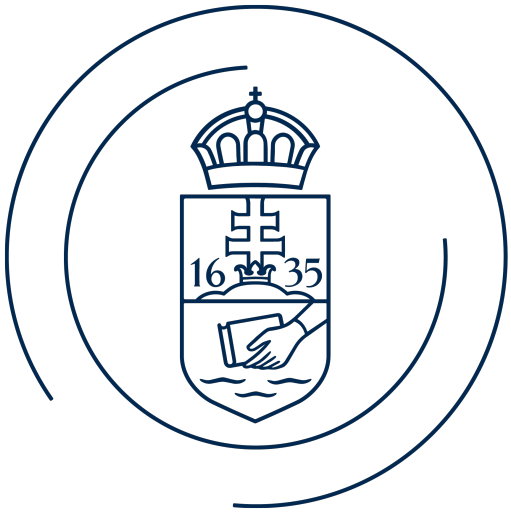

ELTE
EÖTVÖS LORÁND
UNIVERSITY

Cryptography and security (IPM-18sztKVSZKRBG)

EXTRA MILE

Minimum requirements

- There are 2 different IT security related problems described in this paper
- Please send your solutions to **ntihanyi@inf.elte.hu** till **15th April 2022**;
- It is strictly prohibited to share your solutions.

EXTRA MILE #1 - QR code challenge

Questions:

a. Recover the PIN code hidden in this QR code. (**15 points**)

Challenge #2 - SSH public key

A 2048 bit PKCS#1 format SSH public key is given:

```
 -----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEBbjr/6D+EbSjX4U2+4VY6
Nv4ZTfWqhUmM17GQVRf2nQqt4TkjYgQcaSQuB6J5SZHl7bRmAM7KQivQa8v2SzFb
QQZSmdBE1ZRLmiarLe6dC+wXLZqykbel18nAsQxeaGSgQzDupCHwdufOAEv5WlQy
FowfF12Ezm8iyxHUix0PHSS5iu6Jcvm7TWG/bVv5PEz0B+jHGRqm0O7nbE7CePX2
M5/Vn5pJIDXzs+5zmGW7HcaZl+STMzfs0LlETvnkVb0ANEhmJqLMeHd2XHL38bHJ
jQjEZqFOwnMsSC/U7FPIB9Aii/5hqpouhYnv8dxlH/UcCSa0+SVp47pPVM22oRlV
vQIDAQAB
-----END PUBLIC KEY-----
```

Questions:

a. Recover the SSH private key from the public key(**25 points**)

b. Demonstrate that the SSH private key is working on a real Virtual Machine infrastructure. (**5 points**)