Embedded Security Systems
Laboratory Tasks 5

Deadline: 25.05.2017

Task 1 (100%)

Implement the Diffie-Hellman protocol between the Java Card and a Terminal (implemented in standard Java SE). To generate a shared secret key you should use the `KeyAgreement` class from the JC API and Bouncy Castle (for the terminal). Note that you have to use the same elliptic curve on both sides.

The Java Card applet should generate the keypair on-card (you can use task 1 from the previous list) and implement an instruction `INS=0x40` that outputs the shared secret. Compare the shared secret computed on both sides. Note that the Elliptic Curve DH algorithm implemented on the card returns the `SHA1` value (20 bytes) of the x-coordinate (check if Bouncy Castle does the same or returns the x-coordinate directly).