

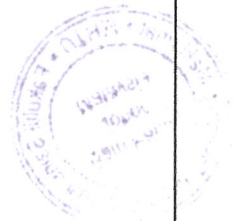


**UNIVERSITI TUN HUSSEIN ONN MALAYSIA**

**FINAL EXAMINATION  
SEMESTER II  
SESSION 2017/2018**

COURSE NAME : FUNDAMENTAL OF INFORMATION SECURITY  
COURSE CODE : BIS 10103  
PROGRAMME CODE : BIS  
EXAMINATION DATE : JUNE/JULY 2018  
DURATION : 3 HOURS  
INSTRUCTION : ANSWERS ALL QUESTIONS

**TERBUKA**



THIS QUESTION PAPER CONSISTS OF **THREE (3)** PAGES

Q1 Differentiate ALL of the following terms:

- (a) Linear Cryptanalysis and Differential Cryptanalysis.
- (b) HTTP and HTTPS.
- (c) Block Chain and Databases.
- (d) Cryptocurrency and digital cash.

(20 marks)

Q2 (a) Find the hidden words communicated from `dolphin.jpg` as shown in Figure Q2(a). The format of the message is in Hexadecimal. Given that ASCII Codes for “A” is 41, “B” is 42 ,....”Z” is 5A and “.” is 2E.

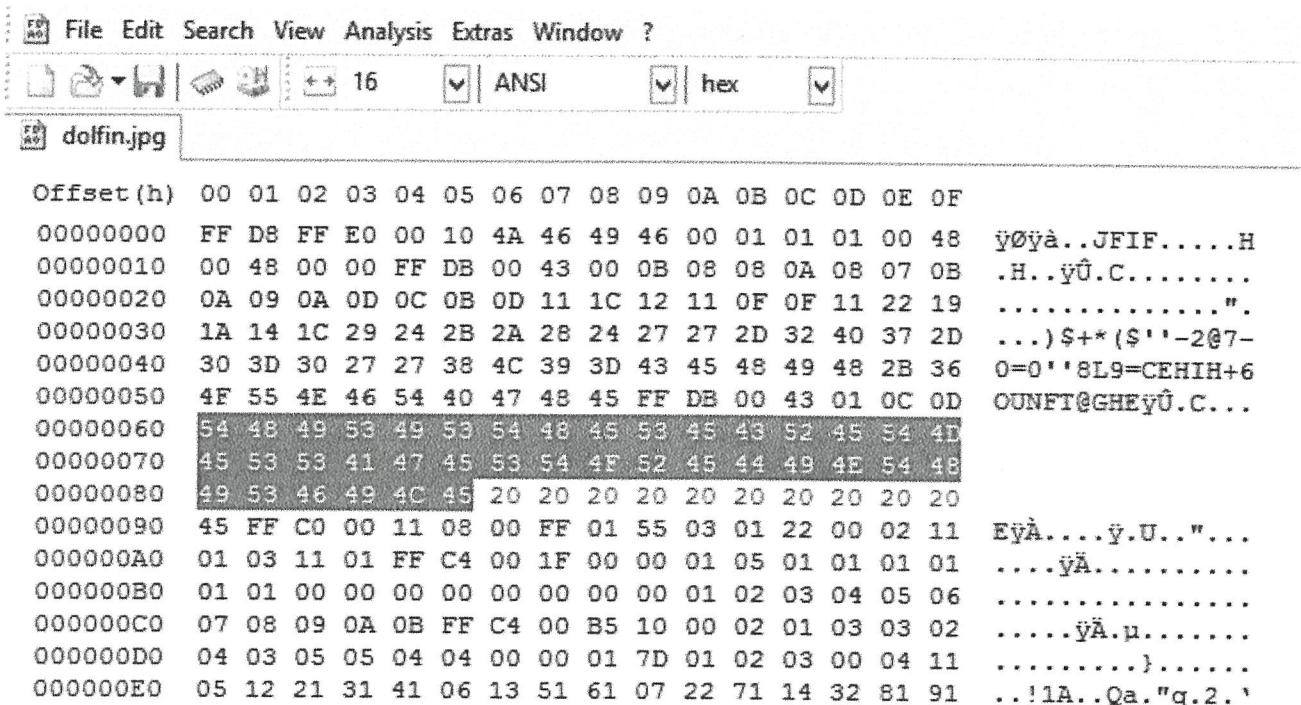


FIGURE Q2(a)



(b) Given a message “IREALLYLOVEUTHMATECHNICALUNIVERSITYIN MALAYSIA” using SHIFT +13 as the key.

(10 marks)

- Q3** (a) State **TWO (2)** purposes for creating a Digital Signature for an electronic document. (4 marks)
- (b) Describe **TWO (2)** processes for creating a Digital Signature for an electronic document. (4 marks)
- (c) Describe **THREE (3)** steps for creating a Digital Certificate for an electronic document using MD5 algorithm and Public Key Infrastructure (PKI). (12 marks)
- Q4** Discuss **EIGHT (8)** steps for an organization to protect their computer network against ransomware attack. (20 marks)
- Q5** You had just been appointed as a security administrator for a new private Bank. Your Information Technology and Security team has been asked to prepare a proposal for implementing a secure online banking system (e-BANK). With this new e-BANK, any customer is able to register and perform online banking.
- Propose **ONE (1)** security solution that addresses confidentiality, integrity and availability requirement associated with this system. (20 marks)

- END OF QUESTION -

