| | | | |
|---|---|---|---|
| Course Name | Complexity and Cryptography | | |
| Semester, Year | Second Semester, 2018 (Winter Term) | Number of Credits | 2 credits |
| Course level | 6000 | Course Number | 27107 |
| Instructor(s) (Institution) | Thomas Zeugmann (大学院情報科学研究科) | | |
| Course Objectives | Students become acquainted with fundamental algorithms that are needed in modern cryptography and their complexity.<br>We develop some understanding of what is meant by "intractable problem" and why certain "intractable problems" are fundamental for modern public-key cryptography. The subject of cryptography is introduced and a short historical overview is provided (including one-time pads).<br>Students become acquainted with the demands of modern cryptography, learn some of the most widely used public-key cryptosystems and their security and vulnerability. They also get acquainted with the ``Advanced Encryption Standard" (AES), its security and vulnerability.<br>Students learn why cryptographic protocols are needed and why ensuring their security is extremely difficult. | | |
| Course Goals | Algorithmic theory and state-of-the-art algorithmic design techniques are taught as far as these techniques are relevant for modern cryptography and cryptanalysis. Students should learn the advantages and disadvantages of modern cryptosystems and should develop a certain level of competence of how to use them. In particular, they should learn that any ignorance of certain requirements made may allow for successful attacks. | | |
| Course Schedule | 1) Addition, Multiplication (Divide and Conquer, Solving Recursive Equations)<br>2) Division and Matrix Multiplication<br>3) Number Theoretic Problems<br>4) More Number Theoretic Problems (Modular Exponentiation, Discrete Roots)<br>5) Testing Primality and Taking Discrete Roots<br>6) Factoring, Discrete Logarithms<br>7) Elliptic Curves<br>8) Hard Problems<br>9) Hash Functions, MD and SHA Hash Function Families<br>10) Classical Two-Way Cryptosystems<br>11) Security and One-Time-Pads<br>12) Public Key Cryptography, RSA<br>13) Public Key Cryptography, Merkle--Hellman, Diffie--Hellman<br>14) Authentication, Cryptographic Protocols<br>15) Advanced Encryption Standard | | |
| Homework | For homework, original materials will be distributed, and references will be indicated in the class. | | |
| Grading System | Evaluation will be carried out by the final examination. | | |
| Textbooks / Reading List | CryptoSchool Joachim von zur Gathen Springer 2015<br>Complexity Theory and Cryptology, An Introduction to Cryptocomplexity Jorg Rothe Springer 2005<br>An Introduction to Mathematical Cryptography (2nd edition) Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman<br>A Course in Number Theory and Cryptography (2nd edition) Neal Koblitz Springer 1994 | | |
| Websites | | | |
| Website of Laboratory | https://www-alg.ist.hokudai.ac.jp/index-j.html<br>https://www-alg.ist.hokudai.ac.jp/ | | |
| Additional Information | Basic knowledge of discrete mathematics, probability theory and data structures is needed. We assume familiarity with linear algebra.<br>It is strongly recommended to attend "Theory and Practice of Algorithms" prior to this lecture. | | |