ITMO University

Basic course of Mathematics for Cryptography

Course Workload		Assessment form (examination/ graded test/ ungraded test)
ECTS	Hours	
3	108	Exam

The course introduces students to the mathematical foundations of modern cryptographic schemes. It covers the factorization and discrete logarithm problems as fundamental hard problems for constructing modern algorithms. Upon completion of the course, students will gain both theoretical knowledge of modern cryptography and practical skills in working with the mathematical framework underlying contemporary schemes.

Course structure:

1. Introduction to Cryptography. Historical ciphers and their mathematical basis.

1.1. The absolutely secure Vernam cipher. Drawbacks of practical use.
1.2. Demonstrating the vulnerability of historical ciphers and the underlying mathematics. Frequency analysis as a method for breaking substitution ciphers. Brute-force attacks.
1.3. Substitution and permutation ciphers. The Spartan scytale, Cardano grille, Caesar and Vigenère ciphers. Mechanization of encryption: the Enigma cipher machine.

2. Cryptography in the Digital Age. Asymmetric ciphers, key exchange protocols, digital signatures. Mathematics underlying asymmetric algorithms.

2.1. The mathematics underlying the RSA algorithm. Euler's totient function and theorem. Fermat's little theorem. The extended Euclidean algorithm.
2.2. The concept of a hash function. Cryptographic hash function. Using hash functions to reduce message size for signing.
2.3.The problem of finding a root modulo a composite number. The concept of quadratic residue. Legendre, Jacobi, and Kronecker symbols. The Chinese Remainder Theorem.
2.4. The discrete logarithm problem for building cryptographic schemes. The ElGamal cryptosystem and its security.
2.5. The Rabin cryptosystem. Advantages and disadvantages. The mathematics underlying the cryptosystem.

2.6. RSA, ElGamal, and Rabin digital signatures. The security of the presented signature schemes.
2.7. Primality tests. Fermat and Miller-Rabin tests. Attacks on the factorization problem. Fermat's factorization method.
2.8. The Diffie-Hellman key exchange protocol. The concept of use, main advantages and disadvantages.
2.9. The concept of a digital signature. Qualified and non-qualified signatures in Russia (according to Russian law).
2.10. Group theory. Multiplicative and additive groups, rings. Special groups for cryptographic tasks (e.g., elliptic curve groups).
2.11. The integer factorization problem for building cryptographic algorithms. The RSA cryptosystem.

3. Cryptography in the Digital Age. Elegant Primitives. Secret sharing schemes, commitment schemes, zero-knowledge proof (ZKP) protocols, and variants for constructing digital signatures.

3.1. Secret Sharing Schemes. Newton's and Lagrange's interpolation formulas.
3.2. ZKP for Proving Knowledge of Graph Isomorphism.
3.3. Shamir's Secret Sharing Scheme and its properties. Advantages and disadvantages.
3.4. Concepts of Zero-Knowledge Proof (ZKP) Protocols. Ali Baba's cave as a visual example of a protocol.
3.5. ZKP for Proving Knowledge of a Composite Number's Factorization.
3.6. Blind Signatures. RSA blind signature. Application in building electronic voting systems.
3.7. Commitment Schemes. A simple scheme based on hash functions.
3.8. Design Principles for Cryptographic Primitives Based on Hard Mathematical Problems.
3.8. Mignotte's Secret Sharing Scheme. Properties. Advantages and disadvantages.
3.9 . Pedersen's Commitment Scheme and its properties.

4. Modern Symmetric Cryptography. Block and stream ciphers. Mathematics underlying symmetric algorithms.

4.1. Data Encryption Standard (DES). Algorithm structure. Feistel networks.
4.2. Random number and sequence generators. True random and pseudorandom number generators. Cryptographically secure generators.
4.3. Stream ciphers. Key differences from block ciphers and application ideas.
4.4. Linear Feedback Shift Registers (LFSR). Definition and properties.
4.5. Definition of block ciphers. The ideal block cipher. Shannon's principles of confusion and diffusion for building a practical block cipher.
4.6. RC4 cipher. Detailed description, use in TLS and SSL, basic cryptanalysis.
4.7. Basic cryptanalysis of DES. Weak, semi-weak, and possibly weak keys.
4.8. Finite fields in AES. Definition of a field, subfields, and field extensions. Field properties.
4.9. Working with polynomials. Polynomial rings, inverse polynomials in the ring, mathematical laws.
4.10. A5 cipher. Detailed description of the A5/1 variant used in the GSM standard. Cipher strength.

4.11. Triple DES (3DES). Concept and implementation.
4.12. Linear congruential generator.
4.13. AES security. Linear and differential cryptanalysis.
4.14. Advanced Encryption Standard (AES). Algorithm structure.