JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF MASTER OF SCIENCE IN IT AND SECURITY AUDIT

1^{ST} YEAR 1^{ST} SEMESTER 2018/2019 ACADEMIC YEAR

KISUMUCAMPUS

COURSE CODE : IIT 5114

COURSE TITLE : SECURING AN E-COMMERCE INFRASTRUCTURE

EXAM VENUE : **STREAM :**

DATE : 13/08/ 2019 **EXAM SESSION : 9.00 – 12.00NOON**

TIME: 2.00 HOURS

INSTRUCTIONS:

1. **Answer Question 1 (Compulsory) and ANY other two questions**
2. **Candidates are advised not to write on the question paper**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

QUESTION ONE 20 MARKS

a) Consider the task of designing a Web server that will target specifically E- commerce, with the objective of accommodating a number of merchant sites, each consisting of a catalog, shopping cart, payment system interfacing with a credit card company, customer profiles repository based on previous transactions, and a recommender system. What specific architectural suggestions would you make to ensure.

(i) Efficiency **(3 Marks)**

(ii) Security **(3 Marks)**

(iii) Reliability? **(3 Marks)**

b) Describe three types of encryptions that can be used to enhance security aspects of an e commerce infrastructure. **(6 Marks)**

c) Security is very important in online shopping sites. There are some security tools that are used to protect and safeguard e commerce transactions. Describe E- Commerce security tools available. **(5 Marks)**

QUESTION TWO 20 MARKS

a) A digital signature can provide three services: message integrity, message authentication, and nonrepudiation. Note that a digital signature scheme does not provide confidential communication. If confidentiality is required, the message and the signature must be encrypted using either a secret-key or public-key cryptosystem. Describe how a digital signature can provide the three services;

i. Message authentication **(5 Marks)**

ii. Message Integrity **(5 Marks)**

iii. Message Nonrepudiation **(5 Marks)**

b) A firewall is a device that filters all traffic between a protected or "inside" network and a less trustworthy or "outside" network. List Five types of firewall. **(5 Marks)**

QUESTION THREE 20 MARKS

a) E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Mention eight (8) e commerce security tool that exist in an e commerce environment. **(8 Marks)**

b) E-commerce security has its own particular nuances and is one of the highest visible security components that affect the end user through their daily payment interaction with business. You are required to describe atleast three types of security threats. **(6 Marks)**

c) Discuss why new and improved security measures are not enough to stop online crime. What is the missing ingredient? **(6 Marks)**

QUESTION FOUR 20 MARKS

a) E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. While security features do not guarantee a secure system, they are necessary to build a secure system. Discuss FOUR (4) categories of Security features in an e commerce environment. **(8 Marks)**

b) Huge amount is being purchased on the internet, because it‘s easier and more convenient. Unfortunately, Cyber criminals are also very busy attempting to commit fraud online. As an E Commerce security expert, you are required to advice online shoppers on a secure online shopping guidelines. **(6 Marks)**

c) Explain the role of digital signature in e commerce **(4 Marks)**

d) Explain the significance of cryptography **(2 Marks)**

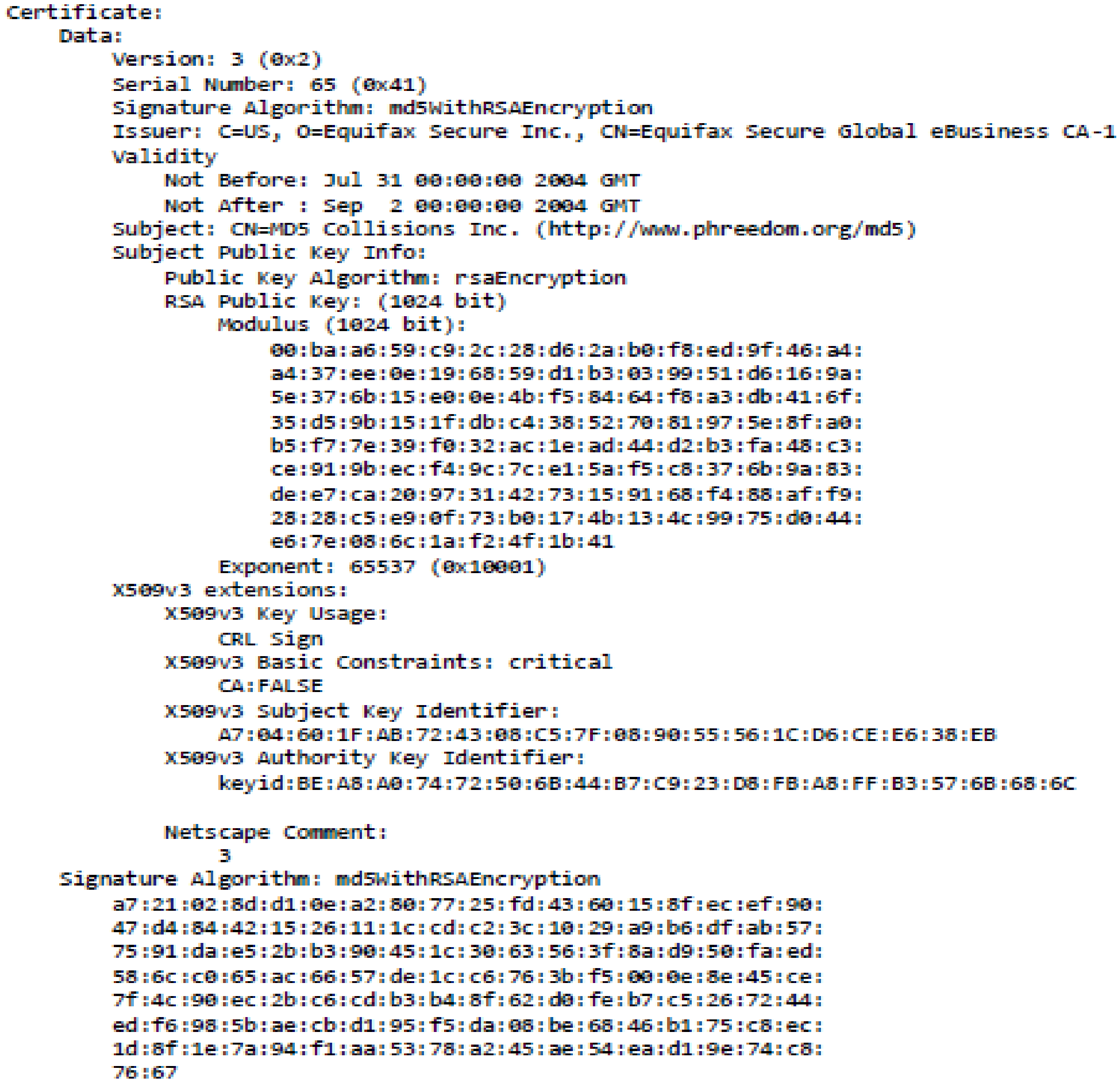
QUESTION FIVE 20 MARKS

a) There are some Emerging security technologies that were recently developed as technologies that appear likely to have an impact on the future of ecommerce and its security. Describe atleast three new security technology according to Pita Jarupunphol and Wipawan Buathong (2016) in their paper entitled The Future of e-Commerce Security. **(4 Marks)**

b) Explain the significance of customer privacy and transaction security in e commerce **(4 Marks)**

c) Existing Online Payment transaction communication is secured by using SSL/TLS protocol in order to protect the connection between the customer and the server. However, SSL/TLS protocol is vulnerable to different attacks. This problem can be solved by evolving Double Verification during the transactions. Explain the steps involve in a secure online payment using Double Verification. **(6 Marks)**

d) During the process of retrieving a web page from a web server using an SSL connection, you receive the certificate shown below. Mention several reasons to not trust this certificate. Mention also if some of the used algorithms are considered insecure nowadays. **(6 Marks)**



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 65 (0x41)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=US, O=Equifax Secure Inc., CN=Equifax Secure Global eBusiness CA-1
        Validity
            Not Before: Jul 31 00:00:00 2004 GMT
            Not After : Sep  2 00:00:00 2004 GMT
        Subject: CN=MD5 Collisions Inc. (http://www.phreedom.org/md5)
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:ba:a6:59:c9:2c:28:d6:2a:b0:f8:ed:9f:46:a4:
                    a4:37:ee:0e:19:68:59:d1:b3:03:99:51:d6:16:9a:
                    5e:37:6b:15:e0:0e:4b:f5:84:64:f8:a3:db:41:6f:
                    35:d5:9b:15:1f:db:c4:38:52:70:81:97:5e:8f:a0:
                    b5:f7:7e:39:f0:32:ac:1e:ad:44:d2:b3:fa:48:c3:
                    ce:91:9b:ec:f4:9c:7c:e1:5a:f5:c8:37:6b:9a:83:
                    de:e7:ca:20:97:31:42:73:15:91:68:f4:88:af:f9:
                    28:28:c5:e9:0f:73:b0:17:4b:13:4c:99:75:d0:44:
                    e6:7e:08:6c:1a:f2:4f:1b:41
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage:
                CRL Sign
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:
                A7:04:60:1F:AB:72:43:08:C5:7F:08:90:55:56:1C:D6:CE:E6:38:EB
            X509v3 Authority Key Identifier:
                keyid:BE:A8:A0:74:72:50:6B:44:B7:C9:23:D8:FB:A8:FF:B3:57:6B:68:6C

            Netscape Comment:
                3
    Signature Algorithm: md5WithRSAEncryption
        a7:21:02:8d:d1:0e:a2:80:77:25:fd:43:60:15:8f:ec:ef:90:
        47:d4:84:42:15:26:11:1c:cd:c2:3c:10:29:a9:b6:df:ab:57:
        75:91:da:e5:2b:b3:90:45:1c:30:63:56:3f:8a:d9:50:fa:ed:
        58:6c:c0:65:ac:66:57:de:1c:c6:76:3b:f5:00:0e:8e:45:ce:
        7f:4c:90:ec:2b:c6:cd:b3:b4:8f:62:d0:fe:b7:c5:26:72:44:
        ed:f6:98:5b:ae:cb:d1:95:f5:da:08:be:68:46:b1:75:c8:ec:
        1d:8f:1e:7a:94:f1:aa:53:78:a2:45:ae:54:ea:d1:9e:74:c8:
        76:67
```