

**JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY**  
**SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS**  
**DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING**  
**UNIVERSITY EXAMINATION FOR THE DEGREE OF MASTERS OF IT SECURITY**  
**AND AUDIT**  
**1<sup>ST</sup> YEAR 2<sup>ND</sup> SEMESTER 2019/2020 ACADEMIC YEAR**  
**KISUMU CAMPUS**

---

**COURSE CODE: IIT 5121**

**COURSE TITLE: ADVANCED CRYPTOGRAPHY AND CYBERSECURITY**

**EXAM VENUE: STREAM: IT SECURITY AND AUDIT**

**DATE: 9/12/19 EXAM SESSION: 9.00 – 12.00NOON**

**TIME: 3.00 HOURS**

---

**INSTRUCTIONS**

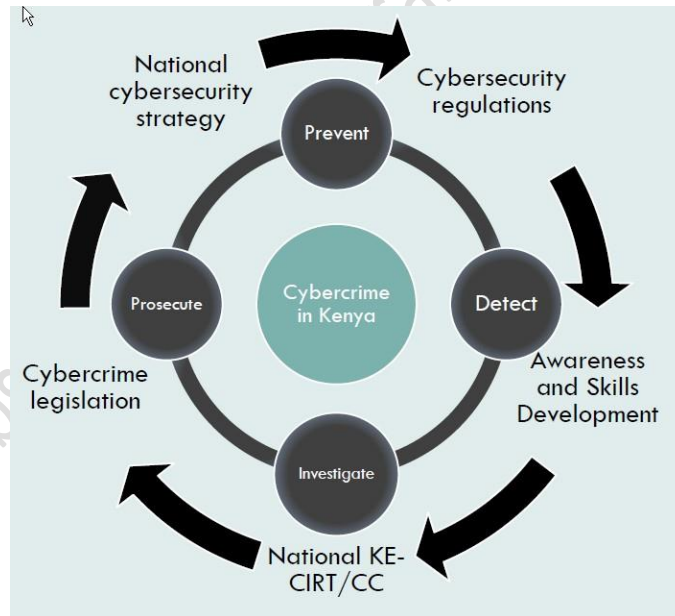
- 1. Answer ANY THREE questions**
- 2. Candidates are advised not to write on the question paper**
- 3. Candidates must hand in their answer booklets to the invigilator while in the examination room**

**Question 1 [20 marks]**

- a) Using a diagram briefly discuss the historical development of the cyber-warfare (10 marks)
  
- b) Briefly discuss the following major cyber-warfare cases. Your discussion should include the elements of the mode of attack and the impact of the attack on the country (20 marks)
  - i) Stuxnet
  - ii) Estonian Government
  - iii) 2016 US Elections
  - iv) Ukrainian Power Grid

**Question 2 [20 marks]**

- a) Effective cybercrime prevention requires a concerted effort from understanding the threat landscape, develop good investigative techniques (IT security and Forensics), involvement of administrative authorities (Government/management), address legal and regulatory issues, involve legislative arms of the government and develop a national cybercrime strategy as depicted in the figure below.



- Briefly discuss at least five common techniques used by attackers and the motivations behind such attacks. (5 marks)

- b) What is National KE-CIRT/CC? Discuss the role this organization plays in Cybersecurity and cybercrime prevention in Kenya. **(10 marks)**
- c) Discuss the phases of cybersecurity warfare **(5 marks)**

**Question 3 [20 marks]**

- a) Explain the differences between symmetric and asymmetric encryption. **(5 marks)**
- b) Differentiate between stream and block ciphers. **(5 marks)**
- c) Identify both the advantages and disadvantages of:
- i) Stream Ciphers
  - ii) Block Ciphers. **(6 marks)**
- d) Discuss any four characteristics of a good cipher? **(4 marks)**

**Question 4 [20 marks]**

- a) The Serianu Cybersecurity reports provide a landscape of the cyber related activities in Kenya in 2016, 2017 and 2018. Discuss at least three differences and three similarities between these three reports in reference to the trend of cyber activities. **(15 marks)**
- b) In Cybersecurity, we should think about resilience in terms of systems and organizations. The general idea behind resilience is to adapt to adverse conditions and recover. Discuss the three elements behind resilience. **(5 marks)**

**Question 5 [20 marks]**

- a) Using a diagram discuss the concept of PKI. Your discussion MUST include CA, certificate exchange, encryption and hashing scheme **(10 marks)**
- b) Explain the algorithm behind RSA encryption scheme **(10 marks)**