VE475
Introduction to Cryptography

Syllabus

Manuel — UM-JI (Summer 2022)

1 Presentation

The focus of this course will be the understanding of cryptology, that is the study of techniques for securing digital information, transactions or computations.

In order to fully benefit from this course, students are expected to only conduct and submit their own, personal work.

2 Teaching team

Details related to the instructor and Teaching Assistants (TAs) are summarized in the following table.

Instructor and TAs	Contact	Office hours	Location
Manuel	charlem@sjtu.edu.cn	Anytime	Piazza
		On appointment	TBA
Grid	saltyfish@sjtu.edu.cn	TBA	TBA
William	william_wu@sjtu.edu.cn	TBA	TBA

3 Schedule

The Summer semester is 13 weeks long, including one week for the finals.

Lectures:

- Tuesday 14:00 – 15:40
- Thursday 14:00 – 15:40
- Friday 12:10 – 13:50 (even weeks)

No labs or recitation classes are planned, however there will be a review class before each exam.

4 Course content and objectives

This course has been tailored with three main goals in mind:

- Understand the basics of cryptology and security

- Become familiar with the most common cryptographic protocols
- Be able to relate theory and practice in cryptology

Hence, at the end of this course, students should be provided with a solid basis for any further study in the field of cryptology and security; In particular they should have developed the necessary skills to decide on validity and security of some given cryptographic solutions.

These goals are fulfilled through the following course outcomes:

- Know the most common symmetric key cryptography protocols (chap. 2)
- Know the most common public key cryptography protocols (chap. 3)
- Understand the importance of true randomness in cryptography (chap. 2)
- Understand the basics on hash functions in cryptography (chap. 4)
- Know the various security levels and be able to derive their corresponding key length depending on the most efficient attacks available (chap. 1,2,3,4)
- Know the basic algorithms to solve real life problems such as digital signatures, secret sharing, or traitor tracing (chap. 5,6,7)
- Be able to perform basic programming in a cryptographic context, i.e. using large numbers or low level logical operations (assignments)
- Get a high level overview of the various sub-fields of cryptography (projects, chap. 1,8,9,10)
- Understand the mathematics used in cryptography (chap. 1,2,3,4,8)

The detailed organisation of this course is given as follows:

Weeks 1–7	**Weeks 8–12**
0. Course information	5. Digital signatures
1. Cryptology overview	6. Secret sharing
2. Block ciphers	7. Traitor tracing
3. Public Key Cryptography	8. Elliptic Curve Cryptography
4. Hash functions	9. Quantum Cryptography
	10. Side channel attacks
Midterm exam	**Final exam**

5 Grading policy

The final average will be composed of four "sub-grades", apportioned as follows:

- Quizzes: 20%
- Final exam: 20%
- Midterm exam: 20%
- Homework: 15%
- Projects: 25%

Any late submission will result in a 10% deduction per day from the grade of the corresponding work. After three days no submission will be accepted.

For the final grade a curve will be applied such that the median is in the range B–B+.

A 5% bonus on the assignment part of the course is awarded to students who setup and use encrypted emails. To validate your setup send (i) an encrypted email to each member of the teaching team, (ii) we will respond to your message and ask you a question, then (iii) answer that simple question as a proof that you can read our encrypted email.

6 Honor code

It is of a major importance for any submitted work to be the result of one own research and understanding. In particular it is not acceptable to reuse the work from another student, or downloaded from the internet. Students can however help each others in an up-building way by sharing ideas and understanding on the course.

If in any case code or details from a textbook or internet is reused, the source should be clearly stated such as not to induce any possible confusion.

According to JI Honor Code copying the work of others will result in **severe penalties**.

Exams

Only the following documents are allowed during the exams.

- The electronic version of the lecture slides with notes on them;
- The printed version of the lecture slides with notes on them;
- A mono or bilingual paper dictionary;

Any document, material, or mean of information and communication not explicitly listed above is strictly prohibited. In particular a **non-exhaustive** list of forbidden materials is as follows.

- Assignments (questions and answers);
- Notebooks or separate files containing notes;
- Calculator or any program allowing to run calculations;

7 General information

The following references and links can be used to find information relevant to the course.

- This course is loosely based on the books *Introduction to Modern Cryptography* from J. Katz and Y. Lindell and *Cryptography, theory and practice* from D. Stinson.
- All the course related materials will be available on Canvas.
- **Never** use baidu as a search engine for questions related to cryptology.

To improve communication between the students and the teaching team please observe the following guidelines.

- Any student facing a special situation likely to impact his studies, such as serious illness or full time work, is expected to contact me as early as possible in order to discuss it and see if any solution can be found.

- When sending an email related to this course please include the tag "[ve475]" in the subject (e.g. `Subject: [ve475] special request`)
- When contacting a TA for a grade issue or any other major problem send me a carbon copy (`cc`). Not doing it might result in omissions, not up-to-date grades etc...If such problem occurs and there is no record of the issue the request will be **automatically rejected**.
- Never attach a large file ($>$ 2 MB) to an email, use SJTU jBox service instead and only include a link in the email.
- Keep in touch with the teaching team, feedbacks and suggestions will be much appreciated.