PS Einführung Kryptographie und IT-Sicherheit

Salzburg, T01, 14:45 *02.06.2025*
***Abgabe**: bis FR 30.05. 12:00 an uhl@cs.sbg.ac.at*

34.) Implementieren sie die Chosen Ciphertext Attacke 3 gegen RSA (Slide 157 der VO). Bedenken sie, dass sie dafür auch die Abbildung des Plaintexts auf numerische Blöcke realisieren müssen. Überlegen / diskutieren sie, was gemacht werden müsste wenn im Kontext dieses Angriffs Alice nur sinnvolle Dokumente unterschreiben würde !

35.) Fortsetzung Aufgabe 34: Implementieren sie eine Variante des Angriffs, in dem versucht wird, dass die von Alice zu unterschreibenden Texte tatsächlich sinnvolle, korrekte Texte sind (und keine zufälligen Strings / Bytehaufen). Überlegen sie auch die Komplexität die zu erwarten ist dass dieser Angriff zu einem Erfolg führen könnte.

36.) Was ist ein linearer Kongruenzgenerator (LCG) ? Illustrieren wie, warum ein LCG nicht kryptographisch sicher sein kann.

VIEL ERFOLG !!