PS Einführung Kryptographie und IT-Sicherheit

Salzburg, T01, 14:45 *31.03.2025*
***Abgabe**: bis SO 30.03. 15:00 an uhl@cs.sbg.ac.at*

14.) Erklären sie das Fuzzy Vault Scheme zur Erzeugung von kryptographischen Schlüsseln aus biometrischen Messungen. Wann muss dieses Verfahren verwendet werden anstelle des Fuzzy Commitment Schemes ?

15.) Implementieren sie als einfaches Bildverschlüsselungsverfahren eine Permutation der Zeilen eines Bildes. Dazu soll als Parameter (z.B. 1, 2, 4, ...) eine Anzahl von horizontalen Bildblöcken definiert werden können, innerhalb derer jeweils die Permutationen angewendet werden (also Permutationen auf das ganze Bild für 1, Permutationen innhalb der oberen und unteren Bildhälfte für 2, u.s.w.). Versuchen sie anschliessend, unter Ausnutzung der Tatsache dass ähnliche Bildzeilen meist nebeneinander liegen, eine Ciphertext only Attacke gegen das verschlüsselte Bild (für verschiedene Parameterwerte und Bilder).

16.) Implementieren sie die in der VO besprochene short Key XOR Verschlüsselung (Text wird über ascii-Nummern binär dargestellt und mit ensprechendem "binärem" Text Key XOR verschlüsselt, variable Key-länge für Experimente erforderlich). Bestimmen sie mit der in der VO besprochenen "Counting Coincidences" Methode die Länge des jeweils verwendeten Keys.

VIEL ERFOLG !!