PS Einführung Kryptographie und IT-Sicherheit

Salzburg, T01, 14:45 *28.04.2025*
***Abgabe**: bis SO 27.04. 15:00 an uhl@cs.sbg.ac.at*

17.) Fortsetzung Aufgabe 16.): Bestimmen sie mit der in der VO besprochenen Methode mit Iteration über die Länge der Keys unter Berechnung der Hamming Distanz (Slide 65, 2. Verfahren) die Länge des Keys in dem in Aufgabe 16.) realisierten short Key XOR Verschlüsselungsverfahren.

18.) Fortsetzung Aufgabe 11.): Führen sie eine Known Plaintext Attacke gegen den in Aufgabe 11.) implementierten Cipher durch und ermitteln sie aus den erzeugten Daten automatisch den für z verwendeten Wert.

19.) HÜ9 auf S. 85 der VO-Slides.

20.) HÜ2 auf S. 93 der VO-Slides (die beiden Fragen im ersten Item sind zu bearbeiten).

VIEL ERFOLG !!