MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Avd. Matematik

SJÄLVSTÄNDIGT ARBETE I MATEMATIK

Torsdagen den 16 juni kl. 10:00-11:00 presenterar Erik Vesterlund sitt arbete "Security Aspects of Bitcoin" (15 högskolepoäng, grundnivå).

Handledare: Björn Bergstrand och Karl Rökaeus

Plats: Sal 32, hus 5, Kräftriket

Sammanfattning: Digital signatures (ECDSA) and hash functions (SHA-256) are used to secure ownership and transactions of the cryptocurrency Bitcoin. We describe the strengths and vulnerabilities of these technologies, and motivate where and why they appear in the Bitcoin protocol.

Alla intresserade är välkomna!