Challenge-Response-Algorithm Abgabe 4

Dominic Manuel Weinberger
Lukas Feistritze

AES-Key: 128 bit (16 byte)

20 byte challenge of A:

```
00100010 00100000 11010000 01110001 01111110
11010111 01011110 00111001 11101111 01110110
11111111 10001010 00000100 01001111 01011000
10010100 11001101 10111100 00110101 00111010
```

20 byte challenge of B:

```
11011110 00110110 10010001 01010010 10011100
11000000 11100110 11000111 10011100 10011101
01011000 00100011 01100111 01010001 01100011
00010110 00110010 10111100 00000101 00011011
```

Message 1: challenge of A

ClientB encrypts challenge of A, generates challenge of B, concatenates both in Message 2!

Message 2: response to challenge of A || challenge of B

ClientA extracts response to challenge of A, decrypts response to challenge of A; if decrypted response to challenge of A == challenge of A, then B is authenticated

ClientA extract challenge of B, encrypts it, sends it to B in Message 3

Message 3: response to challenge of B

ClientB decrypts response to challenge of B (Message3), if response to challenge of B == challenge of B, then A is authenticated