The Project

You can choose between a project on codes (code theory), or a project on cryptography (and security).

1 Codes

If the project is on codes, then it should be a presentation of one type of codes, or a family of codes.

For the given code, you should present:

1. Mode of the presentation of the code , e.g., in case of linear codes, we may have a generator matrix, a parity check matrix, or a system of equations.
2. In case you have more than one way to present the code, show the relations between them.
3. Specify the most important properties of your code.
4. Show encoding and decoding functions, with examples.
5. Compare your codes with linear codes.
6. Discuss error correction.
7. Formulate conclusions about your code.

2 Ciphers

You can choose a specific cipher and present it:

1. Specify what kind of cipher it is (block/stream, symmetric, public-key, etc).
2. Specify area of application.
3. Show how it is working, with a detailed description.
4. Show encryption and decryption functions (with examples).
5. Compare your encryption algorithms with other learned in the course.
6. Discuss possible attacks.
7. Formulate conclusions about your cipher.

3 Applications

You can also choose to present applications of code and cryptography, and examples include: secure protocols (ssl, tls, ssh, IPSec, Kerberos, Certificates, ...), key management and distribution, authentication schemes (such as the ones used for credit cards).

For the selected application, you should:

1. Give a complete presentation (with examples).
2. Specify what kind of cipher(s)/encoding it is used for that application.
3. Show how code/cryptography theory is used.
4. Present and justify the area where this application is used.
5. Compare your selected application, others that are similar.
6. Discuss possible attacks/weaknesses.
7. Formulate conclusions about your application.

For all cases, you should explain your choice.

You should prepare a 25 min Presentation (40%) + Written Report (due by the end of semester–60%).