PS Einführung Kryptographie und IT-Sicherheit

Salzburg, T01, 14:45 *16.06.2025*
***Abgabe**: bis FR 14.06. 12:00 an uhl@cs.sbg.ac.at*

37.) Beweisen sie die Bedingung für die El Gamal Unterschriftsverifikation und klären sie ob für die Unterschriftsverifikation das geheime K bekannt sein muss. Was hat ihre Erkenntnis für eine Konsequenz ?

38.) Implementieren sie die Tandem Davies-Mayer Hashfunktion mit AES und vergleichen sie deren Laufzeitverhalten für steigende Nachrichtengrössen mit einer SHA-3 Variante mit gleicher Hashlänge.

39.) Implementieren sie OTP Ver- und Entschlüsselung mit dem Blum-Blum-Shub Generator (wie beschrieben) und vergleichen sie die Ausführungsgeschwindigkeit mit OTP Ver- und Entschlüssleung durch einen nativen Stream-cipher aus dem eStream Portfolio.

40.) Warum muss beim Diffie-Hellman Key-Exchange neben n auch $\frac{n-1}{2}$ eine Primzahl sein (und beweisen sie ihre Erklärung) ?

VIEL ERFOLG !!