Embedded Security Systems
Laboratory Tasks 1

Deadline: 09.03.2017

Task 1 (35%)

Write a function `hash(byte[] in,byte fun)` in Java that generates the hash value of input `in` using the algorithm denoted by `fun`. Use at least the following algorithms: SHA1 (`fun = 0x01`), SHA-256 (`fun = 0x04`), SHA-512 (`fun = 0x06`). Use `BouncyCastle`.

Task 2 (65%)

Learn about explicit parameters for elliptic curves in Bouncy Castle http://www.bouncycastle.org/wiki/display/JA1/Elliptic+Curve+Key+Pair+Generation+and+Key+Factories. Write a program that creates a key pair for the curve `brainpoolP256r1` (see https://tools.ietf.org/html/rfc5639#page-11) and prints the public key. Your program should set the parameters explicitly. What can you tell about the length and encoding of the public key?