IT Sicherheit Übung 2

Prof. Dr. Rüdiger Weis

Steganographie

Programmieren Sie ein Python Skript, welches eine gegebene Datei im niederwertigste Bits eines bmp-Bild versteckt und eine Authentifizierung und Verschlüsselung der einzubettenden Datei in Python.

- Authentifizieren Sie die Daten mittels HMAC-SHA512.
  - Erzeugens Sie 128 bit Salt.
  - Hashen Sie die Konkatination der 128 bit Salt und dem MAC-Passwort mittels SHA-512 zur Erzeugung des HMAC-SHA512 Schlüssels.
  - Stellen sie den MAC den Daten voran.
- Verschlüsseln Sie die Daten inklusive des MAC mit dem XTEA Algorithmus im CFB Mode.
  - Erzeugen Sie 128 bit Salt.
  - Hashen Sie hierzu die Konkatination der 128 bit Salt und dem Passwort mittels SHA-512 und verwenden Sie die höchstwertigen 128 bit für die XTEA Verschlüsselung.
  - Programmieren Sie den XTEA Algorithmus in Python.

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

encrypt aesteganohide.py -e -m macpassword -k password text.txt bild.bmp

decrypt aesteganohide.py -d -m macpassword -k password bild.bmp.sae