

Implementation of an ECC with M-511

CS448 - Introduction to IT Security

Who? Yoann Kehler, Duong Ta

When? June 08, 2017

Outline

- What goals have we had?
- What have we done?
- What have we learned?

Term Project Goals

Term Project Goals

- understand the maths behind ECC

Term Project Goals

- understand the maths behind ECC
- implement a library with M-511 with:
 - key generation
 - encryption and decryption
 - signature and verification

Term Project Goals

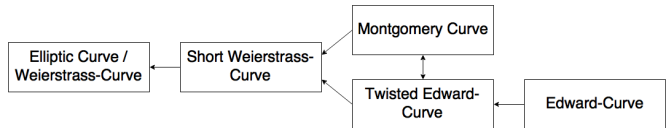
- understand the maths behind ECC
- implement a library with M-511 with:
 - key generation
 - encryption and decryption
 - signature and verification
- hike Jirisan

Put it into practice!



How to generate a curve?

variety of elliptic curves



Architecture of our Implementation

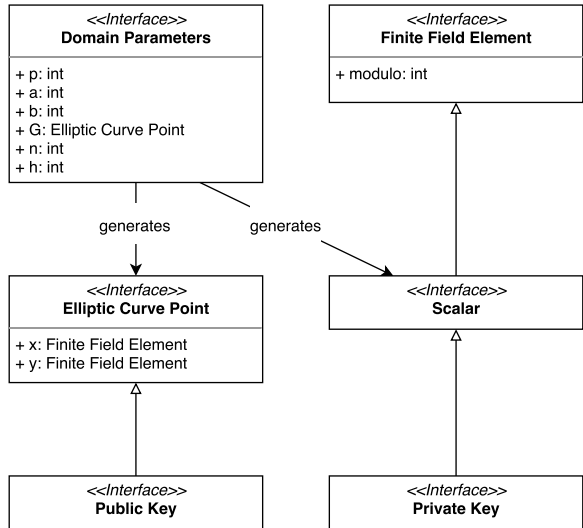


Figure: Class Diagram of our Implementation

Lessons Learned

References I