256 ビット ECC(ECC-256)の推奨係数

1. 楕円曲線暗号(ECC)の係数

素数型の楕円曲線の式は下記

$y^2 = x^3 + ax + b \pmod p$

ここで、x,y,a,b は整数で p 及び r(位数)は素数。

楕円曲線上の任意の点 Q=(Qx,Qy)に対し、r×Q は無限遠点になる。

p と r には$p - \sqrt{p} < r < p + \sqrt{p}$の関係がある。

2. 256 ビット ECC の係数

ANSI 及び NIST の推奨パラメータを示す。

ANSI(米国国家規格協会)のパラメータの名称の先頭は secp である。

NIST(米国国立標準技術研究所)のパラメータの先頭は NIST である。

3. secp256k1

Koblitz 型。a=0 で b が小さい奇数が特徴。

(1) 16 進表示

p=fffffffffffffffffffffffffffffffffffffffffffffffffffffffefffffc2f

r=fffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd0364141

a=0

b=7

(2) 10 進表示

p=115792089237316195423570985008687907853269984665640564039457584007908834671663

r=115792089237316195423570985008687907852837564279074904382605163141518161494337

a=0

b=7

4. secp256r1, NIST P-256

ランダム型。a=p-3 が特徴。

(1) 16 進表示

p=ffffffff00000001000000000000000000000000ffffffffffffffffffffffff

r=ffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551

a=ffffffff00000001000000000000000000000000ffffffffffffffffffffffffc

b=5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

(2) 10 進表示

p=115792089210356248762697446949407573530086143415290314195533631308867097853951

r=115792089210356248762697446949407573529996955224135760342422259061068512044369

a=115792089210356248762697446949407573530086143415290314195533631308867097853948

b=41058363725152142129326129780047268409114441015993725554835256314039467401291