INSTITUTO POLITÉCNICO NACIONAL

ESCOM

24-9-2024

Session 4: DHKE with elliptic curves

Nombre: Álvarez García Brandon Azarael

Nombre de la materia: Selected topics in cryptography

Grupo: 7CM1

Nombre de la profesora: Dra. Sandra Díaz Santiago

Ejercicios de programación

1. Let the user establish the public parameters of DHKE with elliptic curves: a prime number p, such that $|p| \geq 4$ bits, a non-singular elliptic curve given by a, b over $\mathbb{Z}_p^*$, and a generator point $G \in \mathbb{E}(a, b)$.

Para la resolución de este ejercicio, simplemente implemento una clase como en las practicas pasadas, en donde pueda definir todos los parámetros de la curva elíptica

```
usage
class DiffieHellmanEllipticCurve:
    def __init__(self, p, a, b, G):
        self.p = p
        self.a = a
        self.b = b
        self.G = G
```

2. Let the user to establish an integer k_A, such that $2 \leq a \leq |\mathbb{E}(a, b)| - 1$ and compute $A = k_A G$.

```
def main():

    ''''
    p = 127
    a = 10
    b = 1
    G = (0, 1, 1)
    ''''

    p = 191
    a = 1
    b = 6
    G = (0, 31, 1)

    dh = DiffieHellmanEllipticCurve(p, a, b, G)

    k_A = int(input("Introduce la clave privada k_A (2 ≤ k_A ≤ p-1): "))

    A = dh.scalar_multiplication(k_A, G)
    print(f"Punto público A = k_A * G: ({A[0]}, {A[1]}, {A[2]})")

    xb = int(input("Introduce el valor de x de BOB: "))
    xy = int(input("Introduce el valor de y de BOB: "))

    point_bob = (xb, xy, 1)

    bob = dh.scalar_multiplication(k_A, point_bob)
    print(f"Punto resultante B = k_A * BOB: ({bob[0]}, {bob[1]}, {bob[2]})")
```

Cree una función llamada main() en donde creo una instancia y aquí solicito el valor de k_a y pueda computar el proceso de DHKE, las funciones son reutilizadas de practicas pasadas, como algoritmo de Euclides, suma de puntos.

Ejecución y pruebas

```
D:\Programs\Anaconda\python.exe "D:\ESCOM\10°Semestre\Cripto 2\Practicas\Practice_4\DHKE.py"
Introduce la clave privada k_A (2 ≤ k_A ≤ p-1): 3
Punto público A = k_A * G: (120, 63, 1)
Introduce el valor de x de BOB: 172
Introduce el valor de y de BOB: 2
Punto resultante B = k_A * BOB: (101, 66, 1)

Process finished with exit code 0
```

```
D:\Programs\Anaconda\python.exe "D:\ESCOM\10°Semestre\Cripto 2\Practicas\Practice_4\DHKE.py"
Introduce la clave privada k_A (2 ≤ k_A ≤ p-1): 5
Punto público A = k_A * G: (172, 2, 1)
Introduce el valor de x de BOB: 120
Introduce el valor de y de BOB: 63
Punto resultante B = k_A * BOB: (101, 66, 1)

Process finished with exit code 0
```

Este proceso fue visualizado por la profesora de forma presencial, las imágenes presentadas es una simulación del proceso que se realizo