MODERN CRYPTOGRAPHY

JINTAI DING

Time: W 17:05-18:40
Office: 730 Shuangqing Building
Class romm: Old Qinghua Hall 107
email: jtding@Tsinghua.edu.cn
Office hour: W 15:00-16:00 or by appointment

No textbook

Topics:

Introduction to Symmetric crypto; RSA, Deffie-Hellman, Elliptic Curve crypto; Matsumto -imai and linearization attack; HFE cryposystems and Kipnis-Shamir attack; Algebraic attacks and its applications; UOV cryptosystems; Rainbow; Multivariate Encryption, Multivariate Hash function; NTRU; LLL lattice reduction; Learning with error; Ring Learning with Error; Lattice attack.

Prerequisite: Undergraduate linear algebra, matrix theory and abstract algebra.

Wechat will be used for communication for the class.

Homework will not be collected. We suggest that you do all the suggested problems in the classes.

Grading: Each test will account for 30 percent of the grade with 3 tests for the class. Projects will account for 15 percent of the grades.

The final grades are assigned as: A: 90-100 percent, B: 80-89 percent, C: 67-79 percent, D: 55-66 percent

ADDING / CHANGING CLASS: If you need to petition into this class (either because you need to add the course or because you want to change it), you must ask permission from the college office.

Mathematics is like learning to ride a bicycle or learning any other athletic skill- you can not learn how by only watching someone else do it. It is important that you learn by doing. Although you will see many problems worked through in lectures, it is imperative that you do the suggested exercises.

CALCULATORS: The use of calculators is permitted on all tests.

GRADING POLICY ON TESTS: Partial credit on problems is given only for work which is mostly correct. A few points will be deducted if only one or two minor errors were made. However, you should not expect partial credit for attempting to solve a problem by the wrong method. You will always be required to show appropriate work to support your answers. Do not expect to get full credit for a correct answer, if the appropriate explanation of how you got the answer is not given. When questions require written explanations, the answer will be graded on its clarity, as well as its content. The usual rules of written English apply; full sentences and paragraphs are expected. To be acceptable for full credit, written answers should be understandable the first or second time they are read.

REGRADING POLICY: If you feel an error has been made in grading your tests, you may request regrading. You stand to gain points, if we agree with your complaint; however, there is always the chance that further scrutiny of your test will determine that you should lose points. Therefore, examine your test carefully before requesting regrading. Requests for regrading must be made in writing within one week from the day the test was returned to you. You must return your test paper along with a brief and clearly worded written explanation of what you perceive the error to be. Errors in totaling your points are easy to describe and correct.

CHANGES IN SYLLABUS: If some deviations from this syllabus as we go through the course, we reserve the right to make those changes as necessary. Any such changes will be announced in class with ample warning for all students.