As some of the concepts and theories we have seen during this module are quite complex, it may seem difficult to prepare for the exam. In general, the exam will test your knowledge of the main concepts and applications of cryptography, rather than the mathematics behind it.

In preparing for the exam, you should focus on:

1. Basic cryptography definitions and terminology (plaintext, ciphertext, key, …)
2. Classical ciphers and basic cryptographic operations (substitution, transposition, …)
3. Main cipher families (conventional vs. public key, block vs. stream, …) and basic concepts (diffusion, avalanche effect, …)
4. Symmetric cipher modes of operations (EBC, CBC, …)
5. Attacks (brute-force vs. cryptanalysis, known/chosen plaintex/ciphertext, replay, masquerade, meet-in-the-middle, …)
6. Keylength and block size (DES, AES, RSA vs. ECC…) and how they impact security
7. Security properties of hash functions (birthday paradox, collision resistance, 1st/2nd pre-image resistance, …)
8. Randomness sources and basic tests
9. Message authentication (using hash functions, symmetric/asymmetric encryption, …), user authentication (Kerberos, …), signatures
10. TLS and how it can provide security for unsecure protocols.

I will not require knowledge of:

1. Complex mathematical operations (AES mix-columns, the theory of ECC, …)
2. Complex protocols and constructions (math basis of SHA3, …)

The multiple choice and true/false questions will focus on concepts and definitions, and they will test you knowledge of key terminology. The 3 open questions and problems will focus instead on security properties of cryptographic functions, or applications of cryptography.