Topics for the final exam from the Applied Cryptography (winter 2018)

Random and pseudorandom number generators

Advanced Encryption Standard

Triple DES

Modes of block cipher

Galois Fields and their applications in cryptography

RSA cryptosystem

Diffie-Hellman key exchange algorithm

Elliptic Curve Cryptosystems

Hash functions

Digital signatures

Message authentication codes