Network Security Assignment 04

Ankit Kumar 2021015
Lakshay Chauhan 2021060
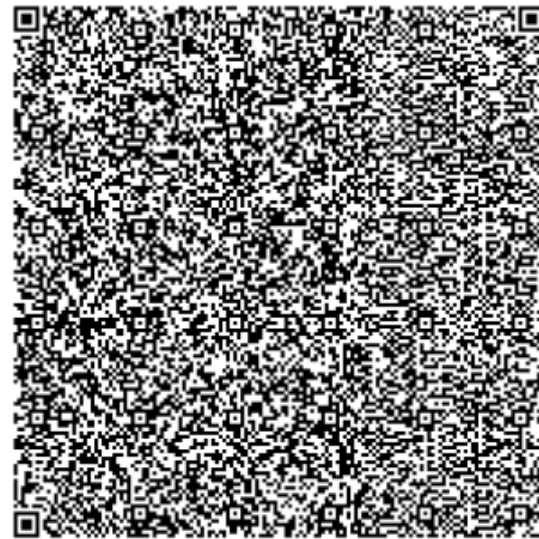
Project 3
On-the-go verification of Driver's License

Sample Driving Licence
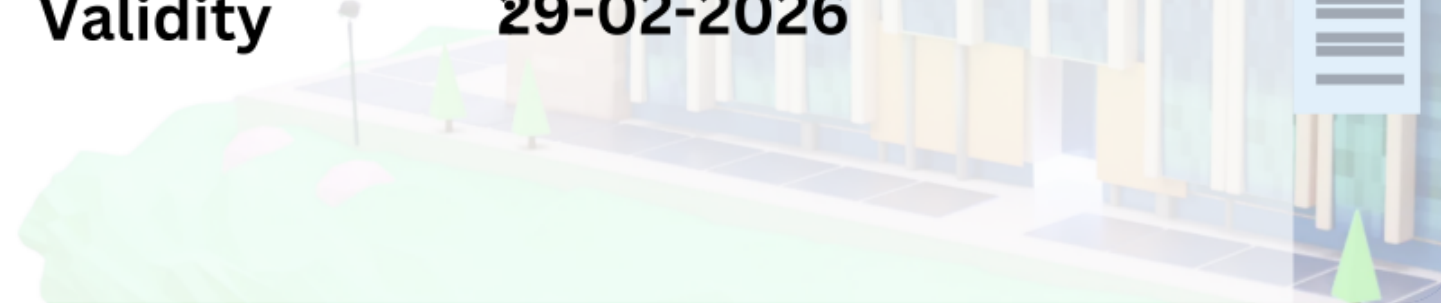
Transport Department Government of IIITD

Licence to Drive Vehicles Throughout Campus

Licence No.	:	DL-654321
Name	:	Lakshay Chauhan
S/W/D	:	Father
DOB	:	01-01-2002
Address	:	H2-102, IIIT Delhi Hostels

Date of Issue 16-04-2024

Validity 29-02-2026

The above image is a sample driver's license. The driver's license contains the following information:

- DL No: The driver's license number
- DOI: The date of issue of the driver's license
- Validity: The validity of the driver's license
- Name: The name of the driver
- DOB: The date of birth of the driver
- Address: The address of the driver

How is the code working

data.json

this is how a new driving licence is generated. This is also used create data_signature from data that prevents data temparing

```
{
    "driving_license": {
        "license_number": "DL-123456",
        "full_name": "Ankit Kumar",
        "date_of_birth": "01-01-2001",
        "address": "H2-102, IIIT Delhi Hostel",
        "issue_date": "15-04-2024",
        "expiry_date": "29-02-2025",
        "categories": ["A", "B"],
        "restrictions": ["Glasses"]
    }
}
```

Generate QR will create QRs using the data.json that can be inserted into the driving licence card
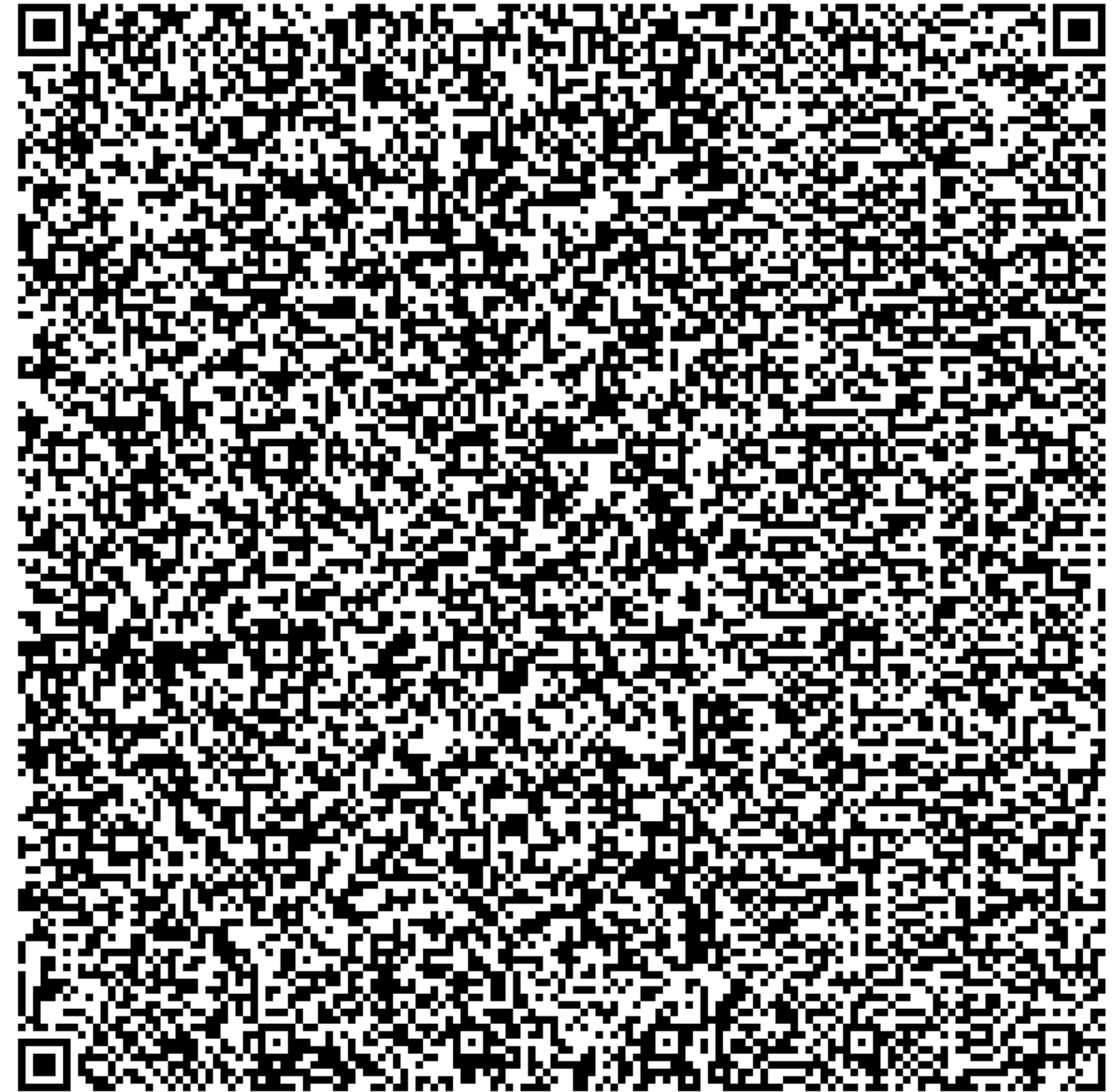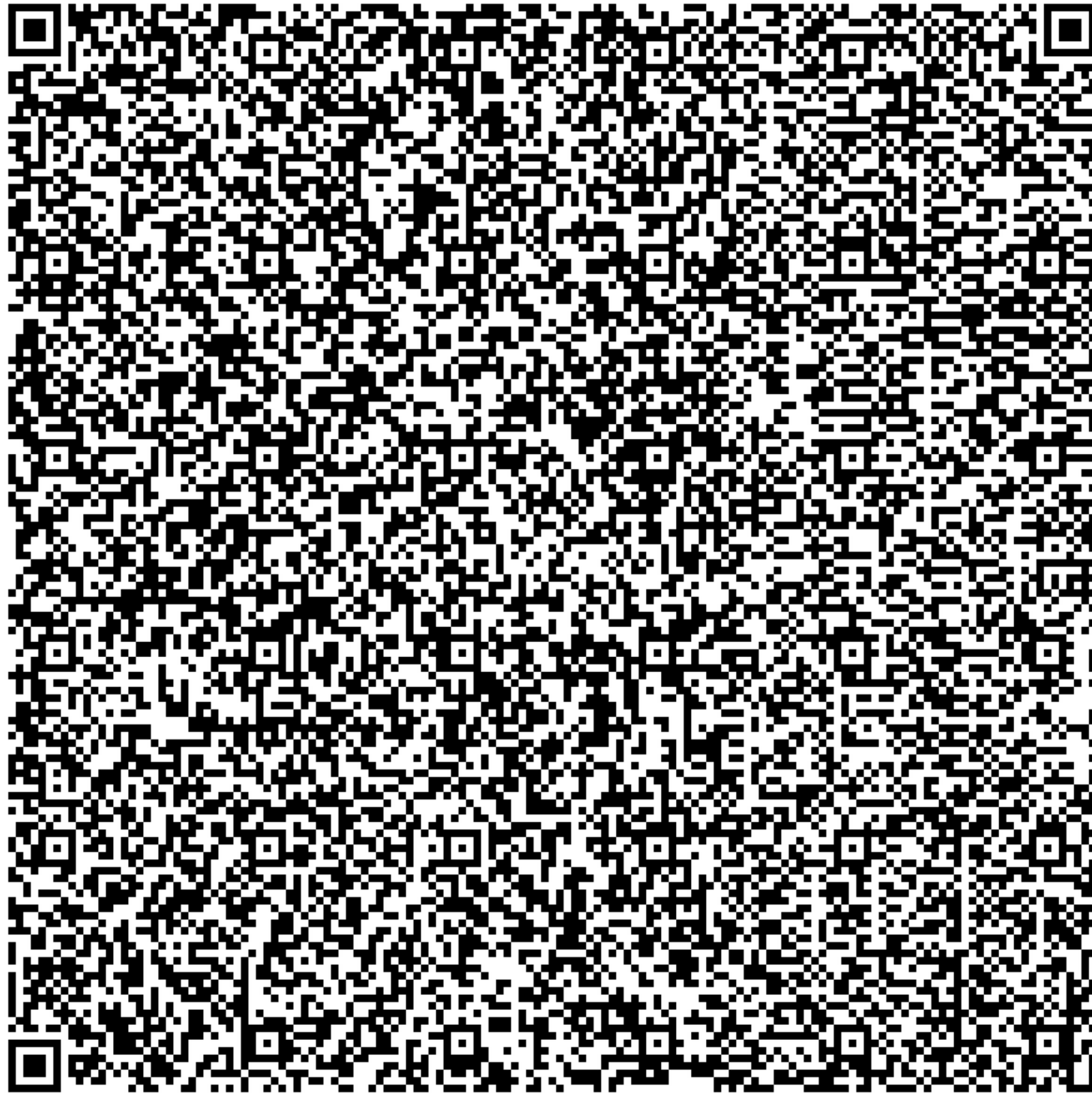
if data.json is tempared or new qr code is generated by editing any of the fields, but the attacker cannot recreate the data_signature which was actually created with the data.json and salt using SHA256 algorithm.
Not only that, the data_signature is also being signed by the public key of the server.

Thank you