

Name:

Enrolment No:



UNIVERSITY OF PETROLEUM & ENERGY STUDIES

End Semester Examination (Online) – Dec, 2020

Course: E-commerce Payment

Semester: V

Program: BBA (E-business)

Time: 03 hrs.

Course Code: DSIT 3003

Max. Marks: 100

IMPORTANT INSTRUCTIONS

1. The student must write his/her name and enrolment no. in the space designated above.
2. Use of calculator allowed.
3. Differentiation in marks will be based on how adequately explanations are given and illustrated.

SECTION A

Q.No

1. Each Question will carry 6 Marks
2. Instruction: Complete the statement / Select the correct answer(s) – Any answer should not exceed 100 words

Marks

COs

Multiple choice questions

In a Cryptography RSA Algorithm calculation:
Given, $p=13$, $q=17$, $e=5$.

Formulae:

$$d = (2(\phi(n)) + 1) / e.$$

Choose the private key, encryption formula, and decryption formula respectively, given the encrypted value for the message “89” is “72”.

1.

- i) $(77,221)$, $89^{221} \bmod 5$, and $72^{77} \bmod 5$
- ii) $(77,221)$, $89^5 \bmod 221$, and $72^{77} \bmod 221$
- iii) $(77,221)$, $89^5 \bmod 221$, and $77^{72} \bmod 221$
- iv) $(38,221)$, $89^5 \bmod 221$, and $38^{72} \bmod 221$
- v) $(77,221)$, $89^{221} \bmod 5$ and $72^{221} \bmod 77$
- vi) $(77,221)$, $89^5 \bmod 221$, and $72^5 \bmod 77$

5

CO3

2.	<p><u>Match the following:</u></p> <table border="1" data-bbox="233 260 1219 947"> <tr> <td data-bbox="233 260 727 327">a. iPaaS</td> <td data-bbox="727 260 1219 327">i. G2E</td> </tr> <tr> <td data-bbox="233 327 727 443">b. M-commerce</td> <td data-bbox="727 327 1219 443">ii. Type of e-commerce business model</td> </tr> <tr> <td data-bbox="233 443 727 510">c. EDI</td> <td data-bbox="727 443 1219 510">iii. E-bill payment</td> </tr> <tr> <td data-bbox="233 510 727 625">d. Online facilities to employees to leave</td> <td data-bbox="727 510 1219 625">iv. Type of e-commerce business model</td> </tr> <tr> <td data-bbox="233 625 727 693">e. Brokerage</td> <td data-bbox="727 625 1219 693">v. Future to EDI</td> </tr> <tr> <td data-bbox="233 693 727 760"></td> <td data-bbox="727 693 1219 760">vi. G2G</td> </tr> <tr> <td data-bbox="233 760 727 875"></td> <td data-bbox="727 760 1219 875">vii. Paper-less exchange of information</td> </tr> <tr> <td data-bbox="233 875 727 947"></td> <td data-bbox="727 875 1219 947">viii. G2C</td> </tr> </table>	a. iPaaS	i. G2E	b. M-commerce	ii. Type of e-commerce business model	c. EDI	iii. E-bill payment	d. Online facilities to employees to leave	iv. Type of e-commerce business model	e. Brokerage	v. Future to EDI		vi. G2G		vii. Paper-less exchange of information		viii. G2C	5	CO1
a. iPaaS	i. G2E																		
b. M-commerce	ii. Type of e-commerce business model																		
c. EDI	iii. E-bill payment																		
d. Online facilities to employees to leave	iv. Type of e-commerce business model																		
e. Brokerage	v. Future to EDI																		
	vi. G2G																		
	vii. Paper-less exchange of information																		
	viii. G2C																		
3.	<p><u>Fill in the blanks by choosing words from options:</u></p> <p>The measure that is used in biometrics to measure similarity or dissimilarity is _____ distance measure. Two identical bit strings have distance of _____; two entirely dissimilar ones have a distance of _____.</p> <p>Interestingly, different biometrics measures have different parameters of similarity measurement—while for _____ uniqueness is based on ridges and furrows, for _____ it is based on nodal points.</p> <p>Options: Euclidean/ Hamming/ Humming/ Manhattan/ one/ zero/ iris scan/ retina scan/ face scan/ fingerprint/ palm scan</p>	5	CO2																
4.	<p><u>Fill in the blanks by choosing words from options:</u></p> <p>TCP is a _____, _____, _____ service. On the other hand, IP is _____ and _____. In case of _____, for each packet received, an acknowledgement is sent to the sender to confirm the delivery.</p>	5	CO4																

	Options: Connectionless, connection-oriented, reliable, unreliable, bit-stream, byte-stream, TCP, IP		
5.	True/False (With explanation. If false why and if true then say what it means. No marks without explanation) Mobile Wallet or E-wallet are not traceable	5	CO2
6.	True/False (With explanation. If false why and if true then say what it means. No marks without explanation) Retina scan is better than Iris scan for security purpose.	5	CO1
SECTION B			
1. Each question will carry 10 marks 2. Instruction: Any answer to the question should not exceed 350 words. Mention assumptions clearly if you are taking one 3. Write point-wise. No marks if written in long paragraphs or if the handwriting is illegible			
7.	Short notes: a) What is the difference between symmetric and asymmetric algorithm in cryptography with illustration? (4) b) Briefly explain the components of Rjindael algorithm. (6)	10	CO3
8.	Discuss the following: a) Types of EDI with brief details (6 Marks) b) Electronic Data Interchange v/s E-commerce (4 Marks)	10	CO1
9.	a) What are the layers in OSI? Describe each layer briefly. b) What is a protocol? Explain the key elements of a protocol. (6+4 Marks)	10	CO2
10.	Short notes on the following: (5 + 5 Marks) a) Types of Software Agents based on their Characteristics or functionality b) Benefits of using Software Agents	10	CO4
11.	Explain the two major parts of SET protocol briefly. Diagram is required for clarity in explanation. (6 Marks for explanation, 4 marks for diagram)	10	CO2

SECTION C			
	<p>1. Each question will carry 20 marks</p> <p>2. Instruction: Write long answer (800 words maximum)</p>		
12.	<p><u>EBay:</u></p> <p>Somewhere in the beginning of March 2014, the C2C giant had noticed an unsolicited database session in their main servers, scanning password files. It was later officially announced that an undisclosed slice of the +120 million users have been compromised for credentials and personal information.</p> <p>How did they get there? Well, e-Bay themselves acknowledged that one of their own has succumbed to a behavioral engineering trick, where the attacker would ask the password from someone who knows it, either pretending to be the original site or another, completely irrelevant, site but relying on the fact that most of us use the same password everywhere. The goal of the perpetrators was to obtain e-Bay staff credentials and with that, to access their database and steal user personal information. From there, they could either collapse the entire e-Bay operation, by using the commandeered user accounts to wreak havoc in the site.</p> <p>E-bay neglected two crucial security principals:</p> <ol style="list-style-type: none"> a. Staff cannot log in unless they know the password but they are also in possession of a physical device such as asymmetric public key generator or a USB key. b. Had the staff been made aware of the trickery, they would most likely never use a common password and they would have been aware of what a legitimate e-Bay page is and what is not. <p><u>PayPro:</u></p> <p>Online retailers share many risks with physical shops: people who want to walk out with the goods without paying, vandals breaking the shop's windows and other malevolent entities. However there is one crime that is the equivalent of a horde of deadbeats filling the shop to the brim, occupying all the staff, each unwelcomed customer holding on to some item on sale, not leaving anything for real customers to inspect but also not actually buying it.</p> <p>Even worse: imagine prospective customers walking by, noticing the store is jam-packed and deciding they would simply not stand in the queue there, but rather shop somewhere less populated.</p> <p>Goal of such attack can be: Ideological, Distraction or Extortion. However, it can be solved.</p> <p><u>Sony:</u></p> <p>Sony was accused of playing with people's credit card. 77 Million user accounts with personal information and 12 Million unencrypted credit card numbers were exposed. From simple SQL injections, where the developer left a field for an attacker to exploit,</p>	20	CO3

by entering live code into it and executing queries and commands on the website through it, to highly sophisticated hacks, such attacks may seem to happen from rookie mistakes but perfect knowledge exists only in retrospective. On one side, the online entrepreneur wants a website to bring the world together, no matter the platform, country, time and language, on the other, one that is sealed to any intrusions.

Some industry best practices include:

1. Data security
2. System alerts and system updates.

Question: From the above excerpts, recognize the type of attack (mention the types like DOS, Trojan Horse, Man-in-the-middle or phishing), that is discussed and provide their solution for:

- a. E-Bay (7 Marks)
- b. PayPro (6 Marks)
- c. Sony (7 Marks)