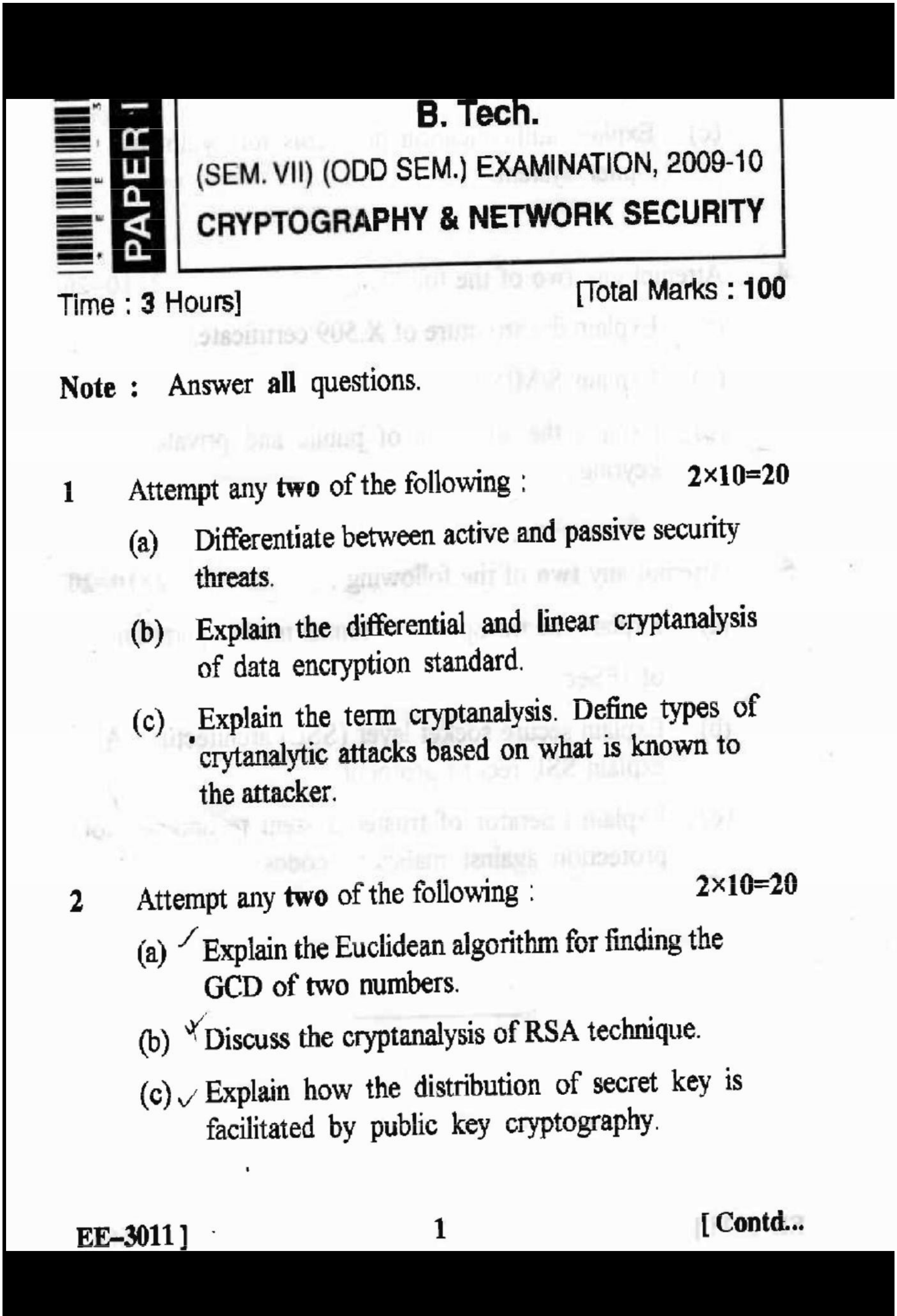

B. Tech.

(SEM. VII) (ODD SEM.) EXAMINATION, 2009-10

CRYPTOGRAPHY & NETWORK SECURITY

Time : **3** Hours] [Total Marks : **100**

Note : Answer **all** questions.

1 Attempt any **two** of the following : 2×10=20

(a) Differentiate between active and passive security threats.

(b) Explain the differential and linear cryptanalysis of data encryption standard.

(c) Explain the term cryptanalysis. Define types of crytanalytic attacks based on what is known to the attacker.

2 Attempt any **two** of the following : 2×10=20

(a) Explain the Euclidean algorithm for finding the GCD of two numbers.

(b) Discuss the cryptanalysis of RSA technique.

(c) Explain how the distribution of secret key is facilitated by public key cryptography.

3 Attempt any **two** of the following : **2×10=20**

(a) ✓ Describe the structure of secure hash function.

(b) ✓ Explain direct and arbitrated methods for digital signatures.

(c) Explain authentication protocols for symmetric cipher system.

4 Attempt any **two** of the following : **2×10=20**

(a) ✓ Explain the structure of X.509 certificate.

(b) Explain S/MIME.

(c) ✓ Explain the structure of public and private keyrings.

5 Attempt any **two** of the following : **2×10=20**

(a) Explain the transport and tunnel mode operation of IPSec.

(b) Explain secure socket layer (SSL) architecture. Also explain SSL record protocol.

(c) Explain operator of trusted system technology for protection against malicious codes.