Summering av kursen
Krypteringsmetoder och säkring av datasystem
DI4014

Matematik
Heltalsdivision, moduloräkning, största gemensamma delare
Diofantiska ekvationer, diskret invers, kinesiska restsatsen
Primtalsbestämning, faktorisering, Eulers sats, diskret exponentiering
Aritemtik i Galoisfält, generator, LFSR
Addition och multiplikationa av matriser, definition av invers matris
Diskret polynomfaltning och diskret polynominvers
Överföringskvalitet

Datasäkerhet
Krypteringssystem (känna till hur man tillämpar Caesarkrypto, substitionskrypto, Vignèrekrypto, XOR, RSA, ElGamal, AES och NTRU med instruktion)
Kärnproblem för olika krypteringssystem (IFP, DLP, ECDLP, DHP, ECDHP, FSP, QRP, QKD, SVP)
Nyckelproblemet, nyckelhantering, lösning med superkryptering, Diffie-Hellman
Signeringssystem (känna till hur man tillämpar engångssignatur, ElGamal, DSA och RSA med instruktion)
Hashfunktioner (grundläggande principer)
Kvantdatorn (grundläggande principer)

Historia
Kriget mellan Grekland och Sparta, Caesarkryptot, arabiska metoder, substitutionskryptot och Maria Stuart, Babbage, Vignèrekryptot, Kerckhoffs princip, Enigman och Turing, Beurling, Lucifer, Diffie-Hellman, RSA