رفعت زيدان خلف

Friday, December 24, 2010
2:48 PM

أنظمة تشفير المفتاح المعلن باستخدام التشاكل الزمري

*رفعت زيدان خلف** *ناجي مطر سحيب**

تاريخ قبول النشر 13 / 7 / 2008

الخلاصة :-

في هذا البحث تمت الاستفادة من مفهوم التشاكل الزمري (group isomorphism) في بناء بعض انظمة تشفير المفتاح المعلن (public keycipher system) حيث تم بناء :-

1- خوارزمية الجمال (EL-Gamal)

2- خوارزمية تبادل المفتاح (key exchange)

كلمات مفتاحية : خوارزمية الجمال, التشاكل ألزمري

المقدمة :

ان الاهتمام المتزايد بحماية المعلومات ادى الى تطوير في علم التشفير وخاصة في مجال انظمة تشفير المفتاح المعلن التي تتميز باستخدامها مفتاحين مختلفين للتشفير ، المفتاح الاول كمفتاح مرسل (Receiver key) والذي يكون عام (معلن) اما المفتاح الثاني كمفتاح مستقبل (Sender key) والذي يكون سري علما بان عملية اكتشاف المفتاح السري عن طريق معرفة المفتاح العام الذي يجب ان تكون عملية معقدة جدا,إن معظم انظمة التشفير الحديثة تستخدم مشكلة اللوغاريتم المتقطع(DLD)لبناء خوارزمياتها والتي تمثل دالة المسار الواحد(one way function) وتتصف بما يلي:-

1- يمكن حساب الدالة ببساطة.

2- حساب معكوس الدالة عملية معقدة جدا.

والطريقة الشائعة لمهاجمة جميع انظمة التشفير والتي تعتمد على ال DLD هو ايجاد خوارزمية معينةلحساب معكوس الدالة في وقت قصير نسبيا وحالما يتم ايجاد مثل هذه خوارزمية ضمن زمرة (group) معينة فان هذه الانظمة سوف تكسر وهو اقصى مايطلب المهاجمون واننا اذا استطعنا ان تكون زمرة بالمواصفات خاصة وتحقق الشروط (2,1) اعلاه فاننا سوف تكون انظمة تشفير مثالية وهذا في الواقع موجود غير ان هنالك زمرة تقترب في هذه الحالة مثل الزمرة الضربية F_q^* (q عدد اولي) والزمرة (Z/nZ)

التشاكل الزمري (group isomorphism) [1]

لتكن كل من (G_1,.) و(G_2,.) زمرة , يقال لدالة $F: G \to G'$ بانها تشاكل زمري اذا كان $f(a,b)= f(a).f(b)$ لكل $a,b \in G$, اما اذا كانت الدالة f متباينة وشاملة فيقال للتشاكل بانه تشاكل تقابلي زمري ويقال للزمرتين $(G, \circ)$و ($G',*$) بانهما متشاكلتين تقابليا ويرمز لهما بالرمز $G \approx G'$

خوارزمية الجمال (EL-Gamal Algorithem)

1-ليكن p عدد اولي كبير .

2-ليكن P:Fp فضاء النص الواضح (Plan text space).

3- ليكن C:Fp*x Fp فضاء النص المشفر (cipher text space).

4- أختر عنصر اولي$\alpha \in Fp^*,\ \alpha \in Z/(p-1)Z$.

5-ضع $\beta = \alpha^a$.

6- القيم α,β,p معلنة و a سرية .

7- تعرف دالة التشفير $e_{\alpha,\beta}$ بواسطة

$$e_{\alpha,\beta}(X,k) = (\alpha^k \bmod p, X \beta^k \bmod p) =(C_1,C_2)$$

حيث ان X هو العنصر الواضح و $k \in Z/(P-1)Z$ عنصر عشوائي

8- نعرف الدالة الحل d_a بواسطة

$$D_a(C_1,C_2)=C_1C_2^{-a} \bmod p$$

حيث $C \in (C_1,C_2)$

$d_a= e_{\alpha,\beta}(X,k)=k$-9

*جامعة ديالى – كلية العلوم – قسم الرياضيات

خوارزمية الجمال باستخدام التشاكل الزمري

(EL – Gamal Algorithm with group isomorphism)

لتكن G زمرة ابيلية (Abelian group) و g $\in$ G عنصر ثابت وليكن $H=\langle g\rangle$ زمرة جزئية دائرية (cyclic set group) من G رتبتها n.

تعرف الدالة f

$$f: Z/nZ \rightarrow H$$

ان الصورة $f(a)=ag$

$$=\underbrace{g+g+g+\dots\dots\dots+g}_{a \text{ من المرات}}$$

ليكن $t \in Z/nZ$ (المفتاح السري)

فان

$V=f(t)\in H$ (المفتاح المعلن)

التشفير:

$M\in H$ (النص الصريح) و $r\in Z/nZ$ عنصر عشوائي

فان

$C_1=f(r)$

$C_2=rv+M$

النص المشفر هو $(C_1, C_2) \in H\times H$

حل الشفرة:

$m=C_2-C_1$

مثال:

P=31

$Gf(31)=\{0,1,2,3,\dots,30\}$

g=2

$H:\langle 2\rangle=\{0,1,2,3,\dots,30\}$

n=31

$Z/31Z=\{0,1,2,3,\dots,30\}$

$f: Z/31Z \longrightarrow H$

t=12 المفتاح السري

المفتاح المعلن $V=f(t)=f(12)=2^{12}=24$

التشفير :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	

النص الواضح :

N	a	j	I
13	0	9	8
m_1	m_2	m_3	m_4

$m_1=13$

عشوائي $r_1=20$

$C_{11}=f(r_1)=f(20)=2^{20}$ mod 31=40mod13=9

$C_{21}=r_1v+m_1=(20*24+13)\text{mod}31=28$

$m_1=13\rightarrow(C_{11},C_{21})=(9,28)$

$m_2=0$

$r_2=13$

$C_{12}=f(r_2)=f(13)=2^{13}\text{mod}31=26$

$C_{22}=r_2v+m_2=(13*24+0)\text{mod}31=2$

$m_2=0\rightarrow(C_{12},C_{22})=(26,2)$

$m_3=9$

$r_3=17$

$C_{13}=f(r_3)=f(17)=2^{17}\text{mod}31=34\text{mod}31=3$

$C_{23}=r_3v+m_3=(17*24+9)\text{mod}31=14$

$m_3=9\rightarrow(C_{13},C_{23})=(3,14)$

$m_4=8$

$r_4=5$

$C_{14}=f(r_4)=f(5)=2^5\text{mod}31=10$

$C_{24}=r_4v+m_4=(5*24+8)\text{mod}31=4$

$m_4=8\rightarrow(C_{14},C_{24})=(1,4)$

النص المشفر (9,28),(26,2),(3,14),(1,4)

$(C_{11},C_{12})=(9,28)$

$m_1=C_{12}-tC_{11}$

$m_1 = (28-12*9) mod31$

$m_1 = (28-15) mod31$

$m_1 = 13 \rightarrow N$

$(C_{21}, C_{22}) = (26,2)$

$m_2 = C_{22} - tC_{21}$

$m_2 = (2-12*26) mod31$

$m_2 = (2-2) mod31$

$m_2 = 0 \rightarrow a$

$(C_{13}, C_{23}) = (3,14)$

$m_3 = C_{23} - tC_{13}$

$m_3 = (14 - 12*3) mod31$

$m_3 = 9 \rightarrow j$

$(C_{14}, C_{24}) = (10,4)$

$m_4 = C_{24} - tC_{14}$

$m_4 = (4 - 12*10) mod31$

$m_4 = (4+(-27)) mod31$

$m_4 = (4+4) mod31$

$m_4 = 8 \rightarrow C$

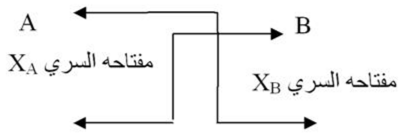
تبادل المفاتيح key exchange

سوف نعطي خوارزمية لتبادل المفاتيح من طريقتين او اكثر اعتمادا على مفهوم التشاكل الزمري

$F: Z \backslash nZ \rightarrow H$

$X \in Z \backslash nZ \rightarrow \quad y = f(x) \in H$

المفتاح السري ↓ — المفتاح المعلن ↓



مفتاح المعلن	مفتاح المعلن
$Y_A = f(X_B)$	$Y_B = f(X_A)$
$K_{AB} = X_A Y_B$	$K_{BA} = X_B Y_A$
$= X_A F(X_B)$	$= X_B F(X_A)$
$= F(X_A X_B)$	$= F(X_B X_A)$

$K_{AB} = K_{BA} = K$

مثال:

$P = 10$

$GF(10) = \{0,1,2,\ldots\ldots,9\}$

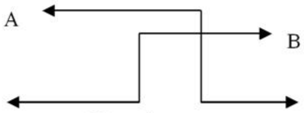
$g = 2$

$H: <2> = \{0,2,4,4,6,8\}$

$n = 5$

$f: Z \backslash 5Z \rightarrow H$

$f(t) = 2^t$



سري $X_A = 4$	سري $X_B = 3$
المعلن $Y_A = 2^4 = 8$	المعلن $Y_B = 2^3 = 8$
$K_{AB} = X_A = X_A X_B$	$K_{AB} = X_B X_A$
$= (4*6) mod10$	$= (3*8) mod10$
$= 4$	$= 4$

$K_{AB} = K_{BA} = 4$

References:

1. schnerier, B, 1996, Applied Cryptography, 2nd edition, p 280, New York UAS, Joha of sons.
2. Denning, D, 1985, Cryptography and data security, 1st edition, p350, London, England, Addison - Wesley.
3. Cohen, H, 2000, a course in computational Algebraic number Theory, 1st edition, p540, London, England, Addison-wesley.
4. Imai, H, 1996, Lecture notes in computer science, 1st edition, 1751, NewYork, UAS, Joha of sons.
5. Salomaa, A, 2007, public key cryptography, 6th edition, p450, berlin, Germany, Springer-verlage.

Public key system by using isomorphism group

Rifat Zeadan khalef* ***Naji muter sahib****

University of Diyala College of science Department of math

Keyword: EL-Gamal Algorithm, group isomorphism

Abstract :

In this paper we deal with the problem of ciphering and useful from group isomorphism for construct public key cipher system, Where construction
1-EL- Gamal Algorithm. 2- key- exchange Algorithm