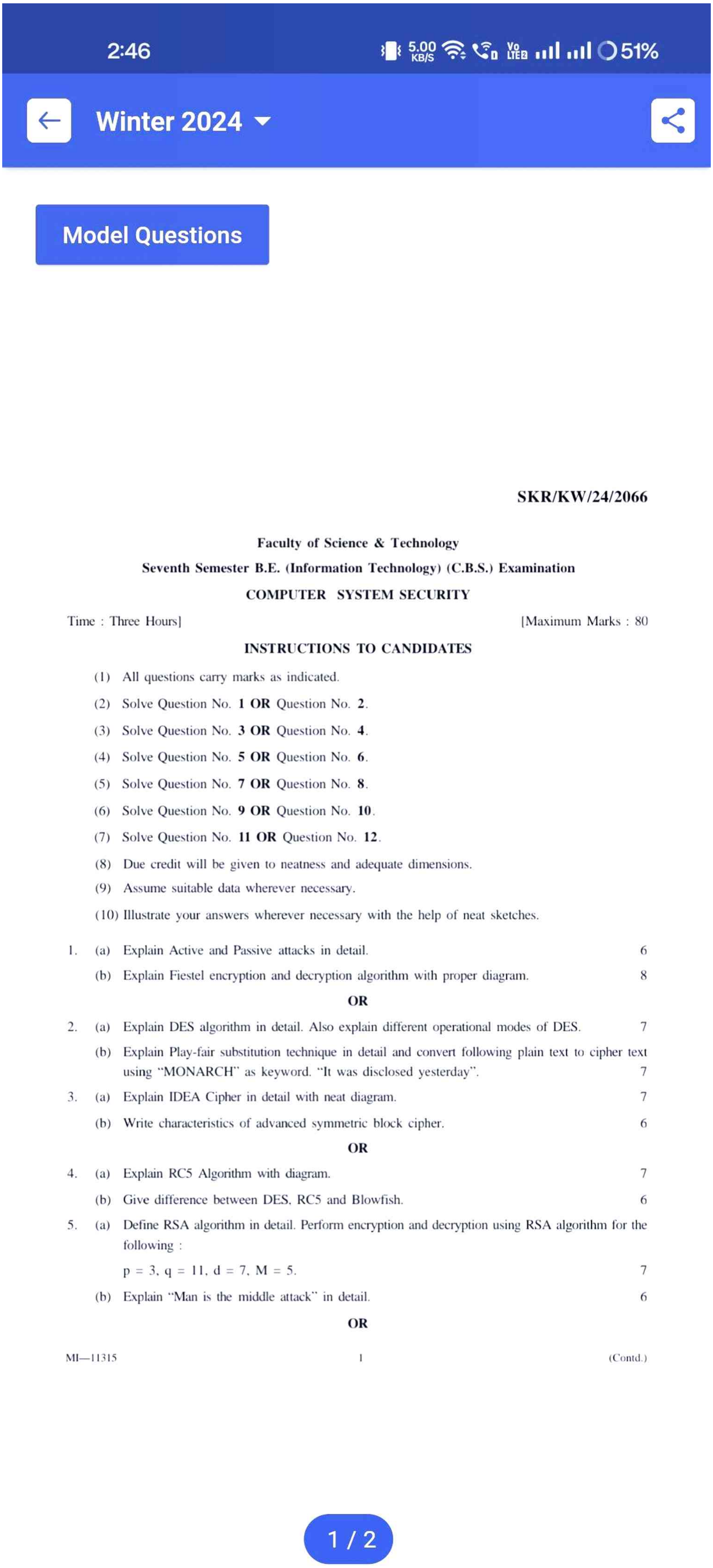


SKR/KW/24/2066

Faculty of Science & Technology

Seventh Semester B.E. (Information Technology) (C.B.S.) Examination

COMPUTER SYSTEM SECURITY

Time : Three Hours] [Maximum Marks : 80

INSTRUCTIONS TO CANDIDATES

(1) All questions carry marks as indicated.

(2) Solve Question No. **1** **OR** Question No. **2**.

(3) Solve Question No. **3** **OR** Question No. **4**.

(4) Solve Question No. **5** **OR** Question No. **6**.

(5) Solve Question No. **7** **OR** Question No. **8**.

(6) Solve Question No. **9** **OR** Question No. **10**.

(7) Solve Question No. **11** **OR** Question No. **12**.

(8) Due credit will be given to neatness and adequate dimensions.

(9) Assume suitable data wherever necessary.

(10) Illustrate your answers wherever necessary with the help of neat sketches.

1. (a) Explain Active and Passive attacks in detail. 6

(b) Explain Fiestel encryption and decryption algorithm with proper diagram. 8

OR

2. (a) Explain DES algorithm in detail. Also explain different operational modes of DES. 7

(b) Explain Play-fair substitution technique in detail and convert following plain text to cipher text using "MONARCH" as keyword. "It was disclosed yesterday". 7

3. (a) Explain IDEA Cipher in detail with neat diagram. 7

(b) Write characteristics of advanced symmetric block cipher. 6

OR

4. (a) Explain RC5 Algorithm with diagram. 7

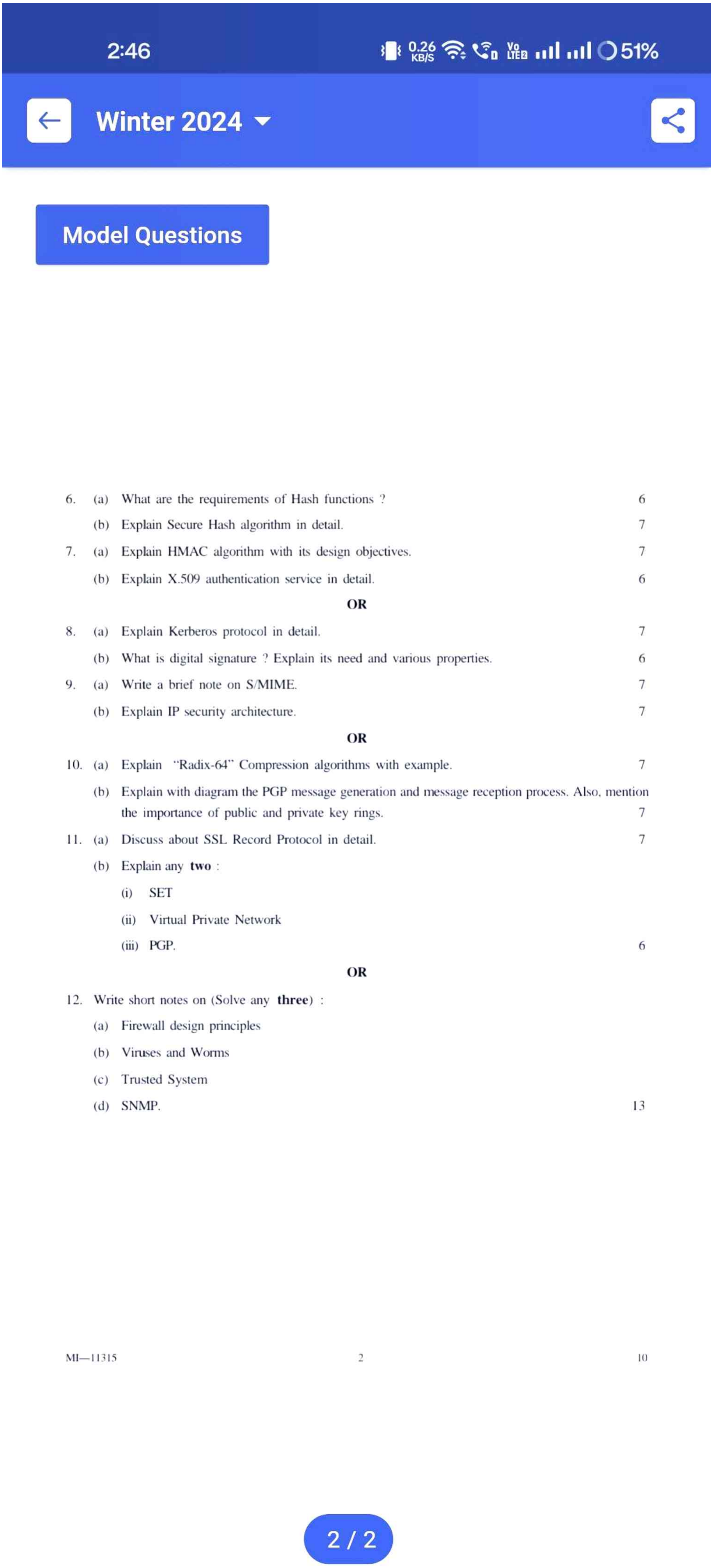
(b) Give difference between DES, RC5 and Blowfish. 6

5. (a) Define RSA algorithm in detail. Perform encryption and decryption using RSA algorithm for the following :

$p = 3$, $q = 11$, $d = 7$, $M = 5$. 7

(b) Explain "Man is the middle attack" in detail. 6

OR



6. (a) What are the requirements of Hash functions ? 6

(b) Explain Secure Hash algorithm in detail. 7

7. (a) Explain HMAC algorithm with its design objectives. 7

(b) Explain X.509 authentication service in detail. 6

OR

8. (a) Explain Kerberos protocol in detail. 7

(b) What is digital signature ? Explain its need and various properties. 6

9. (a) Write a brief note on S/MIME. 7

(b) Explain IP security architecture. 7

OR

10. (a) Explain "Radix-64" Compression algorithms with example. 7

(b) Explain with diagram the PGP message generation and message reception process. Also, mention the importance of public and private key rings. 7

11. (a) Discuss about SSL Record Protocol in detail. 7

(b) Explain any **two** :

(i) SET

(ii) Virtual Private Network

(iii) PGP. 6

OR

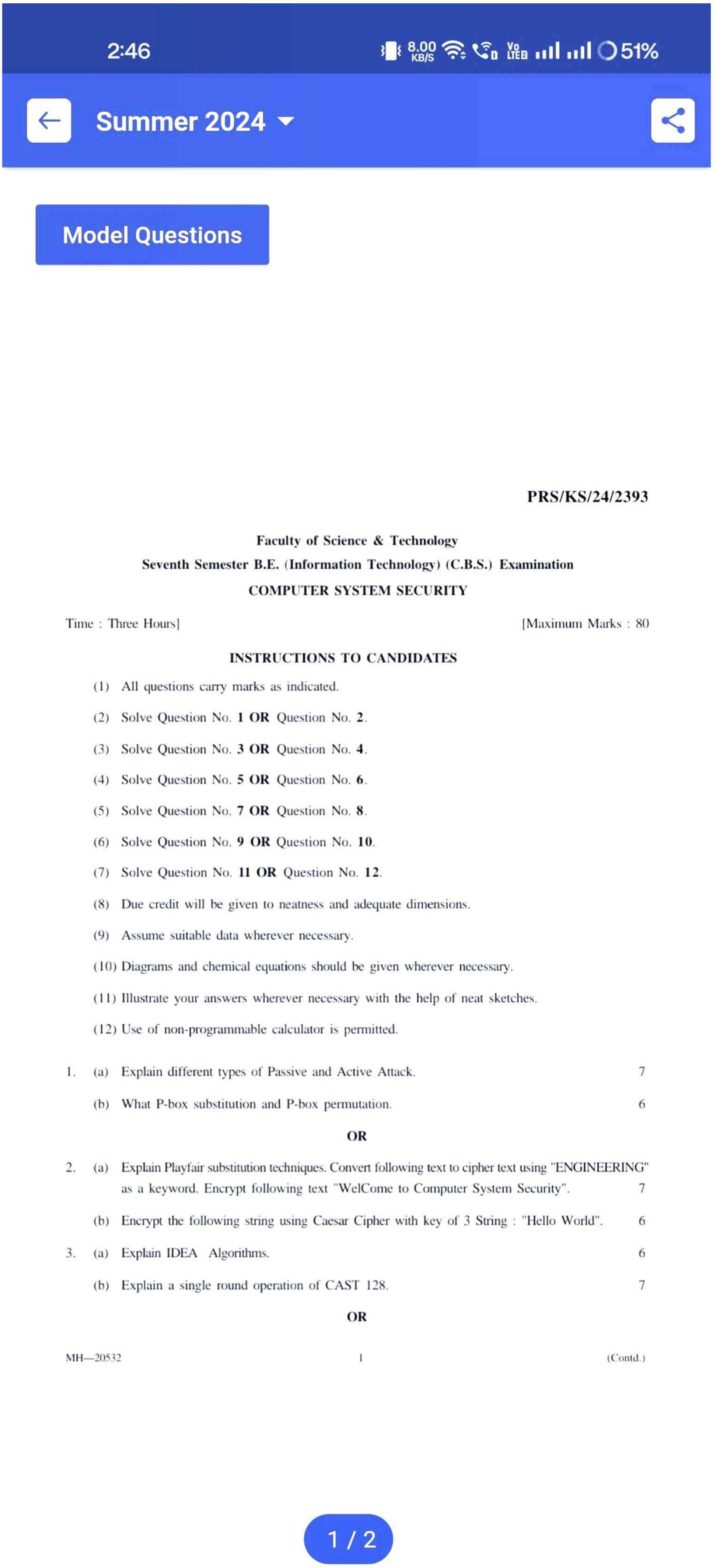
12. Write short notes on (Solve any **three**) :

(a) Firewall design principles

(b) Viruses and Worms

(c) Trusted System

(d) SNMP. 13



PRS/KS/24/2393

Faculty of Science & Technology

Seventh Semester B.E. (Information Technology) (C.B.S.) Examination

COMPUTER SYSTEM SECURITY

Time : Three Hours] [Maximum Marks : 80

INSTRUCTIONS TO CANDIDATES

(1) All questions carry marks as indicated.

(2) Solve Question No. **1 OR** Question No. **2**.

(3) Solve Question No. **3 OR** Question No. **4**.

(4) Solve Question No. **5 OR** Question No. **6**.

(5) Solve Question No. **7 OR** Question No. **8**.

(6) Solve Question No. **9 OR** Question No. **10**.

(7) Solve Question No. **11 OR** Question No. **12**.

(8) Due credit will be given to neatness and adequate dimensions.

(9) Assume suitable data wherever necessary.

(10) Diagrams and chemical equations should be given wherever necessary.

(11) Illustrate your answers wherever necessary with the help of neat sketches.

(12) Use of non-programmable calculator is permitted.

1. (a) Explain different types of Passive and Active Attack. 7

(b) What P-box substitution and P-box permutation. 6

OR

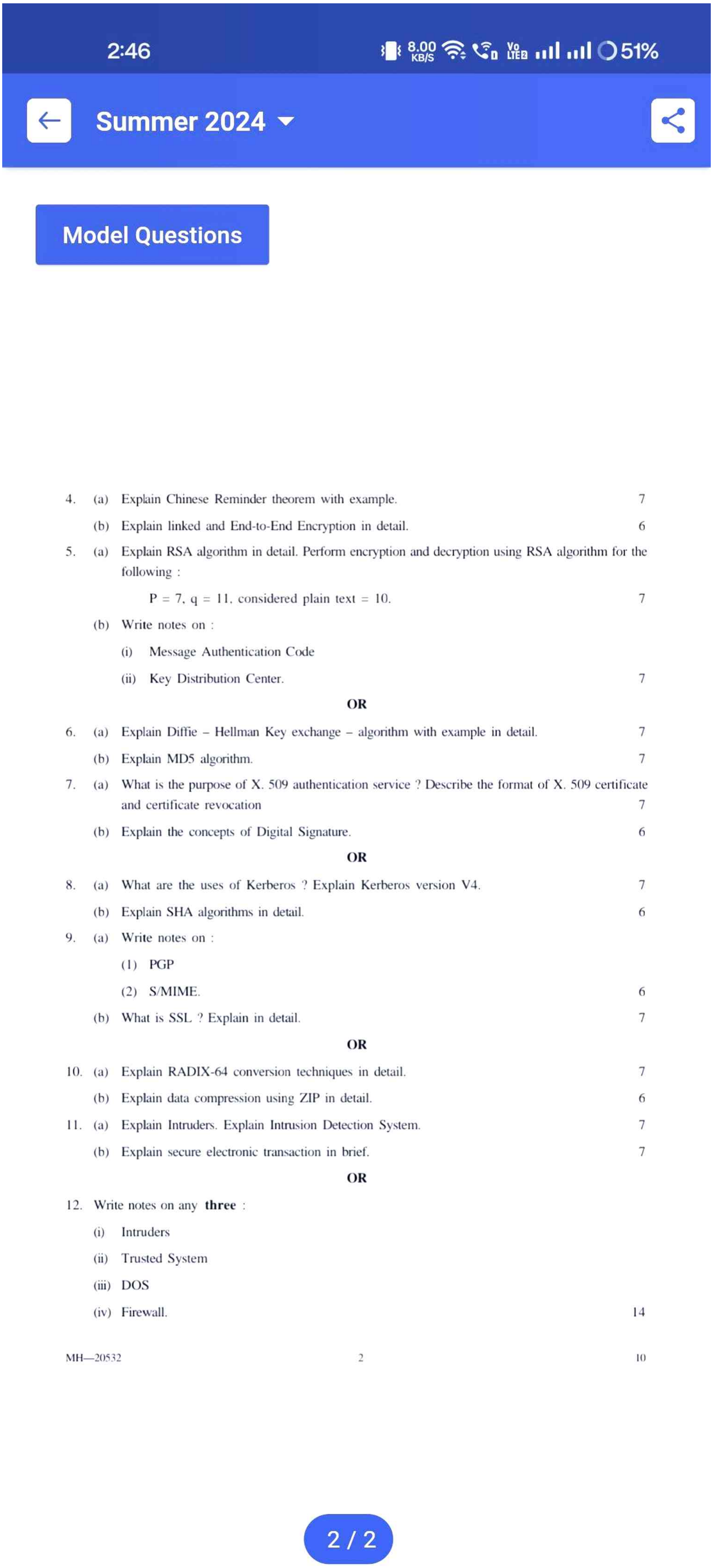
2. (a) Explain Playfair substitution techniques. Convert following text to cipher text using "ENGINEERING" as a keyword. Encrypt following text "WelCome to Computer System Security". 7

(b) Encrypt the following string using Caesar Cipher with key of 3 String : "Hello World". 6

3. (a) Explain IDEA Algorithms. 6

(b) Explain a single round operation of CAST 128. 7

OR



4. (a) Explain Chinese Reminder theorem with example. 7

(b) Explain linked and End-to-End Encryption in detail. 6

5. (a) Explain RSA algorithm in detail. Perform encryption and decryption using RSA algorithm for the following :

P = 7, q = 11, considered plain text = 10. 7

(b) Write notes on :

(i) Message Authentication Code

(ii) Key Distribution Center. 7

OR

6. (a) Explain Diffie – Hellman Key exchange – algorithm with example in detail. 7

(b) Explain MD5 algorithm. 7

7. (a) What is the purpose of X. 509 authentication service ? Describe the format of X. 509 certificate and certificate revocation 7

(b) Explain the concepts of Digital Signature. 6

OR

8. (a) What are the uses of Kerberos ? Explain Kerberos version V4. 7

(b) Explain SHA algorithms in detail. 6

9. (a) Write notes on :

(1) PGP

(2) S/MIME. 6

(b) What is SSL ? Explain in detail. 7

OR

10. (a) Explain RADIX-64 conversion techniques in detail. 7

(b) Explain data compression using ZIP in detail. 6

11. (a) Explain Intruders. Explain Intrusion Detection System. 7

(b) Explain secure electronic transaction in brief. 7

OR

12. Write notes on any **three** :

(i) Intruders

(ii) Trusted System

(iii) DOS

(iv) Firewall. 14