



napiš pseudokod pro generování páru klicu v ECDSA



Zde je pseudokód pro generování páru klíčů v ECDSA:

SCSS

Copy code

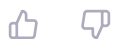
```
// Zvolte křivku a bod G na této křivce
curve, G = select_curve_and_point()

// Vygenerujte náhodné soukromé číslo d
d = random_integer_between_1_and_order_of_G()

// Vypočítejte veřejný klíč Q = d * G
Q = scalar_multiply(d, G)

// Vraťte páru (d, Q)
return (d, Q)
```

V tomto pseudokódu ``curve`` je křivka, na které se bude provádět podpis, ``G`` je bod na této křivce, ``d`` je náhodně vygenerované soukromé číslo a ``Q`` je veřejný klíč, který se vypočítá jako násobek bodu ``G`` a soukromého čísla ``d``. Funkce ``scalar_multiply`` vypočítá násobení bodu ``G`` skalárem ``d``.



napiš pseudokod pro vytvoření podpisu dat ECDSA



Zde je pseudokód pro vytvoření podpisu dat pomocí ECDSA:

SCSS

Copy code

```
// Zvolte křivku a bod G na této křivce
curve, G = select_curve_and_point()

// Zvolte soukromý klíč d a vypočítejte veřejný klíč Q
d, Q = generate_key_pair()
```

```
// Zvolte zprávu, kterou chcete podepsat
message = "Hello, world!"

// Vypočítejte hash zprávy H
H = hash(message)

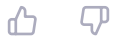
// Vygenerujte náhodné číslo k
k = random_integer_between_1_and_order_of_G()

// Vypočítejte bod R = k * G
R = scalar_multiply(k, G)

// Vypočítejte hodnotu s = (H + d * r) / k mod order_of_G
s = (H + d * R.x) * modular_inverse(k, order_of_G) mod order_of_G

// Vraťte podpis jako dvojici (R, s)
return (R, s)
```

V tomto pseudokódu ``curve`` a ``G`` jsou stejné jako v předchozím pseudokódu. ``d`` a ``Q`` jsou soukromý a veřejný klíč, které jsou vygenerovány pomocí funkce ``generate_key_pair``. ``message`` je zpráva, kterou chcete podepsat, a ``H`` je hash této zprávy. Funkce ``hash`` vypočítá hash zprávy ``message``. ``k`` je náhodné číslo mezi 1 a řádem bodu ``G``. Funkce ``scalar_multiply`` vypočítá násobení bodu ``G`` skalárem ``k``. Funkce ``modular_inverse`` vypočítá modulární inverzi čísla ``k`` vzhledem k řádu bodu ``G``. Bod ``R`` je vypočítán jako násobek bodu ``G`` a náhodného čísla ``k``. Hodnota ``s`` je vypočítána podle ECDSA algoritmu. Podpis je vrácen jako dvojice bodu ``R`` a hodnoty ``s``.



napis pseudokod pro overeni podpisu v ECDSA



Zde je pseudokód pro ověření podpisu dat pomocí ECDSA:

scss

Copy code

```
// Zvolte křivku a bod G na této křivce
curve, G = select_curve_and_point()
```

```
// Získejte veřejný klíč Q a podpis (R, s)
Q = public_key
R, s = signature

// Zvolte zprávu, kterou chcete ověřit
message = "Hello, world!"

// Vypočítejte hash zprávy H
H = hash(message)

// Vypočítejte hodnotu v = H * s^-1 mod order_of_G
v = modular_inverse(s, order_of_G) * H mod order_of_G

// Vypočítejte bod u = v * G + (-v * Q + R)
u = add_points(scalar_multiply(v, G), scalar_multiply(-v, Q) + R)

// Podpis je platný, pokud x-ová souřadnice bodu u je rovna R.x
if u.x == R.x:
    return "Podpis je platný."
else:
    return "Podpis není platný."
```

V tomto pseudokódu ``curve`` a ``G`` jsou stejné jako v předchozích pseudokódech. ``Q`` a ``(R, s)`` jsou veřejný klíč a podpis, který chcete ověřit. ``message`` je zpráva, kterou chcete ověřit, a ``H`` je hash této zprávy. Funkce ``hash`` vypočítá hash zprávy ``message``. ``v`` je vypočítáno podle ECDSA algoritmu. Bod ``u`` je vypočítán podle ECDSA algoritmu. Podpis je platný, pokud x-ová souřadnice bodu ``u`` je rovna ``R.x``.

