CCA – COMPETENCE CENTRE

HTL Anichstraße

noindent

FSST-OpenSSL

Fabio Plunser

17. Februar 2021

Inhaltsverzeichnis

1 Aufgabenstellung **1**

2 Umsetzung **2**
2.1 OpenSSL 2
2.2 Programm 2
2.3 Erklärung 2

Abbildungsverzeichnis

Code

1 Angabge 1
2 Angabge 1
3 Angabge 1
4 Angabge 1

1 Aufgabenstellung

```
# deciphers to "Schoene Crypto Welt" with IV=BBBBBBBBBBBBBBBB and key=
    BBBBBBBBBBBBBBBB aes128-cbc
cyphertext = "
    AAE365272C81078AB6116B361831D0F6A5D3C8587E946B530B7957543107F15E"
bc = binascii.unhexlify(cyphertext)
data = b'D' + bytes([len(bc)]) + binascii.unhexlify(cyphertext) + b'X'
```

Listing 1: Angabge

Der cyphertext soll entschlüsselt „Schöne Crypto Welt“ bedeuten. Um dies zu überprüfen kann https://www.openssl.org/ verwendet werden.

Schreiben Sie ein Programm das unter Verwendnung von openssl obige Aussage überprüft, verbessen Sie ihr Program in dem Sinne dass sie key/iv/plaintexte/ciphertexte als Argumente/Dateien/Usereingaben verarbeiten.

Hinweise

- Sie benötigen die openssl Biblotheksheader, unter Ubuntu 20.04 können Sie diese installieren via:

```
$ sudo apt install libssl-dev
```

Listing 2: Angabge

- em Linker muss mitgeteilt werden dass sie in Ihrem Programm Funktionen verwenden die in einer externen Bibliothek bereit liegen, verwenden sie dazu das flag -l (klein-L) und den Namen der Bibliothek OHNE das führende lib. openssl besteht aus mehreren Bibliotheken, die für AES notwendingen Funktionen befinden sich in libcrypto.

```
$ gcc my_code.c -lbibliothek -o my_executable
```

Listing 3: Angabge

Sie können sich die gelinkten Bibliotheken dann via ldd Kommando ansehen

```
$ ldd my_executable
```

Listing 4: Angabge

2 Umsetzung

2.1 OpenSSL

2.2 Programm

2.3 Erklärung