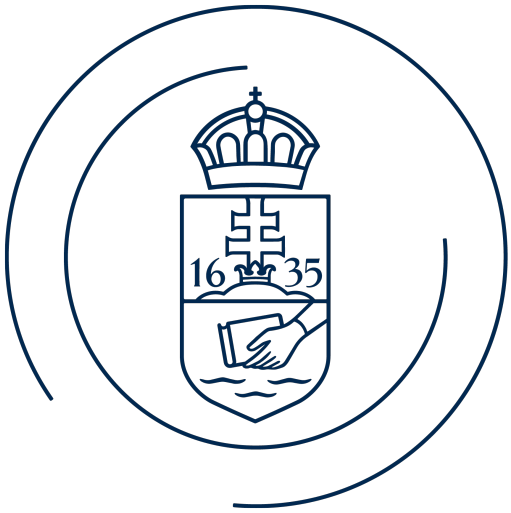

ELTE
EÖTVÖS LORÁND
UNIVERSITY

Cryptography and security (IPM-18sztKVSZKRBG)

Assignment III

Minimum requirements

- There are 4 different IT security related problems described in this paper with varying difficulties;
- You need to collect at least **5 points** from this assignment;
- Always provide step by step solutions;
- Submit your final solution in **one PDF** file including every necessary source code;
- Please send your solutions to **ntihanyi@inf.elte.hu** till **20th April 2022**;
- It is **strictly prohibited** to share your solutions with others.

Challenge #1 - Brute-force

We have the following small script. The embedded password is only 6 characters long.

```
AuthClass ELTE{
  self.username=administrator_elte
  rx = Crypt_SHA2(passwd.input)
  if b64.encode(hex.decode(rx))=="nyuPTeLboduudJ95DKbuMd7iHjozD8vFZ3Gjen9qDvA="
  {
    "Access granted!"
  }
}
```

Questions:

a. Write a program that recover the cleartext password. (**3 points**)

b. Recommend a more secure algorithm for password hashing. (**1 point**)

Challenge #2 - Finite Field

AES is using the following reducing polynomial for multiplication: $x^8 + x^4 + x^3 + x + 1$

a. Solve the multiplication in `GF(8): 0xCA · 0x53 = ?` (**1 point**)

b. Solve the multiplication in `GF(8): 0x11 · 0xDA = ?` (**1 point**)

c. Solve the multiplication in `GF(8): 0x99 · 0xFF = ?` (**1 point**)

d. Solve the multiplication in `GF(8): 0xCC · 0x39 = ?` (**1 point**)

e. Implement the general AES `GF(8)` multiplication in any chosen programming language (**6 points**)

Challenge #3 - Collision

We have the following python script.

```
import md5
def encrypt(password):
hash = md5.new(password).hexdigest()
l = list(hash)
l.sort()
return md5.new(''.join(l)[:13]+"ABCD").hexdigest()
```

Questions:

a. Provide two different strings `s1` and `s2` where `encrypt(s1)=encrypt(s2)` (**1 point**)

b. Implement the solution in any chosen programming language. (**3 points**)

Challenge #4 - AES or RSA

AES and RSA are the most widely used symmetric and asymmetric encryption algorithms.

Questions:

a. Describe the most important differences between AES and RSA (10-12 sentences). (**2 points**)