

B2 = 111 = $x^2 + x + 1$

4. Both sides return the value (X) and (g) from database

X= $x^5 + x + 1$

g = $x^8 + x^4 + x^3 + x + 1$

5. Alice and Bob applied the same functions to find Y1, Y2

Y1 = (A1□□ X □ B1) mod g

Y1 = $(x^2 + x) \square (x^5 + x + 1) \square\square\square x^2$) mod $(x^8 + x^4 + x^3 + x + 1)$

= $[x^7 + x^6 + x^3 + x] \square\square\square x^2$) mod $(x^8 + x^4 + x^3 + x + 1)$

= $[x^7 + x^6 + x^3 + x^2 + x]$ mod $(x^8 + x^4 + x^3 + x + 1)$

Y1 = $x^7 + x^6 + x^3 + x^2 + x$

Y2 = (A2□□ X □ B2) mod g

= $(x^3 + 1) \square\square\square (x^5 + x + 1) \square\square (x^2 + x + 1)$ mod $(x^8 + x^4 + x^3 + x + 1)$

= $[x^8 + x^5 + x^4 + x^3 + x + 1] \square (x^2 + x + 1)$ mod $(x^8 + x^4 + x^3 + x + 1)$

= $[x^8 + x^5 + x^4 + x^3 + x^2]$ mod $(x^8 + x^4 + x^3 + x + 1)$

Table (1): Simple Part of database.

Day-Month	Value (X)	Irreducible polynomial (g)
1-1	$x^5 + x + 1$	$x^8 + x^4 + x^3 + x + 1$
2-1	$x^8 + x^6 + x^4 + x^3 + x^2$	$x^8 + x^4 + x^3 + x^2 + 1$
3-1	$x^5 + x^4 + x^3 + x^2 + x + 1$	$x^8 + x^5 + x^3 + x + 1$
4-1	$x^6 + x^3 + x^2 + x + 1$	$x^8 + x^5 + x^3 + x^2 + 1$
5-1	$x^7 + x^5 + x^4 + x^3 + 1$	$x^8 + x^5 + x^4 + x^3 + 1$
6-1	$x^8 + x^5 + x + 1$	$x^8 + x^5 + x^4 + x^3 + x^2 + x + 1$
7-1	$x^8 + x^2 + 1$	$x^8 + x^6 + x^3 + x^2 + 1$
8-1	$x^6 + x^5 + x^2 + 1$	$x^8 + x^6 + x^5 + x^2 + 1$
9-1	$x^6 + x + 1$	$x^8 + x^6 + x^5 + x + 1$
10-1	$x^7 + x^6 + x^5 + x^2 + 1$	$x^8 + x^6 + x^5 + x^2 + 1$
11-1	$x^7 + x^6 + x^1 + 1$	$x^8 + x^6 + x^5 + x^3 + 1$
12-1	$x^6 + x^5 + x^4 + x^2 + x + 1$	$x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$
13-1	$x^7 + x^6 + x^5 + x^4 + 1$	$x^8 + x^6 + x^5 + x^4 + 1$
14-1	$x^6 + x^4 + x^3 + x + 1$	$x^8 + x^6 + x^5 + x^4 + x^3 + x + 1$
15-1	$x^7 + x^2 + x + 1$	$x^8 + x^7 + x^2 + x + 1$
16-1	$x^7 + x^3 + x$	$x^8 + x^7 + x^3 + x + 1$
17-1	$x^7 + x^6 + x^3 + x^2 + 1$	$x^8 + x^7 + x^3 + x^2 + 1$
18-1	$x^8 + x^7 + x^3 + x^2 + 1$	$x^8 + x^7 + x^4 + x^3 + x^2 + x + 1$
19-1	$x^5 + x + 1$	$x^3 + x^2 + 1$
20-1	$x^7 + x^6 + x^4 + x^3 + 1$	$x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$
21-1	$x^8 + x^7$	$x^8 + x^7 + x^5 + x^4 + 1$
22-1	$x^4 + x^3 + x^2 + 1$	$x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1$
23-1	$x^8 + x + 1$	$x^8 + x^7 + x^6 + x + 1$
24-1	$x^7 + x^6 + x^3 + x^2 + x$	$x^8 + x^7 + x^6 + x^3 + x^2 + x + 1$

$$\begin{array}{r|l} x^8+x^4+x^3+x+1 & 1 \\ \hline & x^8+x^5+x^4+x^3+x^2 \\ & x^8+x^4+x^3+x+1 \\ \hline & x^5+x^2+x+1 \end{array} \oplus$$

Y2= $x^5 + x^2 + x + 1$

To find Secret Key (Sk) :

Sk = (Y1 □ X □ Y2) mod g

Sk=($x^7 + x^6 + x^3 + x^2 + x$) ($x^5 + x + 1$)

($x^5 + x^2 + x + 1$) mod ($x^8 + x^4 + x^3 + x + 1$)

= [$x^{12} + x^{11} + x^7$ + $x^4 + x$]

($x^2 + x + 1$) ($x^8 + x^4 + x^3 + x + 1$)

mod

= [$x^{12} + x^{11} + x^7$ + $x^4 + x^2 + 1$]

mod ($x^8 + x^4 + x^3 + x + 1$)

$x^4 + x^3 + 1$

$x^8 + x^4 + x^3 + x + 1$ | $x^{12} + x^{11} + x^7 + x^4 + x^2 + 1$

$x^{12} + x^8 + x^7 + x^5 + x^4$ ⊕

$x^{11} + x^8 + x^5 + x^2 + 1$

$x^{11} + x^7 + x^6 + x^4 + x^3$ ⊕

$x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$

$x^8 + x^4 + x^3 + x + 1$ ⊕

$x^7 + x^6 + x^5 + x^2 + x$

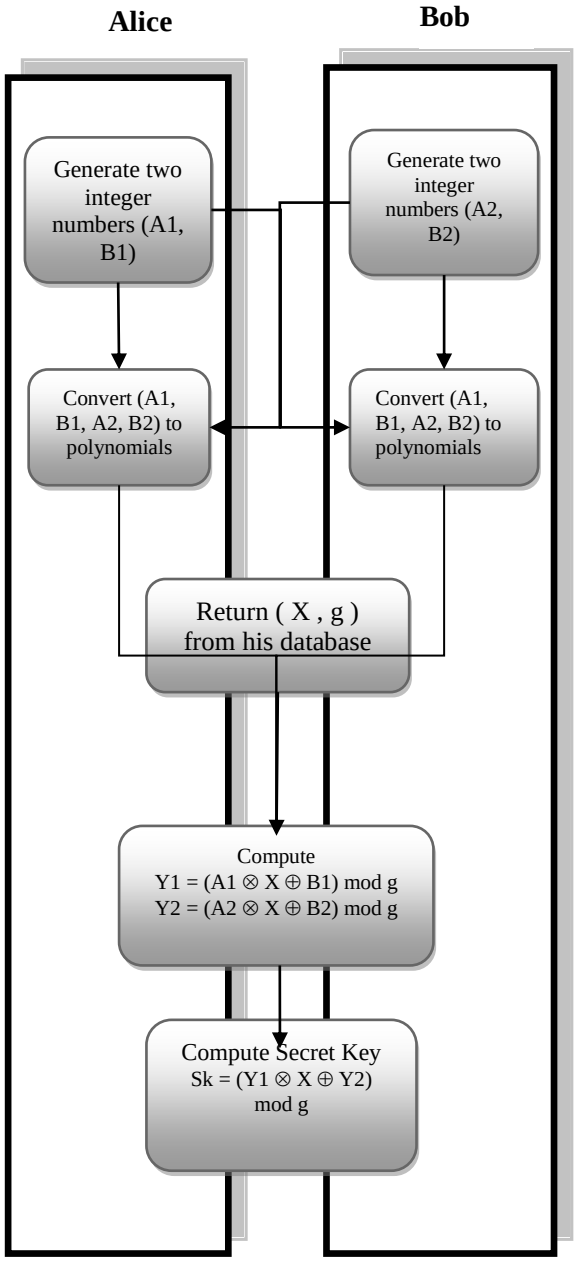
= $x^7 + x^6 + x^5 + x^2 + x$ (Secret Key)

Analysis

Key randomness for the traditional method is very small when choosing a small prime number; on the other hand the randomness of the new method is always very high whatever the irreducible polynomial because the result is always unexpected. The complexity of the traditional method depends on computing the discrete logarithm which take long time specially when choosing very high prime number, while this method is always complex because it depends on irreducible truncated polynomial. when anyone want to know the key he will try all irreducible polynomial (g) and Truncated polynomial (X) on novel function ,so that it became very difficult to conform (g) with (X) .

Conclusion

this paper present an idea for key exchange protocol by modifying the idea of Diffie-Hellman key exchange and completely remove the discrete logarithm and replace it by irreducible truncated polynomial to overcome the problem of large prime numbers and non-full coverage of the finite set, run time of proposal method less than run time of traditional Diffie-Hellman.



Reference

1. [1] Ran C. , Hugo K., "Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels" . 2001.
2. [2] Chandan S., "A Note on Irreducible Polynomials and Identity Testing". 2004.

3. [3] Ron Brown, Jonathan L. Merzel, "INVARIANTS OF DEFECTLESS IRREDUCIBLE POLYNOMIALS" . 2000 .
4. [4] Henry W., "Divisibility Properties of Fibonacci Polynomials over GF(2)" , MSc. Thesis, Department of Statistics and Computer Science, West Virginia University ,1997 .
5. [5] Bhattacharya P., Debbabi M. , Otrok H., " Improving the Diffie Heliman Secure Key Exchange", Computer Security Laboratory Concordia Institute for Information Systems Engineering, Concordia University, Canada, 2005.
6. [6] Jalaj K. Upadhyay, "Key Exchange Protocol Using Encryption Scheme Provably Secure Against CCA", ISC Turkey, 2007.
7. [7] Abeer T. Al-Obaidy , " Security Techniques for E-Commerce Websites ", Ph. Thesis, The Department of Computer Science , University of Technology, 2010.
8. [8] Keith Palmgren, "Diffie-Hellman Key Exchange A Non-mathematician's explanation", ISSA ,2006.
9. [9] William Stallings ," Cryptography and Network Security Principles and Practices, Fourth Edition",© by Prentice Hall ,2005.
10. [10] H. K. Pathak , Manju Sanghi, " Public key cryptosystem and a key exchange protocol using tools of non-abelian group", IJCSE, 2010 .
11. [11] B.Lehane , L.Doyle, D.O'Mahony, " Shared RSA Key Generation In A Mobile Ad Hoc Network", 2003 .
12. [12] Naim Ajlouni , asim El-sheik ," A new Approach in Key Generation and Expansion in Rijandael Algorithm", The international Arab Journal of Information Technology, 2006 .
13. [13] M. Freire-Santosa, J. Fierrez-Aguilara, J. Ortega-Garcia, " Cryptographic key generation using handwritten signature" , 2006 .

بروتوكول مطور لتبادل المفاتيح بالاعتماد على متعددة الحدود المنقطعة

عبد المنعم صالح رحمة رباح نوري فرحان حسام جاسم محمد

الخلاصة

الهدف من هذا البحث هو لتصميم بروتوكول لتبادل المفاتيح لكي يعمل على الحاسبات المتوفره ويكون ملائم لتطبيقات مختلفة لامن البيانات . في هذا البحث تم اقتراح فكرة تعتمد على تحوير فكرة تبادل المفتاح للديفي–هيلمان من خلال إزالة كاملة للوغاريتمات المتقطعة وإبدالها بمتعددة الحدود المنقطعة (truncated polynomial) للتغلب على مشكلة الأعداد الأولية الكبيرة جدا والتغطية الغير كاملة للمجموعة المحددة. وان هذه الطريقة تعتمد بالكامل على المتعدّد الحدود الحسابي. إنّ الرياضياتَ المتعدّدة الحدودَ المَقْطُوعةَ المتعذرة الإنقاصَ (Irreducible polynomial) كفوءةُ ومتوافقةُ جداً بالحواسيب الشخصية.