氣功的鑰匙

組員:楊子賢、林冠宇
指導教授:洪斌哲

前言: 我們的研究主要來探討利用離散型的傅立葉轉換公式來改寫成同餘計算的方式所構成的加解密系統，以及解鎖密文需要用到的由橢圓曲線(ECC)所製造出的交換密鑰系統，讓傳送者藉由交換密鑰方式，安全的傳送密鑰給接受者，密鑰是我們這個題目的重點，而密鑰只能雙方知道，以外的第三者是不會知道的，這兩大系統構成的密碼系統，其實主要源頭是整數論以及代數理論構成的系統，底下將為大家展示研究成果。

橢圓曲線交換密鑰系統:

E : $y^2 \equiv x^2 + ax + b \ mod\ (p)$, a,b $\in Z_p$

$\Longrightarrow$ E(Z_p) = { (x,y)$\in$ Z_p^2 , (x,y) satisfies E} $\cup$ {∞} ,

$E(Z_p) \cong Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_r}$ (Mordell – Weil定理)

取 (1,0,⋯,0) $\in Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_r}$ ，

因為E(Z_p) 和 $Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_r}$ 是同構關係(group homomorphism)，

所以 (1,0,⋯,0) 可以對應到一個 P = (x_0 , y_0)。

因為 (n_1, 0 , ⋯ , 0) = (0 , ⋯ , 0) (mod n_1)，

所以 P 經過 n_1 次運算後會等於 {∞}

$\Longrightarrow$P$\oplus$P$\oplus\cdots\oplus$P = n_1P = ∞

基於上面的原因 所以Bob選的d和Mary選的e必須滿足互質條件

(d ,n_1) = 1 and (e ,n_1) = 1(底下的 ‘運算’ 是橢圓曲線群的運算)

	Bob	傳送鏈	Mary
任取一個正整數	d		e
對P做d 次運算傳送給Mary	dP	→	
對P做e 次運算傳送給Bob		←	eP
對P做d+e次運算	deP		edP

deP = edP = (x_{de} , y_{de}) $\in$ E(Z_p),最後把$x_{de} + y_{de}$ = C mod (p-1)，再把C + n

就會是密鑰 q (這裡的n是雙方先規定好找一個最小的正整數n,目的是讓得出的密鑰q與p-1互質)

英文跟數字的轉換:
原本:空格 A B C D E F G H I J K L M N O P Q R S T U V W
轉換: 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23
原本: X Y Z 0 1 2 3 4 5 6 7 8 9
轉換:24 25 26 27 28 29 30 31 32 33 34 35 36

資料的加解密系統演算程序圖:

(1)基本先前作業:

令 p 為質數和p > 2

固定一個 order 為 p-1 的 $\omega \in Z_p$ ，(p-1是最小正整數使得ω^{p-1}=1)

令 $\xi \in \{\omega^q | \ gcd\ (q, p-1) = 1\}$，此時$\xi$的order也會是p-1 (p-1是最小正整數使得ξ^{p-1}=1)

密鑰: q and ξ

公鑰: p and ω

資料形式: $(a_1, a_2, \ldots, a_{p-1}) \in Z_p^{p-1}$

加密: $\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{p-1} \end{bmatrix} \equiv \begin{bmatrix} \xi^{-1} & \xi^{-2} & \cdots & \xi^{-(p-1)} \\ \xi^{-2} & \xi^{-4} & \cdots & \xi^{-2(p-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \xi^{-(p-1)} & \xi^{-2(p-1)} & \cdots & \xi^{-(p-1)^2} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_{p-1} \end{bmatrix}$ (mod(p))

解密: $\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_{p-1} \end{bmatrix} \equiv (p-1)^{-1} \begin{bmatrix} \xi & \xi^2 & \cdots & \xi^{(p-1)} \\ \xi^2 & \xi^4 & \cdots & \xi^{2(p-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \xi^{(p-1)} & \xi^{2(p-1)} & \cdots & \xi^{(p-1)^2} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{p-1} \end{bmatrix}$ (mod(p))

(2)演算法

令 A = $\begin{bmatrix} \xi^{-1} & \xi^{-2} & \cdots & \xi^{-(p-1)} \\ \xi^{-2} & \xi^{-4} & \cdots & \xi^{-2(p-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \xi^{-(p-1)} & \xi^{-2(p-1)} & \cdots & \xi^{-(p-1)^2} \end{bmatrix}$ 和 B = $(p-1)^{-1} \begin{bmatrix} \xi & \xi^2 & \cdots & \xi^{(p-1)} \\ \xi^2 & \xi^4 & \cdots & \xi^{2(p-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \xi^{(p-1)} & \xi^{2(p-1)} & \cdots & \xi^{(p-1)^2} \end{bmatrix}$

製作鑰匙 q

傳送者:

先把英文字和數字轉換成對應3的進位的係數向量 $\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_{p-1} \end{bmatrix}$

加密 : $\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{p-1} \end{bmatrix}$ = A · $\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_{p-1} \end{bmatrix}$

傳送密文 : $\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{p-1} \end{bmatrix}$

接收者:

解密: $\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_{p-1} \end{bmatrix}$ = B · $\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{p-1} \end{bmatrix}$

把三進位係數向量 $\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_{p-1} \end{bmatrix}$ 轉回對應的英文字與數字

實例:

E(Z_5) = { (x , y) ϵ Z_5 : $y^2 \equiv x^3 + x + 1\ (mod\ 5)$ } $\cup$ {∞}
= {∞ , (2,1) , (2,4) , (3,1) , (3,4) , (4,2) , (4,3) , (5,1) , (5,4)}
|E(Z_5)| = 9 ，所以 Alice 選 d 和 Bob 選 e 使得 (d,3) = 1 , (e,3)=1
假設 d = e = 2
起始點為 P = (3,1)

Alice		Bob
dP	→	
	←	eP
deP = (4,2)		deP = (4,2)

4 + 2 = 6 ≡ 2 mod 4
因為 gcd (2 + C , 4) = 1 ， 使得 C = 1
所以 q = 3
ω = 2
$\xi = 2^3 = 8 \equiv 3 \ mod(5)$
$\xi^{-1} = 2 \ mod(5)$

Alice 的明文為 Justin
所以她對應 的 3 進位係數矩陣 $\begin{bmatrix} 1 & 0 & 1 & 2 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 2 & 2 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{matrix} 3^0 \\ 3^1 \\ 3^2 \\ 3^3 \end{matrix}$

加密: $\begin{bmatrix} 2 & 4 & 3 & 1 \\ 4 & 1 & 4 & 1 \\ 3 & 4 & 2 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 2 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 2 & 2 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 & 3 & 0 & 3 & 1 \\ 3 & 4 & 2 & 1 & 4 & 3 \\ 0 & 3 & 2 & 0 & 2 & 2 \\ 2 & 3 & 3 & 4 & 1 & 4 \end{bmatrix} \ mod(5)$ (密文矩陣)

解密: $4 \cdot \begin{bmatrix} 3 & 4 & 2 & 1 \\ 4 & 1 & 4 & 1 \\ 2 & 4 & 3 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 3 & 0 & 3 & 1 \\ 3 & 4 & 2 & 1 & 4 & 3 \\ 0 & 3 & 2 & 0 & 2 & 2 \\ 2 & 3 & 3 & 4 & 1 & 4 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 & 1 & 2 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 2 & 2 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \ mod(5)$

所以 Bob 得回明文的三進位係數矩陣，再將係數矩陣轉換回來，可以得到原明文Justin

結論:

我們用橢圓曲線系統來製作雙方的鑰匙，這樣做出來的鑰匙比較不容易被破解，然後在設計一個離散型傅立葉轉換公式來做加密跟解密系統，安全性在密碼學中有著很重要的地位，加密者與解密者雙方一定要保護好密鑰，以免洩漏，而加解密所使用的質數p通常可以很大，這時要用用程式計算。

參考資料:

A first course in wavelets with fourier analysis (second edition)
Cryptography theory and practice (third edition)
The arithmetic of elliptic curves 作者:Joseph H.Silverman