The written exam will consist of two theoretical questions from the following list of general topics and two problems to solve. You will not allow to use any source of information and communicate with your colleagues. Violators will be disqualified from the exam and receive zero points for it

List of theoretical questions

Part 1: blockchain

1. Blockchain: definition and industrial examples
2. Public/private and permissioned/permission-less blockchains
3. Blockchain fork types and examples
4. Bitcoin: block structure and Merkle proof
5. Bitcoin: Proof-of-Work, automatic target value adjustment
6. Bitcoin: transactions types and structure, coin emission and circulation
7. Bitcoin: unspent transaction outputs and micropayments
8. Proof-of-X consensus protocols
9. Byzantine fault-tolerant consensus protocols
10. Smart contracts. Ethereum, Gas and Solidity
11. Lightning
12. Atomic swaps
13. Timestamping and Anchoring
14. Non-interactive zero-knowledge proof and blockchains

Part 2: cryptography

1. Secret key cryptosystem
2. Block ciphers
3. Hash functions and Merkle trees
4. Public key cryptosystems
5. Elliptic curves arithmetics
6. Esoteric protocols
7. Secret sharing schemes and threshold cryptography
8. Database systems: relations, schema, transaction, query

Problems

Part 1: blockchain

Here you would be asked to describe a blockchain-based solution for a given problem or to motivate blockchain useless for a given task.

Part 2: cryptography

1. Exponentiation by squaring algorithm
2. Extended Euclidian algorithm for inversion
3. RSA signature
4. Lagrange Interpolating Polynomial using Modulo
5. ElGamal encryption
6. Blakleys' secret sharing scheme
7. Addition of elliptic curves points

Examination ticket example

1. Bitcoin: transactions types and structure, coin emission and circulation
2. Elliptic curves arithmetics
3. Present general overview of blockchain systems in the supply chain for cargo delivery
4. Calculate 7^{21} mod 13 using exponentiation by squaring algorithm.