Embedded Security Systems
Laboratory Tasks 3

Deadline: 20.04.2017

Task 1 (40%)

Create a java card applet similar to the one from task 1 in http://cs.pwr.edu.pl/hanzlik/ess_lab1.pdf. You should use the `MessageDigest` class. Create a list of hash functions supported by the simulator (or card) you use. **Tip:** the `getInstance(byte algorithm, boolean externalAccess)` method returns an error SW when the algorithm is not supported.

Task 2 (60%)

Create a java card applet that on `INS=0x10` generates an RSA key pair and returns the value of the public key. Moreover, on `INS=0x20` the applet should return the secret key. You can use the class `KeyPair` to store and generate new keys from empty `RSAPublicKey` and `RSAPrivateKey` keys created using the `KeyBuilder` class.

What length of RSA keys is supported by the simulator? Use `Python` or `Java` with `BigInteger` to check if the generated RSA key is correct, i.e. use the returned keys to encrypt and decrypt something (choose a random message $m < N$, compute $c = m^e \mod N$, $m' = c^d \mod N$ and check that $m = m'$, where (e, N) is the public key and d is the private key).