DIAC - Directions in Authenticated Ciphers

July 05 & 06, 2012

Location: most likely Stockholm (long days to have discussions around the clock)

Deadlines: submission: May 7; notification June 4

Motivation: Want to protect messages against espionage and against forgery, faster and/or more secure than with current approaches, so let's have a **competition** for authenticated ciphers.

Purpose of this workshop is to evaluate the state of the art in authenticated encryption and to gather community input regarding desired future directions.

Scope and function similar to SASC 2004 and the ECRYPT Hash Workshop 2007.

ECRYPT

http://hyperelliptic.org/DIAC