

Themes of the course “Gryptography”
(O. Bogopolski, summer semester 2023)

1. Background from number theory
2. Symmetric cryptosystems
3. AES
4. Asymmetric cryptosystems
5. Primality testing
6. RSA and Rabin encryption
7. Discrete logarithm cryptographic schemes
8. Diffie-Hellman key exchange
9. ElGamal
10. Elliptic curve cryptography
11. Hash functions and applications
12. Security questions and attacks