# Wymiana kluczy ECDH i własne parametry krzywych eliptycznych.

Mikołaj Koszowski 274392
Hubert Nowakowski 274415

Zad 5. wariant 4
Kod źródłowy: github.com/Fisher16/KiBD

Stworzyliśmy notebook pokazujący jak poprawnie dobrać parametry systemu szyfrowania z kluczem publicznym wykorzystującym krzywe eliptyczne. Istotnym warunkiem jest brak punktów osobliwych (eng. singular point), co dla krzywych postaci:

$$y^2 = x^3 + ax + b$$

Sprowadza się do warunku:

$$4a^3 + 27b^2 \neq 0$$

Ten i inne warunki sprawia, że możemy sprowadzić algebrę na krzywej do algebry ciała skończonego szeroko wykorzystywanej w kryptografii. Zaletą kryptografii krzywych eliptycznych jest większa trudność odwrócenia mnożenia w tej przestrzeni w porównaniu z odwróceniem funkcji jednokierunkowych stosowanych w innych typach kryptografii klucza publicznego. Sprawia to że dla danego poziomu bezpieczeństwa jest możliwe używanie krótszego klucza, a przewaga ta będzie tylko rosła z czasem, co widać w załączonej tabeli.

NIST Recommended Security Bit Level:

| Security Bit Level | RSA | ECC | ratio RSA:ECC |
|---|---|---|---|
| 80 | 1024 | 160 | 6 |
| 112 | 2048 | 224 | 9 |
| 128 | 3072 | 256 | 12 |
| 192 | 7680 | 384 | 20 |
| 256 | 15360 | 512 | 30 |

**Artykuł opisujący podatności:**
*Degenerate Fault Attacks on Elliptic Curve Parameters in OpenSSL:* https://eprint.iacr.org/2019/400.pdf

**Źródła:**
https://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/
https://mathworld.wolfram.com/SingularPoint.html
RSA and ECC: A Comparative Analysis https://www.ripublication.com/ijaer17/ijaerv12n19_140.pdf