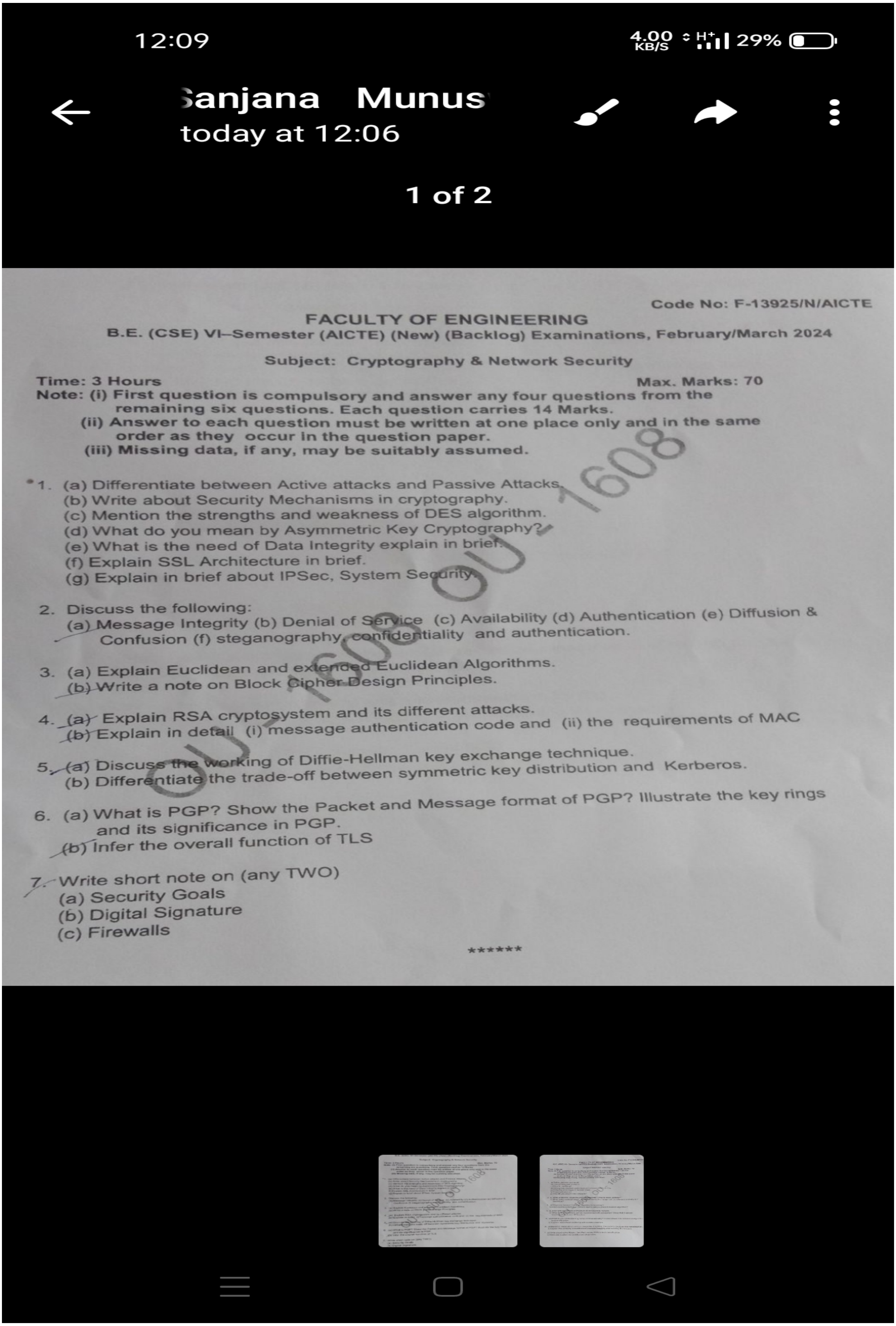

Code No: F-13925/N/AICTE

FACULTY OF ENGINEERING

B.E. (CSE) VI–Semester (AICTE) (New) (Backlog) Examinations, February/March 2024

Subject: Cryptography & Network Security

Time: 3 Hours **Max. Marks: 70**

Note: (i) First question is compulsory and answer any four questions from the remaining six questions. Each question carries 14 Marks.
(ii) Answer to each question must be written at one place only and in the same order as they occur in the question paper.
(iii) Missing data, if any, may be suitably assumed.

1. (a) Differentiate between Active attacks and Passive Attacks.
(b) Write about Security Mechanisms in cryptography.
(c) Mention the strengths and weakness of DES algorithm.
(d) What do you mean by Asymmetric Key Cryptography?
(e) What is the need of Data Integrity explain in brief.
(f) Explain SSL Architecture in brief.
(g) Explain in brief about IPSec, System Security.

2. Discuss the following:
(a) Message Integrity (b) Denial of Service (c) Availability (d) Authentication (e) Diffusion & Confusion (f) steganography, confidentiality and authentication.

3. (a) Explain Euclidean and extended Euclidean Algorithms.
(b) Write a note on Block Cipher Design Principles.

4. (a) Explain RSA cryptosystem and its different attacks.
(b) Explain in detail (i) message authentication code and (ii) the requirements of MAC

5. (a) Discuss the working of Diffie-Hellman key exchange technique.
(b) Differentiate the trade-off between symmetric key distribution and Kerberos.

6. (a) What is PGP? Show the Packet and Message format of PGP? Illustrate the key rings and its significance in PGP.
(b) Infer the overall function of TLS

7. Write short note on (any TWO)
(a) Security Goals
(b) Digital Signature
(c) Firewalls

******