طرق التشفير وفك التشفير باستخدام زمرة المنحنى البيضوي

Proposed Methods to Encryption Decryption by Group of Elliptic Curve

الاستاذ الدكتور

ستار بدر سد خان

جامعة بابل / كلية العلوم

المدرس المساعد

نجلاء فلاح حميد

جامعة الكوفة / كلية العلوم

طرق التشفير وفك التشـــفير باستخدام زمرة المنحنى البيضـــوي

Proposed Methods to Encryption Decryption by Group of Elliptic Curve

الاستاذ الدكتور

ستار بدر سد خان

جامعة بابل / كلية العلوم

المدرس المساعد

نجلاء فلاح حميد

جامعة الكوفة / كلية العلوم

المستخلص:

تُشكـّلُ مجموعـةُ نقـاطِ المنحنـى الإهليليجيـةِ زمـرة أبداليـة، التـي اعتبـرت كاختيار مناسب لبناء مشكلة مشابهة لمشكلةِ اللوغاريتم المنفصلةِ. هذا يُنشأ ويفتح باب جديد لمعالجةِ زمراً خاصة وعمليات جديدة.

في هذا البحث، حاولنا الاستفادة نظام ديفي– هيلمان لاستبدال المفاتيح وذلك باستعمالها كمفتـاح سـري فـي طـريقتين مقتـرحتين للتشـفير باسـتخدام المنحنيـات الإهليليجية.

I: Introduction:

Elliptic Curve systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz from the University of Washington, and Victor Miller [1]. The elliptic curve cryptosystem (ECC) was thus created. Since then, numerous researchers and developers have spent years researching the strength of ECC and improving techniques for its implementation. Today, the scientific efforts are looking for a

smaller and faster public key cryptosystem, a practical and secure technology, even for the most constrained environments [2].

For any cryptographic system based on the DLP, there is an analogue for Elliptic Curve [3]. One of these systems is Diffie – Helman key exchange system.

This paper proposed methods to encrypt and decrypt the message, by using the Diffie–Hellman Exchanging key (which is a secrete point in the proposed methods ($\mathbf{PM_1}$) and ($\mathbf{PM_2}$)**.**

2: Diffie – Helman key exchange system

This system is merely a method for exchanging key; no massages are involved. The following algorithm illustrates this system [3]. Suppose two communication parties, Ali and Benin, want to agree upon a key.

They first fix a finite field $\mathbf{F_q}$, an elliptic curve **E** defined over it and a base point $\mathbf{B \in E}$ (with high order). To generate a key, first Ali chooses a random $\mathbf{a \in Fq}$ (which is approximately the as the number **N** of point of **E** [3]) which he keeps secret. Next, he calculates $\mathbf{aB \in E}$ that is public and sends it to Bob. Benin does the same steps, i.e. she chooses a random integer **b** (secret) and calculates **bB**, which is sent to Ali. Their secret common key is then
$\mathbf{P = abB \in E}$ [4]. The following algorithm illustrates this system.

2-1 The Algorithm of Diffie – Helman key exchange system

- Ali and Benin first choose a finite field $\mathbf{F_p}$ and an elliptic curve **E** defined over it ($\mathbf{E(F_p)}$).
- They publicly choose a random base point $B \in E$.
- Ali chooses a secret random integer e. He then computes $eB \in E$. In addition, send it to Benin.

- Benin chooses a secret random integer d. She then computes dB∈ E. and send it to Ali.
- Then eB and dB are public and e and d are secret.
- Ali computes the secret key edB = e(dB).
- Benin computes the secret key edB = d(eB).

There is no fast way to compute **edB** if only knows **B**, **eB** and **dB**, this is ELDLP.

After these setups, Ali and Benin have the same point (only Ali and Benin know it). Then to start with ($\mathbf{PM_1}$) and ($\mathbf{PM_2}$), let us consider the following algorithms:

Algorithm of (PMI)

- Ali and Benin Compute edB = S = (s1 , s2) .(using Diffie – Hellman Scheme)
- Ali sends a message M∈ E to Benin as follows:
- Compute (s1 * s2)mod N = K.
- Compute K*M = C, and send C to Benin.
- Benin receives C and decrypts it as follows:
- Compute (s1 * s2) mod N = K.
- Compute (K–1)mod N. (where N = #E)
- K–1*C = K–1*K*M = M.

Algorithm of (PM2)

- Ali and Benin Compute edB = S = (s1 , s2) .(using Diffie – Hellman Scheme)
- Ali sends a message M to Benin as follows:
- Compute ($s_1^{s_2}$)mod N = K.
- Compute K*M = C, and send C to Benin.
- Benin receives C and decrypts it as follows:

- Compute ($s_1^{s_2}$)mod N = K.
- Compute (K–1) mod N.
- K–1*C = K–1*K*M = M.

System Test:

Let **E** be an elliptic curve define over $\mathbf{F_p}$ where **p = 3023** with parameters **a = 1, b = 2547** where $(\mathbf{4a^3+27\ b^2})\mathbf{mod\ p = 2027 \neq 0}$. and **#E = 3083**.

Since **#E** is prime number then by theorem(1), every point on **E** in base point, therefore let **B =** (**2237, 2480**).

To apply this system test using ($\mathbf{PM_1}$), at first we must apply Diffie–Hellman Exchanging key

- Ali chooses a secret random integer e = 2313.
- eB = 2313 (2237 , 2480) = (934 , 29)
- And send (934, 29) to Benin .
- Benin chooses a secret random integer d = 1236.
- dB =1236 (2237 , 2480) = (1713, 1709)
- And send (1713 , 1709) to Ali
- Ali computes the secret key e (dB) = 2313 (1713, 1709).
- edB = (2537 , 1632) = S
- Benin computes the secret key d (eB) =1236 (934, 29).
- deB = (2537 , 1632) = S

Now, Ali and Benin have the same point **S =** (**2537, 1632**)

If Ali send a message **M =** (**2284, 2430**) to Benin

— Compute $(\mathbf{s_1 * s_2})$ **mod p =** (**2537 * 1632**) **mod 3083**

= 2998

= K.

(1) Theorem: Let $E(F_p)$ is an elliptic curve E defined over the finite field F_q have prime order $\#E$, then for all $P \in E(F_q)$ and $P \neq O$, then P have the order $m = \#E$. Then P generates subgroup equal to $E(F_q)$ [3] .

— Compute **K*M = 2998** (**2284, 2430**)
= (2179, 1833)
= C, and send it to Benin.

— Benin receives **C** and decrypts it as follows:

— Compute $(s_1 * s_2)$ **mod p = 2998**
= K

— Compute (K^{-1}) **mod N =** $(2998)^{-1}$ **mod 3083**
= 1342

— K^{-1} **C =1342** (**2179, 1833**)
= (2284, 2430)

To apply this system test using the algorithm (PM_2), at first we must apply Diffie–Hellman Exchanging key.

By the same procedure to solve Diffie – Helman scheme we have obtained

S = (2537, 1632)

If Ali sends a message **M = (2284, 2430)** to Benin using (PM_2), he does the following:

— Compute (s_1^{s2}) **mod N =** (2537^{1632}) **mod 3083**
= 323
= K.

— Compute **K* M = 323** (**2284, 2430**)
= (2555, 1066)
= C, and send it to Benin.

— Benin receives **C** and decrypts it as follows:

— Compute (s_1^{s2}) **mod N = 323**
= K.

— Compute (K^{-1}) **mod N =** $(323)^{-1}$ **mod 3083**
= 1594.

—K^{-1} **C = 1594** (**2555 , 1066**)
= (2284, 2430)

$= \mathbf{M}$.

3:Conclusion

The Diffie–Helman scheme is one of the exchanging key cryptosystem, no massages are involved in this scheme, in this report, we try to benefit from this scheme by use the key (which exchange it) as a secret key. (that is, we know now the one of the advantages of the Diffie–Helman key exchange system).

We proposed two different methods to encrypt and decrypt the message. In the second method, we support the system more security of the first method, because the sender compute the exponentiation function between the coordinates of the key in the encryption algorithm (use fast exponentiation method), and the receiver compute the inverse of the exponentiation function between the coordinates of the key in the decryption algorithm. While in the first method, the sender compute the multiplication between the coordinates of the key in the encryption algorithm, and the receiver compute the multiplication between the coordinates of the key in the decryption algorithm.

4: References

[1] **Hankerson, D. and Menezes, A. (2003), "Elliptic Curve Cryptography", University of Waterloo.**

[2] **Meng, T.K. (2001),"Curves For The Elliptic Curve Cryptosystem", M.S.C. Thesis, University of Singapore.**

[3] **Sagheer, A.M. (2004), "Enhancement of Elliptic Curves Cryptography Methods", M.S.C. Thesis, University of Technology, Baghdad.**

[4] **Oswald, E. (2002), "Introduction to Elliptic Curve Cryptography", Institute for Applied Information Processing and Communication, Graz University Technology.**