**Topics in Algebra: Cryptography (Prof. Dr. G. Arzhantseva)**
**Winter semester -- 2019**

## Exam questions

(1) Cryptography principles: definitions, (non) examples. Basic cryptography concepts (primitive, protocol, cover time, etc.). Basic model for secrecy: (non)-examples. Cryptosystem for secrecy: definition, examples. Symmetric versus asymmetric cryptosystems.

(2) Main attacks on encryption algorithms. Passive versus active attacks. Keys: length, size. Brute-force attack: assumptions, estimates on key lengths.

(3) Examples of symmetric cryptosystems: Caesar and Substitution ciphers. The letter frequency analysis. Monoalphabetic and polyalphabetic cyphers. Vigenère cipher. If the given key of a Vigenère Cipher has repeated letters, does it make it any easier to break?

(4) Computational complexity of basic mathematical operations and of the exhaustive key search attack. Complexity classes of algorithms.

(5) Three types of security. Perfect secrecy: definition, examples, equivalent formulations (with proof). Perfect secrecy: Shannon's Theorem (with proof).

(6) RSA cryptosystem: definition, examples, correctness (encryption and decryption are inverse operations). Parameter generation, its complexity. Main attacks.

(7) One-way function, with trapdoor. Theorem: RSA keys vs Factoring (formulation and sketch of proof).

(8) Hash function: definition, types of resistance, (non)-examples. Optimal asymmetric encryption padding.

(9) Discrete logarithm problem. The DLP assumption. The DLP in $(Z/(p-1)Z, +)$ Is breaking the ECC cryptosystem equivalent to solving the DLP?

(10) ElGamal cryptosystem and parameter generation: definition, correctness (encryption and decryption are inverse operations). Theorem: ElGamal keys versus DLP (with proof).

(11) Elliptic curve: definition, singularities, normal forms, tangents. Theorem: intersection of E with a projective line (with proof).

(12) Group structure on the elliptic curve over the algebraic closure, geometrically: definition and theorem (with proof).

(13) Cayley-Bacharach's theorem (with proof).

(14) Associativity (sketch of proof).

(15) Elliptic curves over finite fields: theorems (without proof) and examples. Check that for a prime q, each natural number in the Hasse interval occurs as the order of the elliptic curve group over the field of q elements.

(16) Diffie-Hellman key agreement: protocol, attacks. The DHP problem. The ECDHE.

(17) Digital Signature Scheme. RSA signature algorithm. Attacks: definitions and examples.

(18) DSS with hashing. Hash functions from block ciphers: definition and example, with proof (the example where $(x,y) \rightarrow a^x b^y$).

(19) DSS and Public-key cryptosystem: sign-then-encrypt versus encrypt-versus-sign.

(20) ElGamal variant of DSS: definition and correctness. Security assumptions. Example of misuse (with proof).

(21) ElGamal variant of DSS: example of misuse (with proof). ECDSA: definition and correctness.

(22) Digital currency: definition and security requirements. Distributed ledgers. Blockchain. Security assumptions underlying the generation of the bitcoin address.

(23) Bitcoin transaction and its verification. Merkle tree. Bitcoin mining.

(24) Bit generator. Linear feedback shift register: definition, periods, security. RSA bit generator.

(25) Distinguisher. Next bit predictor. Yao's theorem (sketch of proof).

(26) Error-correcting codes and expander graphs.

(27) Describe the probabilistic pidgeonhole principle and explain, with examples, why it is relevant in cryptography (i.e hash functions, birthday paradox etc).

(28) Describe a variety of attacks that rely on structural weaknesses in respective cryptosystems (for instance, known message attacks for multiplicative systems, or weaknesses of El Gamal under weak random choices).

(29) Describe Shanks algorithm, give examples of its use and outline how to use Shanks Algorithm to compute the order of an elliptic curve of prime order in combination with Hasse's bound.