课程大纲
COURSE SYLLABUS

1.	**课程代码/名称** **Course Code/Title**	**CSE5014/Cryptography and Network Security**
2.	**课程性质** **Compulsory/Elective**	Elective, 专业选修课
3.	**课程学分/学时** **Course Credit/Hours**	2/32
4.	**授课语言** **Teaching Language**	English and Chinese
5.	**授课教师** **Instructor(s)**	Qi Wang, Associate Professor, Department of Computer Science and Engineering, wangqi@sustech.edu.cn 王琦、副教授、计算机科学与工程系、wangqi@sustech.edu.cn
6.	**是否面向本科生开放** **Open to undergraduates or not**	是
7.	**先修要求** **Pre-requisites**	（如面向本科生开放，请注明区分内容。 If the course is open to undergraduates, please indicate the difference.） CS201 Discrete Mathematics CS203 Data Structure and Algorithm Analysis MA212 Probability Theory and Statistics 先修课对本科生无区别，必须先修过以上或等价课程。

8. 教学目标
Course Objectives

1. Learn basics of modern cryptography, with an emphasis on fundamental ideas;
2. Be able to read, write mathematical proofs in cryptography;
3. Be able to analyze security of various cryptographic systems with formal and precise assumptions;
4. Know about certain advanced topics in cryptography

9. 教学方法
Teaching Methods

课堂讲授

10. 教学内容
Course Contents

Section 1	Course overview, cryptography history
Section 2	Perfect secrecy and its limitations
Section 3	Computational model, computational security, computational indistinguishability
Section 4	Pseudo-random generators, pseudo-random functions
Section 5	Chosen-plaintext attacks, , pseudo-random permutations
Section 6	Block ciphers, AES, Modes of operation
Section 7	Chosen-ciphertext attacks, padding oracle attack
Section 8	Authentication, message authentication codes
Section 9	Hash functions, birthday attacks, Merkle tree

	Section 10	Stream cipher, structures of block ciphers
	Section 11	Random oracle model, algebraic structures for crypto
	Section 12	RSA, Rabin's trapdoor function, discrete-logarithm problem, Diffie-Hellman problems
	Section 13	Public-key cryptography, key-exchange protocol, CPA/CCA security
	Section 14	PKCS, El Gamal encryption, digital signatures
	Section 15	Zero-knowledge proofs
	Section 16	Protocol QR, homomorphic encryption, course summary

11. 课程考核
Course Assessment

（①考核形式 Form of examination；②.分数构成 grading policy；③如面向本科生开放，请注明区分内容。If the course is open to undergraduates, please indicate the difference.）
10% quiz in class + 40% homework assignments + 50% final exam + 10% project (optional)
对本科生要求无区别（通常大四选课）。

12. 教材及其它参考资料
Textbook and Supplementary Readings

No textbook.
Introduction to Modern Cryptography, Katz & Lindell
Foundations of Cryptography, Oded Goldreich
A Graduate Course in Applied Cryptography, V. Shoup & D. Boneh
Lecture Notes on Cryptography, Goldwasser & Bellare