

# **Practical Project - Cryptographic Library & App - Part 1**

Names: Elijah Immer, Khalid Rashid, Grant Koenig

**Objective** Implement (in Java) a library and an app for asymmetric encryption and digital signatures at the 128-bit security level.

## **Algorithms**

1. SHA-3 hash and SHAKE extendable output functions.
2. ECDHIES encryption and Schnorr signatures.