PAC 1

Sílvia Sanvicente García

abril 2022

Exercici 1 (2 punts)

L'Alice i el Bob volen fer servir un intercanvi de claus Diffie-Hellman per trobar un secret comú del qual en derivaran una clau secreta per a un algorisme simètric. Acorden fer servir el nombre primer p = 941 i l'arrel g = 627 com a valor públics. Si l'Alice pren com a clau privada a = 347 i el Bob pren com a clau privada b = 781, quin és el valor secret comú?

L'algoritme d'intercanvi de claus de Diffie-Hellman consta dels següents passos:

1. Se seleccionen els valors públics p i alpha
2. A tria el valor aleatori a i calcula kpubA
3. B tria un valor aleatori b i calcula kpubB
4. A i B intercanvien els seus valors kpub
5. A deriva la clau compartida, calculant kAB
6. B deriva la clau compartida, calculant kAB

A continuació es mostra el codi utilitzat per calcular el valor secret comú:

```
def calcularKPUB(alpha, x, p):
    kpub = pow(alpha, x, p)
    return kpub
```

```
def calcularKAB(kpub, x, p):
    kAB = pow(kpub, x, p)
    return kAB
```

```
p = 941
alpha = 627

a = 347
kpubA = calcularKPUB(alpha, a, p)
print("kpubA: ", kpubA)

```

```
b = 781
kpubB = calcularKPUB(alpha, b, p)
print("kpubB: ", kpubB)

kAB = calcularKPUB(kpubB, a, p)
print("kAB: ", kAB)

kAB = calcularKPUB(kpubA, b, p)
print("kAB: ", kAB)
```

El valor secret comú és 470.

Exercici 2 (3 punts)

L'Alice i el Bob decideixen fer servir el mètode de xifratge ElGamal per a les seves comunicacions. Com a valors públics prenen p = 1373 i g = 2.

(1) Si l'Alice fa servir a = 947 com a clau privada, quina és la seva clau pública A?

(2) La clau privada del Bob és b = 716, quina és la seva clau pública B?

(3) Si l'Alice xifra el missatge m = 583 fent servir la clau temporal k = 877, quin és el missatge xifrat (c1, c2) que rep el Bob?

(4) L'Alice decideix canviar la seva clau privada per a = 299. Si el Bob envia a l'Alice el missatge xifrat (661, 1325), podeu desxifrar el missatge?

(1) La clau pública amb ElGamal té la següent forma:

$k_{Pub} = (p, \alpha, \beta)$

i β es calcula:

$\beta = \alpha^d \bmod p$

A continuació es mostra el codi per calcular la clau pública:

```
def clau_publica(p, alpha, d):
    beta = pow(alpha, d, p)
    kpub = (p, alpha, beta)
    return kpub
```

```
p = 1373
alpha = 2
a = 947
kpub = clau_publica(p, alpha, a)
print('kpub A: ', kpub)
```

La seva clau pública d'A és $k_{pubA} = (1373, 2, 177)$.

(2) Per a aquest apartat s'ha fet servir el mateix codi que a l'apartat anterior.

La seva clau pública de B és $k_{pubB} = (1373, 2, 469)$.

(3) Per xifrar un missatge amb ElGamal, cal calcular c1 i c2:

$c_1 = \alpha^v \bmod p$

$c_2 = m \cdot \beta^v \bmod p$

A continuació es mostra el codi utilitzat:

```
def xifrarElGamal(p, alpha, kpub, m, v):
    c1 = pow(alpha, v, p)
    c2 = (m * pow(kpub[2], v, p)) % p
    return (c1, c2)
```

```
m = 583
v = 877
(c1, c2) = xifrarElGamal(p, alpha, kpubA, m, v)
print((c1, c2))
```

El missatge xifrat és (719, 618).

(4) Alice no podrà desxifrar el missatge amb la nova clau privada, si aquest ha estat xifrat amb la clau pública antiga. Alice hauria de crear una nova clau pública a partir de la nova clau privada i enviar aquesta clau pública a Bob perquè pugui xifrar el missatge.

Exercici 3 (1 punt)

Considereu la corba el·líptica $E : y^2 = x^3 + 3x + 5$, definida sobre $\mathbb{K} = \mathbb{F}_{19}$. Calculeu el discriminant $\Delta(E)$, proveu que el punt $P = (4, 9) \in E(\mathbb{K})$ i calculeu $2 \cdot P$.

L'equació d'una corba el·líptica i el seu discriminant tenen la forma següent:

$E(F_p) : y^2 = x^3 + ax + b$

$\Delta(E) = -16(4a^3 + 27b^2) \bmod p \neq 0 \bmod p$

En aquest cas:

$E(F_{19}) : y^2 = x^3 + 3x + 5$

$\Delta(E) = -16(4 \cdot 3^3 + 27 \cdot 5^2) \bmod 19 = 12$

Podem comprovar que un punt pertany a la corba verificant que compleix l'equació que defineix la corba:

$E(F_{19}) : y^2 = x^3 + 3x + 5$

$9^2 = 4^3 + 3 \cdot 4 + 5 \bmod 19$

$5 = 5 \bmod 19$

Podem calcular $2P$ de la següent manera:

$2P = P + P$

$m = \frac{3x^2+a}{2y} \bmod p$

$x_{2P} = m^2 - 2x \bmod p$

$y_{2P} = m(x - x_{2p}) - y \bmod p$

En aquest cas:

$m = \frac{3 \cdot 4^2+3}{2 \cdot 9} \bmod 19 = \frac{17}{6} \bmod 19 = 6$

$x_{2P} = 6^2 - 2 \cdot 4 \bmod 19 = 28 \bmod 19 = 9$

$y_{2P} = 6(4 - 9) - 9 \bmod 19 = -39 \bmod 19 = 18$

$2P = (9, 18)$

Exercici 4 (3 punts)

L'Alice i el Bob faran servir la versió sobre corbes el·líptiques de l'intercanvi de claus Diffie-Hellman fent servir el primer $p = 2671$, la corba $E : y^2 = x^3 + 171x + 853$ i el punt $P = (1980, 431) \in E(\mathbb{F}_{2671})$.

(1) Si l'Alice envia el punt $Q_A = (2110, 543)$ i el Bob fa servir la clau privada $n_B = 1943$, quin punt ha d'enviar el Bob a l'Alice?

(2) Quin és el valor secret comú?

(3) L'Alice i el Bob decideixen tornar a executar l'algorisme amb els mateixos paràmetres públics, però ara l'Alice només envia la coordenada $x_A = 2$ del seu punt Q_A. El Bob ha canviat la seva clau secreta $n_B = 875$. Quin valor, modulo p, ha d'enviar el Bob a l'Alice? Quin és el valor secret comú?

(1) Bob ha d'enviar la seva clau pública, k_{pubB}, la qual es calcula:

$k_{pubB} = n_B \cdot P = 1943 \cdot (1980, 431) = (1432, 667)$

(2) El valor secret comú es calcula de la següent forma:

$k_{AB} = n_B \cdot Q_A = 1943 \cdot (2110, 543) = (2424, 911)$

(3) La nova clau pública de Bob és:

$k_{pubB} = n_B \cdot P = 875 \cdot (1980, 431) = (161, 2040)$

Per calcular el valor secret comú, hem de trobar el valor y_A de la clau pública d'Alice, substituint x_A a l'equació de la corba.

$y^2 = 2^3 + 171 \cdot 2 + 853 \bmod 2671$

$y = 96 \bmod 2671$

$y = -96 \bmod 2671 = 2575 \bmod 2671$

Atès que el segon resultat és l'invers del primer, ens quedem amb el valor $y_A = 96$.

$k_{AB} = n_B \cdot Q_A = 875 \cdot (2, 96) = (1708, 1252)$

Nota: Per fer aquest exercici s'han utilitzat les eines Elliptic Curve Scalar Multiplication i Wolframalpha.

Exercici 5 (1 punt)

Siguin E una corba el·líptica sobre un $\cos \mathbb{K}$ i $\{P_1, P_2\}$ una base per $E[n]$. Proveu que el pairing de Weil, $e_n(P_1, P_2)$, és una arrel n-èssima de la unitat. Observació: teniu present que el pairing de Weil és no degenerat per acabar la demostració.

Podem definir les funcions següents:

$$\operatorname{div}(f_{P_1}) = n(P_1) - n(\mathcal{O})$$
$$\operatorname{div}(f_{P_2}) = n(P_2) - n(\mathcal{O})$$

I definir el pairing de Weil, on S un punt aleatori de la corba:

$$e_n(P_1, P_2) = \frac{f_{P_1}(P_2 + S)}{f_{P_1}(S)} / \frac{f_{P_2}(P_1 - S)}{f_{P_2}(-S)}$$

Podem elevar a la n-èssima potència el numerador del pairing de Weil:

$$\frac{f_{P_1}(P_2 + S)^n}{f_{P_1}(S)^n} = f_{P_1}(P_2 + S)^n f_{P_1}(S)^{-n} = f_{P_1}(n(P_2 + S) - n(S))$$

I elevar a la n-èssima potència el denominador:

$$\frac{f_{P_2}(P_1 - S)^n}{f_{P_2}(-S)^n} = f_{P_2}(n(P_1 - S) - n(-S))$$

Podem aplicar el teorema de la reciprocitat de Weil, on $n(P_2 + S) - n(S)$ és el divisor de $f_{P_2}(X - S)$:

$$f_{P_1}|_{\operatorname{div}(f_{P_2}(X-S))} = f_{P_2}(X - S)|_{\operatorname{div}(f_{P_1})}$$

I com que $\operatorname{div}(f_{P_1}) = n(P_1) - n(\mathcal{O})$:

$$f_{P_1}(n(P_2+S)-n(S)) = f_{P_2}(n(P_1-S)-n(-S))$$

$$\frac{f_{P_1}(P_2+S)^n}{f_{P_1}(S)^n} = \frac{f_{P_2}(P_1-S)^n}{f_{P_2}(-S)^n}$$

Podem observar que, quan el numerador i el denominador s'eleven a la n-èssima potència, són iguals, així que:

$$e_n\left(P_1,P_2\right)^n = \frac{f_{P_1}(P_2+S)^n}{f_{P_1}(S)^n} / \frac{f_{P_2}(P_1-S)^n}{f_{P_2}(-S)^n} = 1$$

Nota: Per respondre a aquest exercici s'ha llegit l'article Aftuck, A. E. (2011). The Weil pairing on elliptic curves and its cryptographic applications.