Lab Assignment no.04 SMPC

Q1)) Allow multiple parties to jointly compute a function over their private inputs without revealing them to each other, obtaining only the correct output

Q2)) The secret is divided into shares distributed among parties and no party or group with fewer than the threshold can reconstruct the secret

Q3)) SMPC: each party shares parts of their data, and computation is performed jointly on these shares without revealing them

Homomorphic Encryption: Computations are performed directly on encrypted data, and the remains encrypted

Q4)) Can be used in finance without revealing sensitive client data

Q5)) The data remais secure, and The secret cannot be reconstructed

Q7)) It allows computations on distributed data without revealing sensitive information to any participant

Q6)) is a method of encrypting a logical circuit so that another party can evaluate it and get the correct output without learning anything about the other party's secret inputs

Q8)) ① Data was distributed

② the final result was correct and reliable

③ each party did not know others data but total sum accurate.