

QP CODE 2100550304

Reg.No

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--



DMI-ST. EUGENE UNIVERSITY

ZAMBIA

DEGREE EXAMINATION – DECEMBER 2023

Semester: X

055EL003 INFORMATION SECURITY

Time: 3:00 Hours

Max. Marks: 100

Answer any FIVE Questions (5 x 20 = 100 Marks)

1. a) What is cryptography? What are the applications of cryptography? (10 Marks)
b) Explain two types of transposition cipher techniques. (10 Marks)
2. a) Briefly describe the message state and key state of the Advanced Encryption Standard. (10 Marks)
b) Explain the key generation of the Data Encryption Standard. (10 Marks)
3. a) Define a cryptographic hash function. (4 Marks)
b) Explain three properties of a hash function. (6 Marks)
c) Define a digital signature. (4 Marks)
d) State three applications of a digital signature. (6 Marks)
4. a) Outline the benefits of Kerberos Authentication. (10 Marks)
b) Describe the components of encapsulating security payload. (10 Marks)
5. a) Describe five design principles of a firewall. (10 Marks)
b) State at four classifications of intrusion detection systems. (10 Marks)
6. a) Explain four types of attacks on cryptosystems. (10 Marks)
b) Explain substitution cipher with an example. (5 Marks)
c) Describe the two types of cryptography. (5 Marks)
7. a) Describe five services of Pretty Good Privacy. (10 Marks)
b) Describe five Applications of Kerberos. (10 Marks)