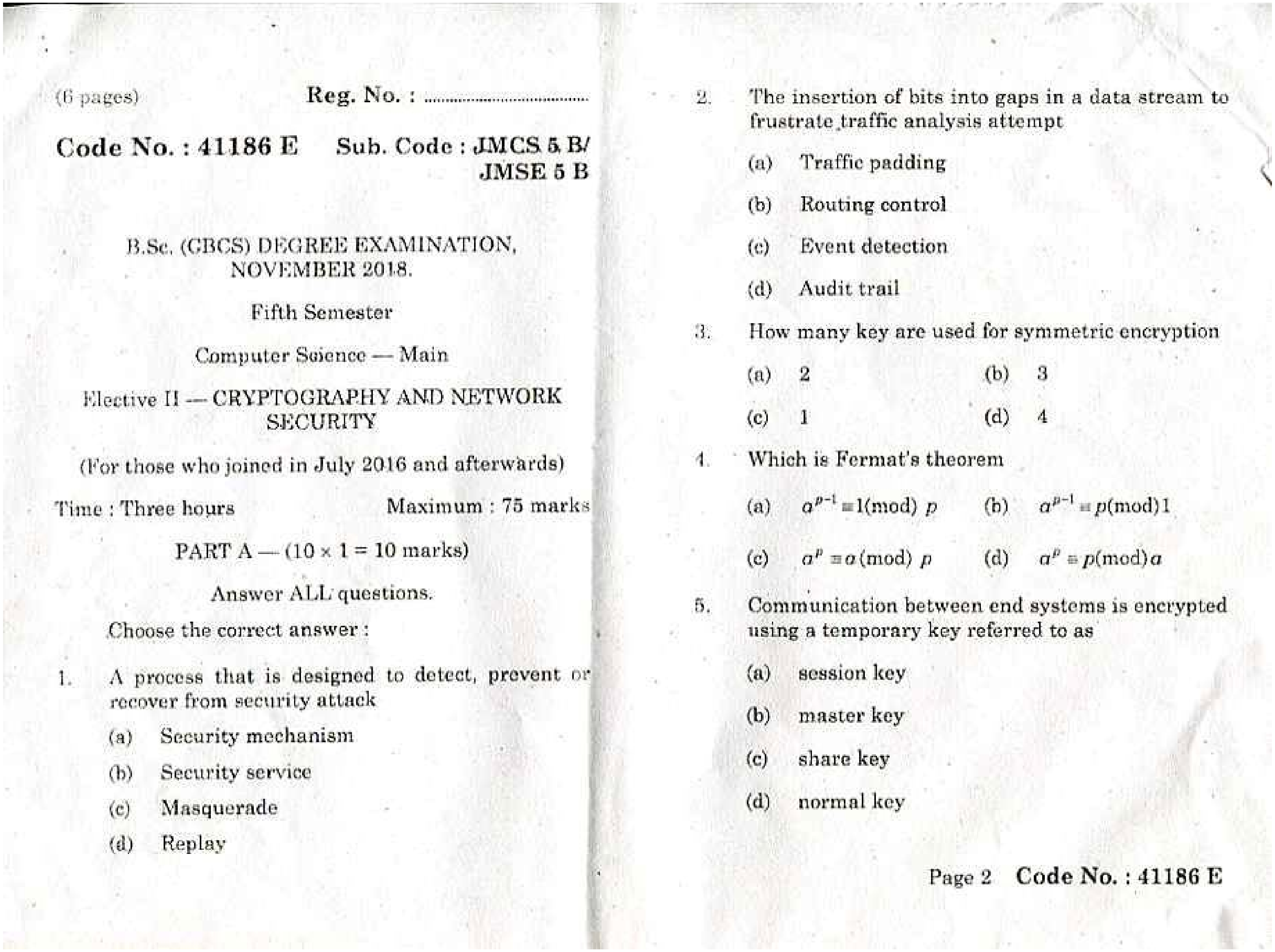

(6 pages) **Reg. No. : ....**

Code No. : 41186 E **Sub. Code : JMCS 5 B/ JMSE 5 B**

B.Sc. (CBCS) DEGREE EXAMINATION,
NOVEMBER 2018.

Fifth Semester

Computer Science — Main

Elective II — CRYPTOGRAPHY AND NETWORK SECURITY

(For those who joined in July 2016 and afterwards)

Time : Three hours Maximum : 75 marks

PART A — (10 × 1 = 10 marks)

Answer ALL questions.

Choose the correct answer :

1. A process that is designed to detect, prevent or recover from security attack

   (a) Security mechanism

   (b) Security service

   (c) Masquerade

   (d) Replay

2. The insertion of bits into gaps in a data stream to frustrate traffic analysis attempt

   (a) Traffic padding

   (b) Routing control

   (c) Event detection

   (d) Audit trail

3. How many key are used for symmetric encryption

   (a) 2 (b) 3

   (c) 1 (d) 4

4. Which is Fermat's theorem

   (a) $a^{p-1} \equiv 1(\text{mod})\ p$ (b) $a^{p-1} \equiv p(\text{mod})1$

   (c) $a^{p} \equiv a(\text{mod})\ p$ (d) $a^{p} \equiv p(\text{mod})a$

5. Communication between end systems is encrypted using a temporary key referred to as

   (a) session key

   (b) master key

   (c) share key

   (d) normal key

6. Release of message contents to any person or process not possessing the appropriate cryptographic key

(a) disclosure

(b) masquerade

(c) content modification

(d) sequence modification

7. Which at the following is application area in client/server

(a) S/mme (b) Kerberos

(c) SSL (d) TLS

8. Which provides security services between TCP and application that use TCP

(a) SSL (b) RSA

(c) DSS (d) ZIP

9. Set of tools for generating new viruses automatically

(a) Kit (b) flooders

(c) Spy ware (d) Adware

10. A backdoor is also known as

(a) Trapdoor (b) Spy ware

(c) Ad ware (d) Root kit

PART B — (5 × 5 = 25 marks)

Answer ALL questions choosing either (a) or (b).

Each answer should not exceed 250 words.

11. (a) Discuss security services in detail.

Or

(b) Explain OSI security architecture in detail.

12. (a) Describe principles of public key crypto system.

Or

(b) Write notes about advanced symmetric block ciphers.

13. (a) Discuss about dittie hellman key exchange.

Or

(b) Write notes about secure Hash algorithm.

14. (a) Explain IP security policy in detail.

Or

(b) Discuss about PGP pretty good privacy.

15. (a) Explain passward selection strotegies in detail.

Or

(b) Discuss about malicious program in detail.

PART C — (5 × 8 = 40 marks)

Answer ALL questions choosing either (a) or (b).

Each answer should not exceed 600 words.

16. (a) Explain data encryption standard in detail.

Or

(b) Explain substitution technique in detail.

17. (a) Discuss fermat's and Euler's theorem in detail.

Or

(b) Discuss RSA algorithm in detail.

18. (a) Describe digital signature standard in detail.

Or

(b) Describe steps involved in authentication process in detail.

19. (a) Write about transport layer security in detail.

Or

(b) Write about secure socket layer architecture in detail.

20. (a) Explain types of firewall in detail.

Or

(b) Explain Intrusion detection in detail.