You are expected to conduct a mini-research/development on a topic related to security and write a project report (5-8 pages) covering the context of the topic, the problem and the solution in the literature, or implementing an algorithm. You can also work on any topic not in the list but in which you are interested. The number of * indicates the difficulty of the topic.

- Phishing: (*)
- Bitcoin (***)
- DoS (**)
- Vulnerabilities of electronic commerce (**)
- Enigma (implementation) (***)
- Firewall and proxy (**)
- Website protection (**)
- Virus and anti-virus (<3 years) (**)
- Poker mental (***)
- Secrete sharing (***)
- Pseudo-random number generation (***)
- DES (implementation) (***)
- AES (implementation) (***)
- Hash functions (***)
- PGP (Pretty Good Privacy) (**)
- Vulnerabilites Linux/Unix/Windows/… (***)
- Mobile system security (***)
- Database security (***)
- Attacks of TCP/IP (**)
- Buffer overflow (implementation) (***)
- Zero-knowledge proof (***)
- Quantum security (***)
- P2P (**)
- Anonymous connectivity (***)
- Homomorphic encryption (***)
- Federated learning (***)
- Differential privacy (***)
- Security in machine learning (***)
- Censureship and filtering of Internet (**)
- Biometrics (**)
- Watermarking and content protection (***)
- Covert channels (***)
- Social network security (**)
- Cloud security (***)
- ......

/

5-8

*