UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

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

CAMPUS: **APK**

EXAM: **MAY 2016**

DATE	24 MAY 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 **[37]**

The ministry of communication of Utopia have recently heard that the owners of the famous instant messaging application, WhatsAppDoc, implemented full encryption in their application's communications. The owners of WhatsAppDoc stated that the communication of the application uses asymmetric encryption with message digests to sign messages for non-repudiation purposes and symmetric encryption to encrypt and keep messages secure.

The minister of communications approached you to please write a memo to explain to the government what this all means. Please structure your memo using applicable headings and use diagrams wherever possible to describe concepts. Ensure to cover points a – e in your discussion.

a) Start the memo by describing the fundamental concepts of symmetric encryption and asymmetric encryption, by focussing on the **number** of keys that is used in both instances.

b) Describe the advantages and disadvantages of symmetric key encryption.

c) Describe the advantages and disadvantages of asymmetric encryption.

d) Describe by using an example and a diagram how public\private key encryption is used to ensure non-repudiation of messages. Include in your discussion the importance of message digests \ hashing, to help assure non-repudiation.

e) Describe by using an example and a diagram how public\private key encryption solves the problem of key distribution in symmetric key encryption and how WhatsAppDoc can use symmetric key encryption to ensure confidentiality. (It is not necessary to include in your discussion the infrastructure that is necessary to ensure the integrity of public keys. We assume the owners of WhatsAppDoc can assure the integrity of public keys).

Marks will be awarded for:

i) Mark allocation for the points above:
   a. **6** marks
   b. **5** marks
   c. **5** marks
   d. **10** marks
   e. **8** marks
   f. Presentation
      i. Clarity and neatness
      ii. Comprehensiveness of your answer based on the content covered in the course
      iii. Readability
      iv. Logical structure – **3** marks

QUESTION 2 **[13]**

2.1 Describe the various aspects of Cobit 5. In your discussion, ensure to discuss why Cobit can be used for Information Security. (10)

2.2 What is ISO 27001 and is it used for? (3)

TOTAL SECTION A **[50]**

SECTION B

QUESTION 1 **[15]**

1.1 You have been employed as the manager in the software integration and development department of the Utopian electricity supplier called, ElecKom. You would like to ensure your development team avoids the top 10 software security design flaws as documented by the IEEE Center for Secure Design. Briefly list and describe five different design flaws that software developers should avoid. (15)

QUESTION 2 **[12]**

The independent country of Utopia has been establishing a national defence force, called the Utopian National Defence Force (UNDF). The national defence force's data in their information technology system needs to ensure only authorised people can get access to specific data. The defence force is used to **classify** information and people and does **not** allow owners of information to control access to the information

2.1 What authorisation policy would you recommend for the UNDF? (2)
2.2 Discuss the authorisation model that supports the authorisation policy you would implement for UNDF? (10)

QUESTION 3 **[15]**

The information security course described three different hardware attacks that consumer's computers are exposed to. List and describe each of these attacks as well as the steps that can be taken to minimise the risk of the specific attack

QUESTION 4 **[8]**

Your manager read in an article that encryption can be accomplished using **symmetric** encryption. Your manager would like to implement symmetric encryption to ensure **non-repudiation**. Using your knowledge about symmetric encryption discuss the **two** types of symmetric encryption that can be categorised according to the **number** of **keys** they use. For each category state if the category can be used to ensure non-repudiation

TOTAL SECTION B **[50]**

TOTAL PAPER **[100]**