Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Implementation of Public key Cryptography Algorithms on Debit cards

G.Annapooranam
Research scholar , M.S.University

Abstract: *As the debit card is used increasingly and widely in all areas,security becomes a important issue for information transmission .Public key cryptography is the important research direction of debit card encryption. Here the first analysis of the principle of public key cryptography , illustrate two typical cryptographics. That are RSA and ECC.However the ECC's uses with smaller keys to provide high security and high speed in a low bandwidth. it's only needed for our real life. So that we select ECC cryptographic to implement the debit card encryption.*

Keywords: *Debit card;RSA; Public key Cryptography;ECC*

I. INTRODUCTION

A debit card is a plastic card with an embedded microchip that can be loaded with data,which is a credit card that is connected to a specific account where money canbe deposited. Debit cards are either smartcard (or) magnetic strip , this card also known as bank card(or) check card. In some of the place the primary account number is assingned exclusively for use on the internel and there is no physical card. The use debit cards has become so widespread that their volume has overtaken (or) entirely replaced cheques. Anyhow information security is one of the main directions of debit card , it's naturally gives rise to the need for reliable,efficient and convenient cryptographic algorithms. Whitefield Diffie and Martin _Hellman proposed public key cryptography (PKC) algorithm which is widely used.it provide secure storage and confidential data and is capable of executing complex cryptographic algorithms such as RSA & ECC
This paper decribes RSA& ECC algorithm compares these two cryptosystem performance applicated in debit card and gives improvement proposar and further development.

II. RULES OF PKC

Public key Cryptography algorithm can be divided into two kinds, which are public key and private key.In PKC system public key is open. But the private key is kept confidential and which cannot be calculated only from the public key. The cryptographic algorithm that are based on mathematical problem. Public key Cryptography is used as a method of assuring the confidentiality ,authenticity and non-repudiability of electronic communication and data storage.Private (or) secret key is an encryption/decryption key known only to the parties that exchange secret message, a key should be shared by the communicators. If the both keys are diffident, the user can decrypt the message, unauthorized user and the sender cannot decrypt this message.

From the PKC ,if sender A send a message (m) to the receiver B , he can find the ciphertext (C) with the encryption function of $Enc_{eB(m)}$ and the secret key,then the transfer the cipher text to Receiver B . When the receiver get message m then he calculate the function of Dec_{dB}(C) to found the message (m)

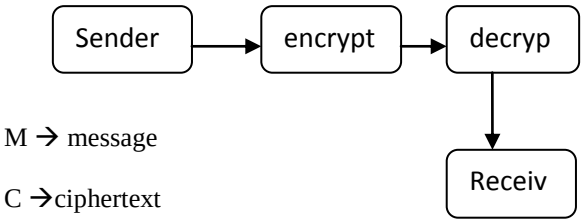

Figure 1: PKC Encryption

A. RSA Cryptosystem

The RSA cryptosystem (Rivest,Shamir,Adleman) is known of the integer factorization family of cryptosystem. This cryptosystem mostly used in the mathematical difficultly of factoring large integers.

The RSA key pair generation algorithm is generated by following steps.

1. Choose two random prime numbers , p and q ,length of l/2
2. Calculate n=p*q and Ø=(p-l)(q-l)
3. Choose integer e to meet l<e< Ø and gcd(e, Ø)=l
4. Calculate integer d to meet l<d< Ø and e*d=l(mod Ø)
5. Get the public key pair(e,n) and the private key pair (d,n)

Here n is RSA's operation mode
E is signified encryption index
l is signified security parameters and
d is sidnified private key

using encryption formula e=me mod n, the RSA encryption scheme get ciphertext

B. ECC Cryptosystem

This Elliptic curve cryptography , which is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography is the same level of security provided by keys of smaller size.Elliptic curves are applicable for encryption, digital signatures, pseudo-random generators and other tasks. They are also used in several integer factorizationalgorithms that have applications in cryptography.

The field is defined by the set of elements and also some operations , which have some special properties .
Order E is the finite field F_p on the elliptic curve
P is a point on the elliptic curve
Then E is defined by formula(1)
B2=a2+xa+y ----------(1)
Here x,y ƐFp
4x3+27y2≠0(mod p) -------(2)

Set the order of P is a prime number n , which is assemblage P is a cyclic sub groups of elliptic curves which generated by P and the curve equation is E and order n constitute a public set of paramaters. The ECC key pair generation algorithm is generated by following steps:

1. Choose a random key d in [1,n-1]
2. Calculate key Q=d*p
3. Get the public key pair (Q,d)

d→ signified private key and Q is signified public key.

For achieving the elliptic curve encryption , the following steps needed,

The plaintext m as elliptic curve point M

1. Choose a random key k in [1,n-1]
2. Calculate C1= k* p
3. Calculate C2=M+k*Q
4. Get the public key pair (C1,C2)

Here C1,C2 are ciphertexts

The decryption process is receiver calculate M by formula M= C2 + d* C1, after that we get plaintext m

III IMPLEMENTATION OF PKC ALGORITHM ON DEBIT CARD

The debit card is mainly used for electronic identification and storing user information. The security services offered by a debit card frequently include both data encryption and public key operation using RSA and ECC algorithms among many algorithms .Creation of digital signature is frequently most computationally intensive operation demanded of a debit card.

The hardware resources of debit card are limited. The ECC encryption is capable of compensate for the limitations of the debit card hardware. On the other side , the key generated from ECC is very short , that means less storage capacity faster information transfer rate and computing power can be achieved. And also the use of ECC in the debit card does not require additional hardware , so that reducing the cost of hardware & improving the usability

Research in cryptography elliptic curve is essentially a huge prime fields GF(p) and is attached on finite field GP(2m) of characteristic 2. Here we study the case of characteristic 2 in this paper ,. In this case , the formula(1) can be further simplified and shown in formula(3)

$$b2+ab=a3+x6, \quad x6\varepsilon F2m \quad (3)$$

Then, the elliptic curve is determined(formula 3), order n with SEA algorithm. Next generate elliptic curve key pair according to the ECC key pair generation algorithm which is identified in 2.2 . Finally , realize debit card information and decryption by the elliptic curve encryption scheme defined in 2.2

Implementing ECC on Intel 8051 , generate the key pair with encryption (5.2s) & (21.3s) and decryption took 17.1s . These results are basically consistent with the expected one .

CONCLUSION

This PKC have proposed by governmental entities all over in the world. The ECC and RSA are all typical public key cryptosystem. This paper compares the two cryptosystems(ECC &RSA), indicate that ECC is quicker evolving capacity and by providing easy and alternative way to researchers of cryptographic algorithm than RSA.

This paper applied ECC encryption to the intel 8051 to achieve encryption and decryption . Although debit card had restricted by hardware,ECC feature are capable to developing debit card also.

Acknowledgments

I would like to thank the anonymous referees for providing useful concept. I am extremely grateful to god. Finally , my special thanks to my friends and family members for spending many hours for developing this paper.

References

[1]. Warwick Ford and Brian O' Higgins IEEE july 1992 , "Public key cryptography and Open systems Interconnection"
[2]. Whitfield Diffie , Proceedings of the IEEE,vol76,No.5, may 1988, "The First Ten Years of Public-Key Cryptography"
[3]. Lanxiang chen, Shuming Zhou 2010 IEEE "The comparision between public key and symmetric key cryptography in protecting storage system"

Author's Biography

I have finished my M.C.A from Bharathidasan University and then completing M.Phil in Periyar university. Now pursuing Ph.D in Manonmaniam sundaranar university , trinelvelli.