CRY- Summer Student in the Cryptography Research Group

**Supervisor:** Dr. Céline Blondeau / Prof. Kaisa Nyberg

**Contact information:** By email: celine.blondeau@aalto.fi

**Job description:** Recently many theoretical attacks on symmetric key cryptographic algorithms have been published. The task of the student will be to implement one of these attacks on a toy-cryptographic primitive. The implementation will be preferably in language C. Also the student should have a basic knowledge on cryptography.

**Additional information:** For information on the Cryptography group and its research, see http://research.ics.aalto.fi/crypto/