情報セキュリティ基礎 演習問題

光成滋生

last update: 2025/11/14

有限体のDH鍵共有

問題

- 大きな素数 p に対して $P \in [1, p-1]$ をランダムに固定して共有する。
  $a \in [1, p-1]$ をランダムに選んで aP を送るDH鍵共有は安全か?

答え

- P と aP から a を求めるには $\bmod p$ で P の逆数 $P^{-1} \bmod p$ を求めればよい。
  これは拡張Euclid互除法などを用いて容易に計算できるため aP に掛けて a が求まり、DLPが解けるので安全ではない。

RSA関数

問題

- $p = 100003, q = 20011, n = p * q$ とする。
  $e = 17$ に対応するRSA関数 $f(x) = x^d \bmod n$ の d を求めよ。
  このとき $x^e = 2025 \bmod n$ となる x は何か。

答え

```
p=100003
q=20011
n = p * q
e = 17
d = pow(e, -1, (p-1)*(q-1))
x = pow(2025, d, n)
```

```
>>> d
235416473
>>> x
1724678439
```

有限体の四則演算

問題

- $p = 100003$ のとき、$\mathbb{F}_p$ 上で演算する。
  $a = 1000, b = 2000$ とする。
  $a + b =$
  $a - b =$
  $a \times b =$
  $1/b =$
  $a/b =$

答え

```
>>> p=100003
>>> a=1000
>>> b=2000
>>> (a+b)%p,(a-b)%p,(a*b)%p,pow(b,-1,p),((a*pow(b,-1,p))%p)
(3000, 99003, 99943, 66652, 50002)
```

楕円曲線の加法

問題

- $p = 100003, \mathbb{F}_p$ 上の楕円曲線 $y^2 = x^3 + 1$ を考える。
  $P_1 = (x_1, y_1) = (0, 1), P_2 = (x_2, y_2) = (-1, 0)$ のとき
  $P_3 = (x_3, y_3) = P_1 + P_2$を求めよ。

答え

- $\lambda = (y_2 - y_1)/(x_2 - x_1) = (0 - 1)/(-1 - 0) = 1,$
  $x_3 = \lambda^2 - x_1 - x_2 = 1 - 0 - (-1) = 2,$
  $y_3 = \lambda(x_1 - x_3) - y_1 = 1(0 - 2) - 1 = -3$

よって $P_3 = (2, -3) = (2, 100000)$

楕円曲線の加法の定義

問題

- 条件X「$P = (x_1, y_1), Q = (x_2, y_2)$ に対して $x_1 = x_2$ で $y_1 = 0$」のとき
  $\lambda = (3x_1^2 + a)/(2y_1)$ の分母が0となってλを計算できない。
  講義の楕円曲線の演算の定義は間違えているのか?

答え

- 条件Xが成り立つ状況を考える。$x_1 = x_2$ で $y_1 = 0$ だから
  $y^2 = x^3 + ax + b$ に $x = x_2$ を代入すると右辺は0となり $y_2 = 0$
  よって $P = (x_1, 0) = Q$
  y 座標が 0 なので $Q = -Q = -P$ でもある。
  対偶を取ると「$Q \neq -P$ ならば条件Xは成り立たない」
  つまり条件Xは除外されているので問題ない。