ELIZADE UNIVERSITY, ILARA-MOKIN, ONDO STATE
FACULTY OF ENGINEERING
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

FIRST SEMESTER EXAMINATION, 2017/2018 ACADEMIC SESSION

COURSE TITLE: Computer Security Techniques

COURSE CODE: ECT523

EXAMINATION DATE: 29th March 2018

COURSE LECTURER: Dr. B. S. Afolabi

HOD's SIGNATURE

TIME ALLOWED: 2½ HOURS

INSTRUCTIONS:

1. ANSWER **ANY FOUR QUESTIONS ONLY**
2. SEVERE PENALTIES APPLY FOR MISCONDUCT, CHEATING, POSSESSION OF UNAUTHORIZED MATERIALS DURING EXAM.
3. YOU ARE **NOT** ALLOWED TO BORROW ANY WRITING MATERIALS DURING THE EXAMINATION.

Question #1

a. In a SQL injection attack, attacker-controlled input is evaluated in the context of a SQL query, resulting in malicious SQL statements executing over sensitive data. Ur/Web allows web applications to directly embed SQL queries in a page; furthermore, those queries may contain information that originates from the user or an untrusted source. Why is this safe in Ur/Web? [6 marks]

b. Why do Computer attacks happen? [5 marks]

c. In which way(s) information security is/are more difficult than physical security? [6 marks]

d. Discuss Three main security goals [3 marks]

Question #2

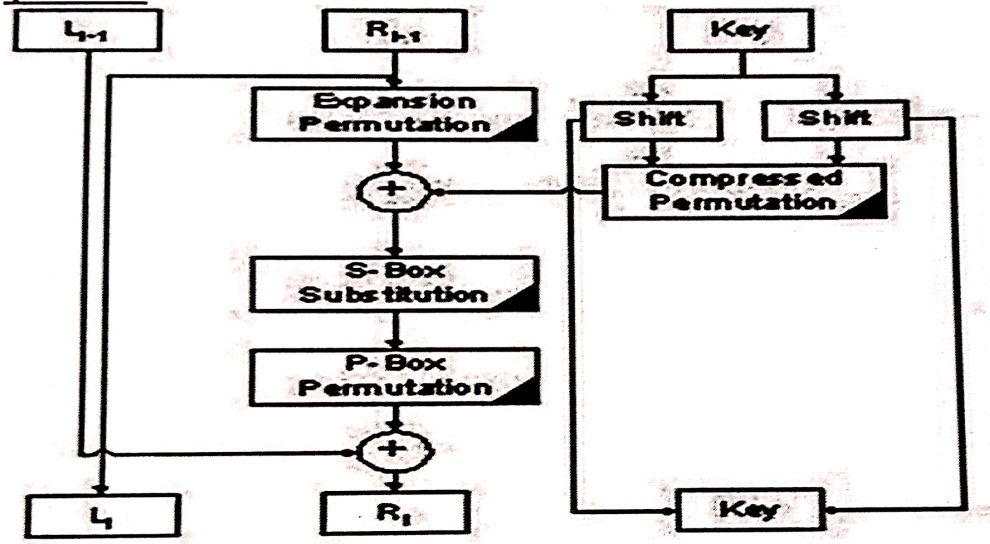
a) Differentiate between Steganography and Cryptography [3 marks]

b) Explain the differences between vulnerabilities and threats [3 marks]

c) What are the drawbacks of DES that motivated the development of AES? Be very specific in your answer. [9 marks]

d) How can one successfully achieve security goals? [5 marks]

Question #3



DES is a product cipher. The above diagram shows a single round of a DES variant (note that the key is not passed through a permuted choice function as in traditional DES) and this variant must be used to answer all the questions related to DES below.

a) For each of the blocks in the diagram, show the width of the various boxes (no. of bits). You can mark it in the diagram if you like. State which elements of the above DES round add confusion and which elements add diffusion? In this DES, how many times the idea of product cipher is used? [8 marks]

b) What is the resulting ciphertext when plaintext "ABCDEFGH" is encrypted twice with DES with the same key 0000000FFFFFFF? [4 marks]

c) Does a substitution need to be a permutation of the plaintext symbols? Why or why not? [4 marks]

d) If you are asked to design a new DES to use a 64-bit key, how would you do it? [4 marks]

Question #4

a) The Rijndael algorithm uses a byte substitution table that comes from a formula applied to $GF(2^8)$. Is it necessary to use that formula? That is, would any substitution table work? What restrictions are there on the form of the table? [5 marks]

b) A property of the Rijndael algorithm is that it is quite regular. Why is this both a good and bad property for a cryptographic algorithm? [3 marks]

c) Suppose that you are the Chief Security Officer (CSO) of Konga or Jumia. You are given a choice of AES and triple DES to secure data for your clients. Which one you would use and why? [6 marks]

d) Why should operating system and user processes need to have different privileges? [6 marks]

Question #5

a) Describe the most important considerations in Password Systems. [6 marks]

b) What would you consider as threats to usage of passwords? [6 marks]

c) Suppose that a user visits a mashup web page that simultaneously displays a user's favorite email site, ecommerce site, and banking site. Assume that:

- The email, ecommerce, and banking sites allow themselves to be placed in iframes (e.g., they don't prevent this using X-Frame-Options headers).
- Each of those three sites is loaded in a separate iframe that is created by the parent mashup frame.
- Each site (email, ecommerce, banking, and mashup parent) come from a different origin with respect to the same origin policy. Thus, frames cannot directly tamper with each other's state.

Describe an attack that the mashup frame can launch to steal sensitive user inputs from the email, ecommerce, or banking site. [8 marks]

Question #6

a) Modern CPUs often support NX ("no execute") bits for memory pages. If a page has its NX bit set to 1, then the CPU will not run code that resides in that page. NX bits are currently enforced by the OS and the paging hardware. However, imagine that programs execute on a machine whose OS and paging hardware do not natively support NX. Further imagine that a compiler wishes to implement NX at the software level. The compiler associates a software-manipulated NX bit with each memory page, placing it at the bottom (i.e., the lowest address) of each 4KB page. The compiler requires that all application-level data structures be at most 4095 bytes large. The compiler allocates each stack frame in a separate page, and requires that a stack frame is never bigger than a page. A stack frame might look like the following:

```
                        ...
              |----------------------|
              |                      |
              +----------------------+
entry %esp--> |    return address    |
              +----------------------+
new %ebp----> |    saved %ebp        |
              +----------------------+
              |    buf[4]            |
              |    buf[3]            |
              |    buf[1]            |
              |    buf[0]            |
              +----------------------+
              | ...other stack vars...|
              +----------------------+
new %esp----> |      NX bit          |
              +----------------------+
```

such that, as shown in the sample code above, an overflow attack in the frame will not overwrite the frame's NX bit. The compiler also associates NX bits with each normal code page. The NX bit for a stack frame is set to "non-executable", and the NX bit for a normal code page is set to "executable". The compiler instruments updates to the program counter such that, whenever the PC migrates to a new page, the program checks the NX bit for the page. If the bit indicates that the page is non-executable, the program throws an exception.

Describe how a buffer overflow attack can still overwrite NX bits. [7 marks]

b) Identify the various possible means of preventing Buffer Overflow Attacks [5 marks]

c) What is Buffer Overflow? [3 marks]

d) List common software vulnerabilities [5 marks]