

Aufgabenblatt 04

Einführung in die Kryptographie PS

Andreas Schlager

27. März 2025

Inhaltsverzeichnis

1 Aufgabe 14	1
2 Aufgabe 15	1
2.1 Verschlüsselungsverfahren	2
2.2 Ciphertext-only Attacke	2
2.3 Ergebnisse	2
3 Aufgabe 16	2
4 Zeitaufwand	2

1 Aufgabe 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?

Antwort.

2 Aufgabe 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 innerhalb 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).

Die Implementierung der Ver- und Entschlüsselung wurde vollständig in der Programmiersprache **Rust** geschrieben. Zur Bildmanipulation wird das image Crate verwendet.

2.1 Verschlüsselungsverfahren

Um ein Bild zu verschlüsseln, wird das Bild aus dem Speicher geladen und durch `permutation_cipher` mit der gewünschten Blockanzahl verschlüsselt. Für dieses Experiment werden 1, 2, 4, 8, 16, 32 Blöcke mit unterschiedlichen Bildern getestet.

```
let original = image::open(&path).expect("Failed to open image");

for blocks in [1, 2, 4, 8, 16, 32] {
    let cipher_image = permutation_cipher(&original, blocks);
    cipher_image
        .save(format!("./img/out/{:02}_{:02}", blocks, filename))
        .expect("Failed to save image");
}
```

Normalerweise würde man das Verschlüsselungsverfahren deterministisch anhand eines Schlüssel durchführen. Für den Zweck dieses Experiments soll allerdings kein Schlüssel ermittelt werden, also können die Zeilen innerhalb eines Blocks einfach gemischt werden. Dafür werden einfach zwei Zeilen eines Blocks zufällig ausgewählt und getauscht. Dieser Vorgang wird dann 1000 Mal wiederholt, um einen gemischten Block zu erhalten.

```
fn permutation_cipher(original: &image::DynamicImage, blocks: u32)
    -> image::DynamicImage {
    let mut img = original.to_rgba8();
    let height = img.height();
    let rows_per_block = height / blocks;

    for block in 0..blocks {
```

2.2 Ciphtext-only Attacke

2.3 Ergebnisse

3 Aufgabe 16

Implementieren sie die in der VO besprochene short Key XOR Verschlüsselung (Text wird über ASCII-Nummern binär dargestellt und mit entsprechendem "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.

Antwort.

4 Zeitaufwand

Zeiteinheiten sind in Stunden [h].

Aufgabe	Coding	Recherche	Schreiben	Σ
Aufgabe 10	5	0.5	6	11.5
Aufgabe 11	1	1	3	5
Aufgabe 12	0	1.5	1	2.5
Aufgabe 13	0	1.5	1	2.5
Σ	6	4.5	11	21.5