Lab 01 (2 hrs): Programming Basics

Program 1: Type Hint, String, Bytes, Hex, Base64

Lab 02 (4 hrs): Classical Cryptography

Part 1 (3 hrs):

Program 1: Vigenère cipher (on alphabet string)

Program 2: Columnar transposition (on alphabet string)

Part 2 (1 hrs):

Program 3: Vigenère cipher (on bytes)

Lab 03 (4 hrs): Symmetric Encryption

Part 1 (3 hrs):

Program 1: DES

Program 2: 3DES

Part 2 (1 hrs):

Program 3: AES

Lab 04 (4 hrs): Public Key Encryption

Part 1 (2 hrs):

Program 1: Textbook RSA (on group)

Part 2 (2 hrs):

Program 2: ElGamal (on group)

Lab 05 (2 hrs): Key Exchange

Program 1: Diffie–Hellman key exchange (on group)

Lab 06 (4 hrs): Signature

Part 1 (2 hrs):

Program 1: Textbook RSA (on group)

Part 2 (2 hrs):

Program 2: ElGamal (on group)

Lab 07 (4 hrs): Hash

Part 1 (2 hrs):

Program 1: SHA-256

Program 2: HMAC

Part 2 (2 hrs):

Program 3: Password store and verification

Lab 08 (8 hrs): Final Project

Option 1 (solo project): DIGEST authentication in real scene (sdu_net)

Option 2 (solo project): implement AES from scratch

Option 3 (group project of 2 students): hs-airdrop

Option 4 (group project of 2 students): Ethereum and smart contract demonstration

Option 5 (group project of 2 students): simple zero-knowledge proof demonstration