UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE: **IT00047/IT00298/IT08X47/IT8X298**
INFORMATION SECURITY

CAMPUS: **APK**

SSA EXAM: **JULY 2016 - SSA**

DATE July 2016	**SESSION** 08:30 – 10:30
INTERNAL EXAMINER	Mr. J du Toit
EXTERNAL EXAMINER	Prof M Loock
DURATION 2 Hours	**MARKS** 100

Please read the following instructions carefully:

1. Write clearly and legibly.
2. Answer all questions.
3. Answer Section A and Section B in **separate** answer books
4. This paper consists of 4 pages

SECTION A

QUESTION 1 [28]

Kerberos is a term used in Information Security to describe an authentication and authorisation protocol. During the course Kerberos was explained using five high level steps.

Step 1 broadly describes how a fictional user, Sally, is authenticated and given a ticket granting ticket.

Step 2 describes how Sally requests access to a service by sending a request to the Ticket Granting Server.

Step 3 describes how the Ticket Granting Server authorises the request and generates an Electronic Ticket destined for Sally.

Step 4 describes how Sally receives the Electronic Ticket from the Ticket Granting Server and constructs a service request message to the application server.

Step 5 describes how the application server receives the service request, authorises the request and creates a session key that is used by the application server and Sally to securely communicate in the future.

Describe, by using an **example**, what happens in **Step 1** and **Step 2**. Note: It is not necessary to describe steps 3 to 5.

Please use diagrams to describe the content of the various packets and tickets. Please use the following acronyms in your examples:

Authentication Server (**AS**)
Application Server (**APS**)
Ticket Granting Sever (**TGS**)
Ticket Granting Ticket(**TGT**)
Electronic Ticket (**ET**)
Symmetric Key **Ki** where **i** is the number of the symmetric key

QUESTION 2 [22]

According to the study material provided, Information Security is based on 5 Security Services, each supported by a number of technologies.

Discuss 2 (two) of these services using the following structure: (11 x 2)

1. Service name (1)
2. A brief discussion of the service (3)
3. A brief discussion of the supporting technologies (3)
4. A detailed discussion of how and where the service and supporting technologies are used in a typical Internet banking system (4)

Ensure the above structure is followed per service to ensure maximum marks.

TOTAL SECTION A [50]

SECTION B

QUESTION 1 **[12]**

The Advanced Encryption Standard (AES) replaced DES as an encryption standard. The AES encryption algorithm executes in a number of rounds. Different steps are performed in each of these rounds. These steps are normally categorised into specific categories that names basically what happens in that category. Name or describe the category of steps that happen in each round: (12)

- Initial Round (2)
- Intermediate rounds (7)
- Last Round (3)

QUESTION 2 **[15]**

2.1 Biba defined a model in 1977 that assists data integrity. Describe how the model works. Please use a diagram to assist in explaining the model. (8)

2.2 The versions of Microsoft Windows from Microsoft Vista and later implements an integrity model call Mandatory Integrity Control, based on the model described by Biba. Describe how the model works by concentrating on the following aspects: (7)

- The integrity levels of the operating system
- The default integrity levels of the various objects and subjects

QUESTION 3 **[15]**

3.1 Describe the steps that are necessary when a person or system requires a digital identity (certificate) from a certificate authority (8)

3.2 **Statement**: RSA encryption uses very big prime numbers. RSA encryption is typically used to directly encrypt large amounts of data. (7)

State if you **agree** or **disagree** with the above statement.
Describe why you agree or disagree with the statement using **processing power** and the **lifetime of keys** as a basis for your argument.

QUESTION 4 **[8]**

4.1	Name two well-known hashing algorithms	(2)
4.2	What can be done to increase the strength of hashed passwords?	(1)
4.3	What type of symmetric cipher is a one-time pad?	(1)
4.4	In this course you learned about two modes of symmetric encryption. These two modes relate to how symmetric encryption handles large amounts of data. Name the two modes of operation.	(2)
4.5	Name any two of the ten rules that are described by the IEEE Center for Secure Design that must be followed in order to design secure software	(2)

TOTAL SECTION B **[50]**

TOTAL PAPER **[100]**