Labreport 06

Julian Deinert, Tronje Krabbe

30. Juni 2016

Inhaltsverzeichnis

1. TODO

1.2

TODO

2. TODO

2.1

TODO

3. Unsichere selbstenwtickelte Verschlüsselungsalgorithmen

3.1 BaziCrypt

Die letzten 10 Bytes des Ciphertexts sind exakt der Key. Oder, genauergesagt, der Key XOR Null, was den Key unverändert lässt. Jetzt ist es sehr einfach, die Dateien zu entschlüsseln. Siehe unser Skript im Appendix. Die drei Plaintexte sind:

> [n01.txt.enc] Hallo Peter. Endlich koennen wir geheim kommunizieren! Bis bald, Max
>
> [n02.txt.enc] Hi Max! Super, Sicherheitsbewusstsein ist ja extrem wichtig! Schoene Gruesse, Peter.
>
> [n03.txt.enc] Hi Peter, hast du einen Geheimtipp fuer ein gutes Buch fuer mich? Gruss, Max

3.2 AdvaziCrypt - Denksport

Da *PKCS7*-Padding blockweise passiert, und der Key 10 Bytes lang ist, können wir davon ausgehen, dass die letzten 10 Bytes des Ciphertexts sich so ergeben:

$$\text{key} \oplus 0x10 = \text{ciphertext}$$

Um nun also den Key zu ermitteln, rechnen wir einfach:

$$\text{ciphertext} \oplus 0x10 = \text{key}$$

Appendix

3.3 3. Skripte

```python
#!/usr/bin/env python
import sys

if __name__ == "__main__":
    filename = sys.argv[1]
    result = ''
    counter = -1
    with open(filename, "rb") as f:
        f.seek(-10, 2) # seek last 10 bytes
        key = [int(b) for b in f.read(10)]
        f.seek(0, 0) # seek beginning of file again
        while True:
            counter += 1
            counter = counter % 10
            b = f.read(1)
            if b == b'':
                break
            num = int.from_bytes(b, 'little')
            result += chr(num ^ key[counter])
    print(result)
```