Introduction to Cryptography

Chapter 0: Course information

Manuel

Summer 2017

Outline

1. Logistics

2. Evaluations

3. Resources

Who?

Teaching team:

- Instructor: Manuel (charlem@sjtu.edu.cn)
- Teaching assistants:
  - Guoyi (louguoyi@sjtu.edu.cn)
  - Hao (hot_hao@sjtu.edu.cn)

Who?

Teaching team:

- Instructor: Manuel (charlem@sjtu.edu.cn)
- Teaching assistants:
  - Guoyi (louguoyi@sjtu.edu.cn)
  - Hao (hot_hao@sjtu.edu.cn)

Important notes:

- When contacting a TA for an important matter such as updating a grade `cc` the message to the instructor
- Add the tag [ve475] in the email subject
  e.g. `Subject: [ve475] late homework`
- Do not send large files ($>$ 2 MB) by email, use Sakai Dropbox

When?

Course organisation:

- Lectures:
  - Tuesday 10:00 – 11:40
  - Thursday 10:00 – 11:40
  - Friday 8:00 – 9:40 (odd weeks)
- Office hours: Tuesday 15:40 – 17:40

Appointments outside of the office hours can be taken by email

What?

Main general 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

What?

Main general 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

Ultimate goal: decide on the validity and security of some given cryptographic solutions

How?

Learning strategy:

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

How?

Learning strategy:

- Course side:
  1. Understand the basic concept of cryptography
  2. Know the most common problems and their solutions
  3. Get an overview of all the subfields of cryptography
- Personal side:
  1. Perform extra research
  2. relate known strategies to new problems
  3. Read/write code

Course outcomes

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

Outline

1. Logistics

2. Evaluations

3. Resources

Assignments and projects

Assignments:

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

Projects:

- Total: 2
- Content: expand understanding of cryptography

Grading policy

Grade weighting:

- Assignments: 30%
- Projects: 20%
- Final exam: 25%
- One midterm exam: 25%

Grading policy

Grade weighting:

- Assignments: 30%
- Projects: 20%
- Final exam: 25%
- One midterm exam: 25%

Late submission: -10% per day, not accepted after 3 days

A curve will be applied for the median to be in the range B – B+

LaTeX policy

Details of the policy:

- LaTeX is a programming language
- Several implementations available
- Cross-platform
- 10% bonus on a mark for a homework **totally** written is LaTeX

LaTeX policy

Details of the policy:

- LaTeX is a programming language
- Several implementations available
- Cross-platform
- 10% bonus on a mark for a homework **totally** written is LaTeX

An assignment not written in a neat and legible fashion can be deducted up to 10% of the awarded mark

Honor code

General rules:

- Not allowed:
    - Reuse the code/work from other students
    - Reuse the code/work from the internet
    - Give too many details on how to solve an exercise

Honor code

General rules:

- Not allowed:
  - Reuse the code/work from other students
  - Reuse the code/work from the internet
  - Give too many details on how to solve an exercise
- Allowed:
  - Reuse part of the code/work from the course/textbooks under the condition of quoting its origin
  - Share ideas and understandings on the course
  - Give hints (not solutions)

Special circumstances

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

Outline

1 Logistics

2 Evaluations

3 Resources

Canvas

On Canvas platform:

- Course materials, assignments, projects
- Announcements and notifications
- Polls
- Challenges

References

Places where to find information:

- *Introduction to Modern Cryptography* (J. Katz and Y. Lindell)
- *Cryptography, theory and practice* (D. Stinson)
- Search the web

References

Places where to find information:

- *Introduction to Modern Cryptography* (J. Katz and Y. Lindell)
- *Cryptography, theory and practice* (D. Stinson)
- Search the web
- Do not use baidu

Key points

- Work regularly, do not wait the last minute/day
- Respect the Honor Code
- Go beyond what is taught
- Do not learn, understand
- Keep in touch with us
- Any advice/suggestions will be much appreciated

Thank you!