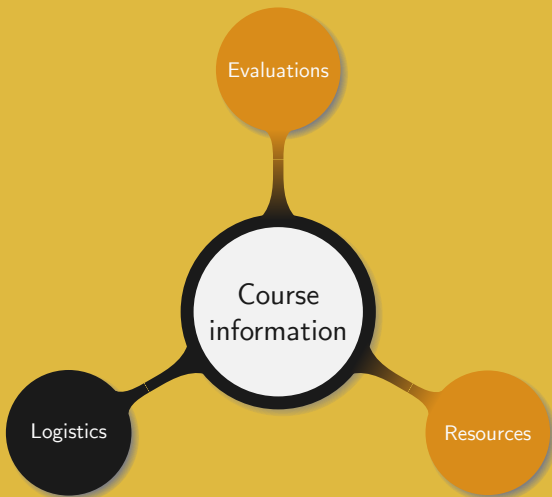


# Introduction to Cryptography

0. Course information

Manuel – Summer 2021





### Teaching team:

- Instructor: Manuel (charlem@sjtu.edu.cn)
- Teaching assistants:
  - Hanyu (whynull@sjtu.edu.cn)
  - Yichao (wangyichao1304@sjtu.edu.cn)

### Important rules:

- When contacting a TA for an important matter, CC the instructor
- Add the tag [VE475] to the subject, e.g. Subject: [VE475] Grades
- Use SJTU jBox service to share large files (> 2 MB)

### Teaching team:

- Instructor: Manuel (charlem@sjtu.edu.cn)
- Teaching assistants:
  - Hanyu (whynull@sjtu.edu.cn)
  - Yichao (wangyichao1304@sjtu.edu.cn)

### Important rules:

- When contacting a TA for an important matter, CC the instructor
- Add the tag [VE475] to the subject, e.g. Subject: [VE475] Grades
- Use SJTU jBox service to share large files (> 2 MB)

Never send large files by email

## Course arrangements:

- Lectures:
  - Tuesday 14:00 – 15:40
  - Thursday 14:00 – 15:40
  - Friday 12:10 – 13:50 (even weeks)
- Office hours:
  - Anytime (Piazza)
  - On appointment (Zoom)

Primary goals:

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

### Primary goals:

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

*Decide on the validity and security of given cryptographic solutions*



## Learning strategy:

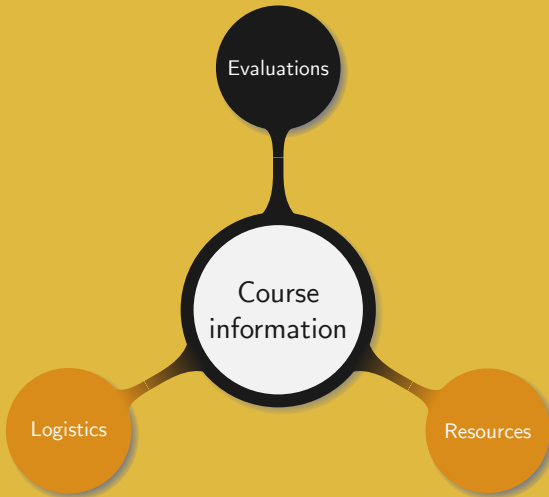
- Course side:
  - ① Understand the basic concepts of cryptography
  - ② Know the most common problems and their solutions
  - ③ Get an overview of many subfields of cryptography

## Learning strategy:

- Course side:
  - ① Understand the basic concepts of cryptography
  - ② Know the most common problems and their solutions
  - ③ Get an overview of many subfields of cryptography
- Personal side:
  - ① Perform extra research
  - ② Relate known strategies to new problems
  - ③ Read and write some code

### Detailed goals:

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



## Homework:

- Total: 10
- Content: basic concepts, coding, mathematics

## Projects:

- Total: 2
- Content: discover new areas of cryptology

## Challenges:

- Total: 3
- Content: code breaking

### Grade weighting:

- Homework: 15%
- Projects: 25%
- Final exam: 30%
- Midterm exam: 30%

### Grade weighting:

- Homework: 15%
- Projects: 25%
- Final exam: 30%
- Midterm exam: 30%

### Assignment submissions:

- Bonus: +10% for a work fully written in  $\text{\LaTeX}$ , limited to 100%
- Penalty: -10% for a work not written in a neat and legible fashion
- Late policy: -10% per day, not accepted after three days

### Grade weighting:

- Homework: 15%
- Projects: 25%
- Final exam: 30%
- Midterm exam: 30%

### Assignment submissions:

- Bonus: +10% for a work fully written in  $\text{\LaTeX}$ , limited to 100%
- Penalty: -10% for a work not written in a neat and legible fashion
- Late policy: -10% per day, not accepted after three days

*Grades will be curved with the median in the range  $\llbracket B, B+ \rrbracket$*





## General rules:

- Not allowed:
  - Reuse the code or work from other students or groups
  - Reuse the code or work from the internet
  - Share too many details on how to complete a task
- Allowed:
  - Reuse part the course or textbooks and quoting the source
  - Share ideas and understandings on the course
  - Provide hints on where or how to find information

Documents allowed during the exams:

- Part A: a mono or bilingual dictionary
- Part B:
  - The lecture slides with **notes on them** (paper or electronic)
  - A mono or bilingual dictionary

Group works:

- Every student in a group is responsible for his group's submission
- If a student breaks the Honor Code, the whole group is guilty

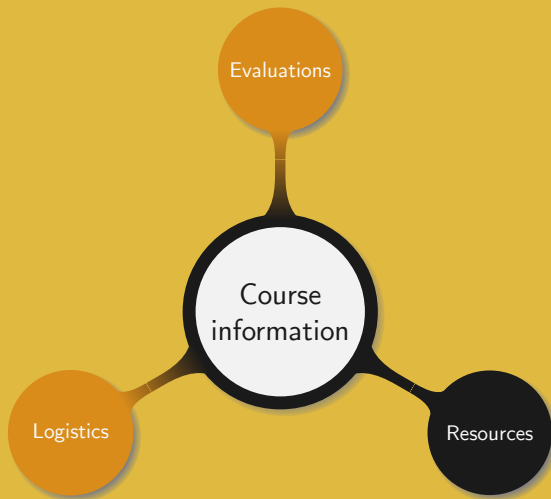
Contact us as early as possible when:

- Facing special circumstances, e.g. full time work, illness
- Feeling late in the course
- Feeling to work hard without any result

Contact us as early as possible when:

- Facing special circumstances, e.g. full time work, illness
- Feeling late in the course
- Feeling to work hard without any result

Any late request will be rejected



## Information and documents available on the Canvas platform:

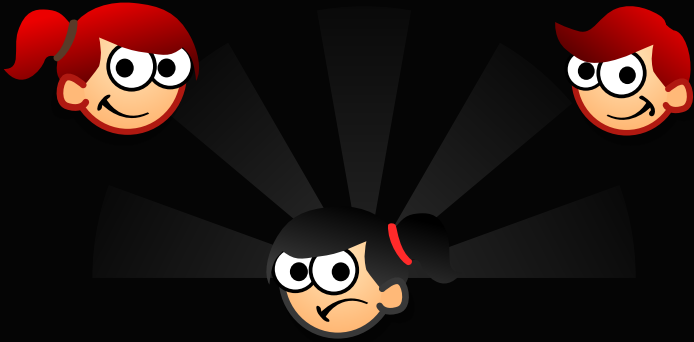
- Course materials:
  - Syllabus
  - Lecture slides
  - Homework
  - Projects
  - Challenges
- Course information:
  - Announcements
  - Notifications
  - Grades
  - Polls

Useful places where to find information:

- *Introduction to Modern Cryptography* (J. Katz and Y. Lindell)
- *Cryptography, theory and practice* (D. Stinson)
- Search information online, i.e.  $\{\text{websites} \setminus \{\text{non-English websites}\}\}$







Thank you!