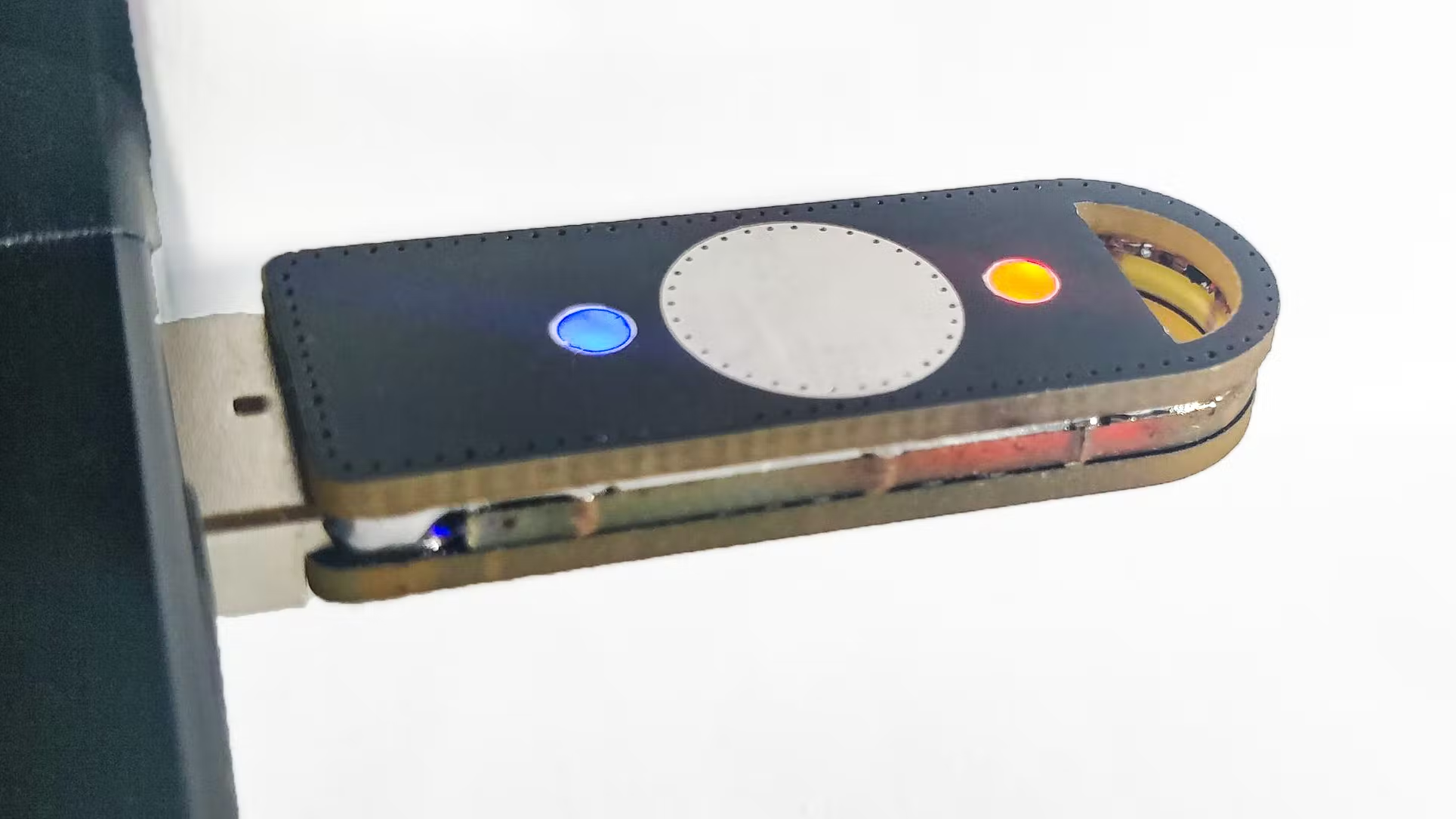
**HW-electronic-key communication protocol**

**This device is used as an electronic token/key that unlocks locked files. Thus, only if it is available, the user can access encrypted files.**

**Command list:**  
All request commands are presented in eight-bit numeric format:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Command | | | Specific | | | | CRC |
| 0 | 0 | 1 | x | x | x | x | CRC |

In which the first three bits specify the command number, the next 4 are responsible for the type of the sent command, and the eighth bit performs the calculation of the CRC. The bit assigned to the CRC will contain either 0 - which will indicate that there is no superscript residue, and 1 - in the case of its presence.

1. ***Check connection of the Key:***

*This command allows the computer to make sure that the HW-electronic-key is really connected to the device.* -> PC: send request to working port “Is the key connected?”

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Command | | | Specific | | | | CRC |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | CRC |

-> BD: send answer to request side

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Response | | | | | | | CRC |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

Responses:  
 if the key was found (response “0000001”), next step.  
 else: message “Key is not connected”.   
 *\* PC App sends requests to BD until Key will be installed or User stops the App.*

1. ***Get key number:***

*This command allows the computer to read HW-electronic-key serial number. Number is like a “login” that allows the PC App to recognize whether the key is really in the database.*

*The key number consists of 7 bits, which are generated by the application at the first entry or by a user with a special command.*

-> PC: send request for key number

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Command | | | Specific | | | | CRC |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | CRC |

-> BD: read and send from BD memory Key number

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Response | | | | | | | CRC |
| x | x | x | x | x | x | x | 0 |

Responses:

*\*Here, the validity of the key in the system database is checked.*  
 if the key number is equal to the number in the PC App database, allow the next step.  
 if the key number is “empty”(00000000), send the message “WARNING: NEW KEY!”, purpose to use the command that allows writing to BD key number or automatic generation.  
 else: message “key is not valid”, interrupt session with message: “NOT VALID KEY-NUMBER!”.  
  
Command allow to set Key number:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Command | | | Specific | | | | CRC |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | CRC |

1. ***Get the Key ID:***

*This command allows the computer to read HW-electronic-key ID. Unlike the Key number, an ID is like a “password” that allows the PC App to provide access to unlock the necessary files. As well as the key number, the key ID also consists of 7 bits that are randomly generated by the program the first time it is entered, and then generated twice for security each time it is used.*

-> PC: send request for key ID

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Command | | | Specific | | | | CRC |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | CRC |

BD: read and send from BD memory ID number

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Response | | | | | | | CRC |
| x | x | x | x | x | x | x | 0 |

if key ID is equal to ID in PC App database, allow decoding.  
 else: message “key is not valid”, interrupt session.  
  
Порядок того, як має відбуватись даний пункт: зчитав з СТМ, перевірив ІД з тою що є в базі, якщо зійшлось, то додав рандомне число, записав в СТМ і записав в базу нове число(суму попереднього та рандомного). Таким чином буде проведено захист.

1. ***Confirmation Key:***

*This command returns "yes" if the ID of the key matches the ID in our database + it must also match the* ***key number.*** *If something is wrong, then the program will not give access to files.*

-> PC: check if Key number and ID confirmed

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Command | | | Specific | | | | CRC |
| 1 | 0 | 0 | 0 | 0 | 0 | 1 | CRC |

BD: read and send from BD memory ID number

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Response | | | | | | | CRC |
| x | x | x | x | x | x | x | 0 |

Response:  
 if “yes”, allow PC access to encrypted file   
 else: “try another Key”, interrupt session

*Timeout: 1 sec - a period, which sets a wait time for command checking.*

**Що варто обговрити:**  
1. скільки буде виділено пам’яті для кожної команди? зробити байти ????  
  
Завдання з зірочкою: Метод шифрування (наприклад 5 команда)