

Es 1

Let $E(\mathbb{Z}_{17})$ be the elliptic curve given by the equation $y^2 = x^3 + 7$. Alice and Bob use $G(2,7)$ as generator for an ECDH to obtain a key session k . Alice's secret key is $sk_A = 5$, Bob's secret key is $sk_B = 12$. What of the following is the session key?

The following is the addition table on $E(\mathbb{Z}_{17})$ where ∞ is the neutral element.

∞	∞	(1,5)	(1,12)	(2,7)	(2,10)	(3,0)	(5,8)	(5,9)	(6,6)	(6,11)	(8,3)	(8,14)	(10,2)	(10,15)	(12,1)	(12,16)	(15,4)	(15,13)
∞	∞	(1,5)	(1,12)	(2,7)	(2,10)	(3,0)	(5,8)	(5,9)	(6,6)	(6,11)	(8,3)	(8,14)	(10,2)	(10,15)	(12,1)	(12,16)	(15,4)	(15,13)
(1,5)	(1,5)	(2,10)	∞	(1,12)	(5,9)	(15,13)	(2,7)	(12,1)	(8,14)	(6,6)	(6,11)	(10,15)	(8,3)	(15,4)	(12,16)	(5,8)	(3,0)	(10,2)
(1,12)	(1,12)	∞	(2,7)	(5,8)	(1,5)	(15,4)	(12,16)	(2,10)	(6,11)	(8,3)	(10,2)	(6,6)	(15,13)	(8,14)	(5,9)	(12,1)	(10,15)	(3,0)
(2,7)	(2,7)	(1,12)	(5,8)	(12,16)	∞	(10,15)	(12,1)	(1,5)	(8,3)	(10,2)	(15,13)	(6,11)	(3,0)	(6,6)	(2,10)	(5,9)	(8,14)	(15,4)
(2,10)	(2,10)	(5,9)	(1,5)	∞	(12,1)	(10,2)	(1,12)	(12,16)	(10,15)	(8,14)	(6,6)	(15,4)	(6,11)	(3,0)	(5,8)	(2,7)	(15,13)	(8,3)
(3,0)	(3,0)	(15,13)	(15,4)	(10,15)	(10,2)	∞	(8,14)	(8,3)	(12,16)	(12,1)	(5,9)	(5,8)	(2,10)	(2,7)	(6,11)	(6,6)	(1,12)	(1,5)
(5,8)	(5,8)	(2,7)	(12,16)	(12,1)	(1,12)	(8,14)	(5,9)	∞	(10,2)	(15,13)	(3,0)	(8,3)	(15,4)	(6,11)	(1,5)	(2,10)	(6,6)	(10,15)
(5,9)	(5,9)	(12,1)	(2,10)	(1,5)	(12,16)	(8,3)	∞	(5,8)	(15,4)	(10,15)	(8,14)	(3,0)	(6,6)	(15,13)	(2,7)	(1,12)	(10,2)	(6,11)
(6,6)	(6,6)	(8,14)	(6,11)	(8,3)	(10,15)	(12,16)	(10,2)	(15,4)	(1,5)	∞	(1,12)	(2,10)	(2,7)	(5,9)	(3,0)	(15,13)	(12,1)	(5,8)
(6,11)	(6,11)	(6,6)	(8,3)	(10,2)	(8,14)	(12,1)	(15,13)	(10,15)	∞	(1,12)	(2,7)	(1,5)	(5,8)	(2,10)	(15,4)	(3,0)	(5,9)	(12,16)
(8,3)	(8,3)	(6,11)	(10,2)	(15,13)	(6,6)	(5,9)	(3,0)	(8,14)	(1,12)	(2,7)	(5,8)	∞	(12,16)	(1,5)	(10,15)	(15,4)	(2,10)	(12,1)
(8,14)	(8,14)	(10,15)	(6,6)	(6,11)	(15,4)	(5,8)	(8,3)	(3,0)	(2,10)	(1,5)	∞	(5,9)	(1,12)	(12,1)	(15,13)	(10,2)	(12,16)	(2,7)
(10,2)	(10,2)	(8,3)	(15,13)	(3,0)	(6,11)	(2,10)	(15,4)	(6,6)	(2,7)	(5,8)	(12,16)	(1,12)	(12,1)	∞	(8,14)	(10,15)	(1,5)	(5,9)
(10,15)	(10,15)	(15,4)	(8,14)	(6,6)	(3,0)	(2,7)	(6,11)	(15,13)	(5,9)	(2,10)	(1,5)	(12,1)	∞	(12,16)	(10,2)	(8,3)	(5,8)	(1,12)
(12,1)	(12,1)	(12,16)	(5,9)	(2,10)	(5,8)	(6,11)	(1,5)	(2,7)	(3,0)	(15,4)	(10,15)	(15,13)	(8,14)	(10,2)	(1,12)	∞	(8,3)	(6,6)
(12,16)	(12,16)	(5,8)	(2,1)	(5,9)	(2,7)	(6,6)	(2,10)	(1,12)	(15,13)	(3,0)	(15,4)	(10,2)	(10,15)	(8,3)	∞	(1,5)	(6,11)	(8,14)
(15,4)	(15,4)	(3,0)	(10,15)	(8,14)	(15,13)	(1,12)	(6,6)	(10,2)	(12,1)	(5,9)	(2,10)	(12,16)	(1,5)	(5,8)	(8,3)	(6,11)	(2,7)	∞
(15,13)	(15,13)	(10,2)	(3,0)	(15,4)	(8,3)	(1,5)	(10,15)	(6,11)	(5,8)	(12,16)	(12,1)	(2,7)	(5,9)	(1,12)	(6,6)	(8,14)	∞	(2,10)

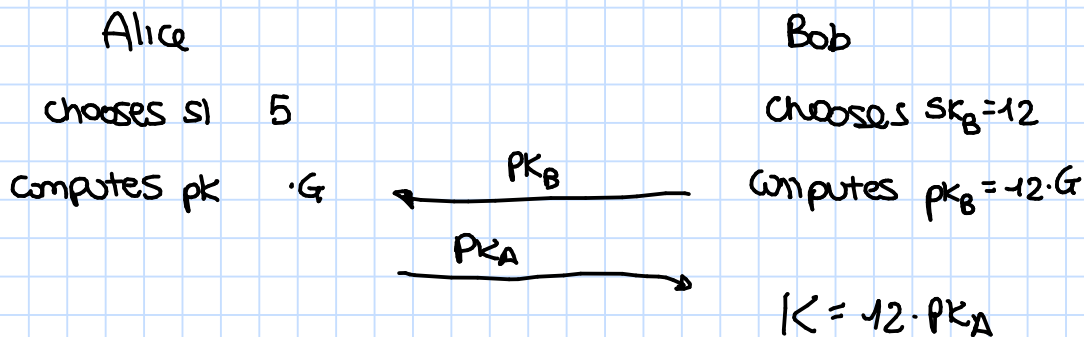
(10,15)

(5,9) X

(6,6)

(5,8)

Protocol:



$$pk_A = 5G = 2G + 2G + G = (12,16) + (12,16) + (2,7) = (-1,5) + (2,7) = (-1,12)$$

$$pk_B = 12G = 5G + 5G + 2G = (-1,12) + (-1,12) + (12,16) = (2,7) + (12,16) = (5,9)$$

$$K = 12pk_A = 12(-1,12) = 6 \cdot 2(-1,12) = 6 \cdot (2,7) = 2(2,7) + 2(2,7) + 2(2,7) = (12,16) + (12,16) + (12,16) = (1,5) + (12,16) = (5,8)$$

Es. 2

Seed $S_0 = 2$

S_1, S_2, \dots numbers generated by a Linear PRNG with $a = 5, b = 1 \bmod 23$

$S_2 = ?$

a) 6

b) 17

c) 15

d) 10 ✓

e) 13

Solution:

$S_0 = \text{seed}$

$$S_{i+1} = aS_i + b \bmod n$$

$$S_1 = aS_0 + b \bmod n = 5 \cdot 2 + 1 \bmod 23 = 11$$

$$S_2 = aS_1 + b \bmod n = 5 \cdot 11 + 1 = 10$$

Es 3

Find $x \in \mathbb{Z}_{401}$ such that $x \cdot 262 \equiv 1 \pmod{401}$ and $5 \cdot x \equiv 375 \pmod{401}$

$$x = 375 \cdot 5^{-1} \pmod{401}$$

$$401 = 5 \times 80 + 1$$

0

$$5 = 1 \times 5 + 0$$

1

$$0 - 80 \pmod{401} \equiv 321$$

$$375 \cdot 321 = 120375 \equiv 75 \pmod{401}$$