

Labreport 06

Julian Deinert, Tronje Krabbe

30. Juni 2016

Inhaltsverzeichnis

1. TODO	1
1.2	1
2. TODO	1
2.1	1
3. Unsichere selbstentwickelte Verschlüsselungsalgorithmen	1
3.1 BaziCrypt	1
3.2 AdvaziCrypt - Denksport	1
3.3 3. Skripte	2

1. TODO

1.2

TODO

2. TODO

2.1

TODO

3. Unsichere selbstentwickelte Verschlüsselungsalgorithmen

3.1 BaziCrypt

Die letzten 10 Bytes des Ciphertexts sind exakt der Key. Oder, genauer gesagt, 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

Wenn wir davon ausgehen, dass der Key vollständig (wenn auch ‘verschlüsselt’) in der Datei vorhanden istm dann sind auf jeden Fall die letzten 10 Bytes des Ciphertexts die verschlüsselten Key-Bytes. Jetzt kann man auf die Anzahl der Padding-Bytes schließen, indem man darauf achtet, wann die hinteren Bytes aufhören, Teil des vermeintlichen, verschlüsselten Keys zu sein. Dies kann allerdings auch Glückssache sein...

Appendix

3.3 3. Skripte

```
#!/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)
```