Introduction to blockchain. FInal exam.

Please submit your solutions as scan or clear fotos in single pdf documents as a reply to this email no later than 14:30. No late submission will be allowed. All cases of plagiarism will result at 0 grade for the whole exam. The maximal point will be 4 (1 point for each assignment). In practical problems please show all preliminary computations.

1. Block ciphers. Main building blocks. Example of block cipher.
2. Find the digital signature of message m=5 over elliptic curve $y^2 = x^3 - 3x - 6$ over F_{11} (by means of GOST R 34.10-2012). The generator is G=(1;5), size of cyclic subgroup 15, senders' open key Q=(6;4). To generate digital signature use secret parameter k=2
3. Describe Bitcoin's transactions types and its structure. How is coin emitted and circulated in a bitcoin network.
4. Present general overview of blockchain systems for digital right management.
   Describe the following:
   a. Is there a trusted central authority to maintain the system?
   b. What are the events to be tracked within the system?
   c. Are there any privacy issues?
   d. Any idea for smart contracts?
   e. Is blockchain beneficial for the considered area? Yes or No, elaborate