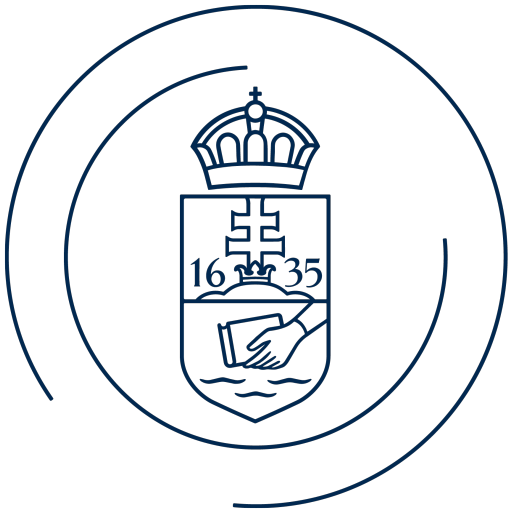

ELTE
EÖTVÖS LORÁND
UNIVERSITY

Cryptography and security
(IPM-18sztKVSZKRBG)

Assignment I

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;
- Please send your solutions to **ntihanyi@inf.elte.hu** till **25th March 2022**;
- It is strictly prohibited to share your solutions.

Challenge #1 - Shannon Entropy

In information theory, the **entropy** of a random variable is the average level of uncertainty inherent to the variable's possible outcomes. The ASCII characters are numbered from 0 to 255, hence the maximum entropy of an ASCII string is 8 bits $(2^8 = 256)$. We have the following ASCII string:

```
63864192837289378213728372893782831783273827373727376122 8
19518576075986998905764553012264711591128570856965959402 4
44531655927273797239218141824248086816028499381698198865 9
39062956454949910471787520911687720233006622996348095941 7
59680645554974661972791876464441493215195714488687853734 6
70177241338593795678290614012152015234783978899113367959
36842787769119782188988770440036842908282004241814010897 3
```

Questions:

a. Can you calculate the Shannon entropy of this string? (**1 points**)

b. Implement the solution in any chosen programming language (**2 points**)

Challenge #2 - Something wrong

The output of a random number generator is the following:

```
389745661337066518721312714156744807719607623268 7
```

Questions:

a. Can you find the flaw in this generator? (**2 points**)

Challenge #3 - Encrypted text

The encryption algorithm is unknown.

```
Vfkmfj Cfireu Lezmvijzkp zj r Ylexrizre glsczt ivjvrity
lezmvijzkp srjvu ze Slurgvjk. Wfleuvu ze 1635, VCKV zj fev
fw kyv crixvjk reu dfjk givjkzxzflj glsczt yzxyvi vultrkzfe
zejkzklkzfej ze Ylexrip. Kyv 28000 jkluvekj rk VCKV riv
fixrezqvu zekf ezev wrtlckzvj, reu zekf ivjvrity zejkzklkvj
cftrkvu kyiflxyflk Slurgvjk reu fe kyv jtvezt srebj fw kyv
Urelsv. VCKV zj rwwzczrkvu nzky 5 Efsvc crlivrkvj, rj nvcc
rj nzeevij fw kyv Nfcw Gizqv, Wlcbvijfe Gizqv reu Rsvc Gizqv,
kyv crkvjk fw nyzty nrj Rsvc Gizqv nzeevi Crjqcf Cfmrjq ze 2021.
```

Questions:

a. Can you decipher the text? (**1 points**)

b. Implement the solution in any chosen programming language (**6 points**)

Challenge #4 - PRNG (X,Y,Z)

Random numbers are very important in many fields of computer science. Predictable random numbers can pose high security issues in modern applications. The following formula were used to generate random numbers:

$$A_{n+1} \equiv (XA_n + Y)(\mathbf{mod}\, Z)$$

```
A_60= 24641675116207691401945061402307095306 9
A_61= 71744889648624900918616152933820948112
A_62= 31379530235796140157650549756408820 1464
A_63= 65184588491602661601360554078566915563
A_64= 32478422870850556711299952452235954722 6
A_65= 26157666426922926299712046744486438125 3
A_66= 91964492393066574896153531497877807434
A_67= 13453247198096447237325917166235115711 3
```

Questions:

a. Can you calculate the next number A_{68} ? (**2 points**)

b. Implement the solution in any chosen programming language (**6 points**)