Prof. Dr. Rüdiger Weis

Sicherheit in Verteilten Systemen

Übungsblatt 2

Aufgabe 1 (12 P) Steganographie

Programmieren Sie ein Python Skript, welches eine gegebene Datei im niederwertigste Bits eines bmp-Bild versteckt. Verwenden Sie das Module Image.

Aufruf: `steganohide.py text.txt bild.bmp`
Ausgabe Modifizierte Bilddatei mit Zusatzendung .ste: `bild.bmp.ste`

Aufgabe 2 (42 P) Authentifizierung und Verschlüsselung

Implementieren Sie zusätzlich eine Authentifizierung und Verschlüsselung der einzubettenden Datei in Python.

- Authentifizieren Sie die Daten mittels HMAC-SHA256. Hashen Sie dazu das übergebene MAC-Passwort mittels SHA-256 zur Erzeugung des HMAC-SHA256 Schlüssels. Stellen sie den MAC den Daten voran.
- Verschlüsseln Sie die Daten inklusive des MAC mit dem XTEA Algorithmus im CFB Mode. Hashen Sie hierzu das übergebene Passwort mittels SHA-256 und verwenden Sie die höherwertigen 128 bit für die eigentliche Verschlüsselung.

Die modifizierte Bilddatei soll die Zusatzendung .sae erhalten.
Implementieren Sie ebenfalls die Entschlüsselung und MAC-Überprüfung.

Aufruf:

encrypt:
```
aesteganohide.py -e -m macpassword -k password text.txt bild.bmp
```
decrypt:
```
aesteganohide.py -d -m macpassword -k password bild.bmp.sae
```