JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR SCIENCE IN COMPUTER SECURITY AND FORENSICS

1ST YEAR 2ND SEMESTER 2024/2025 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: ICB 1106

COURSE TITLE: CIRCUIT THEORY AND BASIC ELECTRONICS

EXAM VENUE: LAB 7 **STREAM: BSC COMP. SECURITY**

DATE: 22/4/2025 **EXAM SESSION: 9.00-11.00**

TIME: 2.00 HOURS

INSTRUCTIONS:

1. **Answer Question 1 (Compulsory) and ANY other two 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**

JOOUST OBSERVES ZERO TOLERANCE TO EXAM CHEATING

QUESTION ONE **[30 MARKS]**

(a) A forensic investigator needs to determine whether a suspect's IoT device was in use during a specific time frame. Explain how measuring electrical charge and current consumption patterns can help establish digital evidence in a cybercrime investigation. [4 Marks]

(b) A government cybersecurity agency is analyzing a suspected malware attack on a power grid. Attackers have manipulated electrical pathways to cause abnormal voltage fluctuations. Explain which method (nodal or mesh analysis) would best help in identifying the cause. [3 Marks]

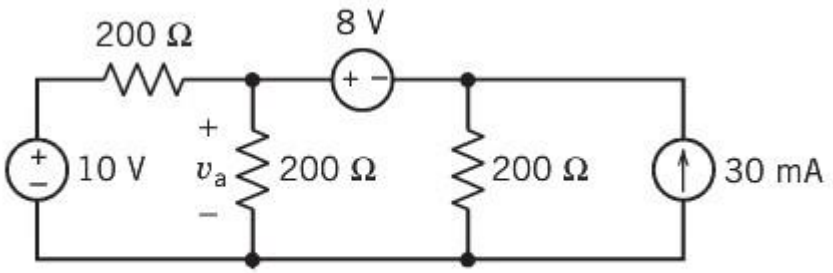
(c) A malicious hardware implant is secretly consuming power inside a secure facility's computer system. How can Kirchhoff's Current Law (KCL) help security experts detect its presence? [3 Marks]

(d) Determine the voltage v_a in the circuit below by using

(i) Nodal analysis [3 Marks]

(ii) Mesh analysis [3 Marks]

(iii) Thevenin's and Norton's theorem. [6 Marks]



(j) A covert listening device is embedded in an office wall and uses an Op-Amp-based audio amplifier to boost captured conversations. Explain how a forensic investigator can analyze and disable the device using circuit theory. [4 Marks]

(k) During an investigation, a suspect's USB drive is found to have a modification in its diode circuitry that leaks encryption keys via power variations. Explain how a forensic expert can confirm and analyze this security breach. [4 Marks]

QUESTION TWO **[20 MARKS]**

(a) A security researcher discovers that a hacker is using power analysis attacks to extract cryptographic keys from a secure device.

(i) Explain how analyzing *charge*, *current*, and *voltage* variations can reveal sensitive data. [6 Marks]

(ii) Explain the countermeasures that can be implemented to prevent such attacks. [6 Marks]

(b) A hacker attempts to bypass a smart home's security system by *injecting an electrical pulse* to manipulate its sensors. Using Ohm's and Kirchhoff's Laws, explain how a forensic analyst can reconstruct the event and identify system vulnerabilities. [8 Marks]

QUESTION THREE **[20 MARKS]**

(a) A forensic team is reverse-engineering an embedded security chip suspected of leaking sensitive data. Using *Thevenin's* and *Norton's Theorems*, explain how the chip's internal behavior can be modeled to reveal its weaknesses. [8 Marks]

(b) A cybercriminal is suspected of using malicious firmware to alter the power signatures of security cameras. Explain how *Laplace Transforms* can help analyze the circuit's transient response and detect unauthorized modifications. [6 Marks]

(c) A hacker is extracting encryption keys from IoT security cameras by analyzing their power consumption patterns. Explain how the *Maximum Power Transfer Theorem* applies to side-channel attacks and how forensic investigators can counteract them. [6 Marks]

QUESTION FOUR **[20 MARKS]**

(a) A forensic analyst suspects that an attacker is exploiting diode behavior in a smart card to leak information. Explain how special-purpose diodes can be used to mitigate side-channel attacks. [6 Marks]

(b) A malware-infected microcontroller has been programmed to modify the behavior of transistor-based amplifiers in a secured system. Explain how forensic analysts can trace the anomalies and reconstruct the attack. [8 Marks]

(c) A cybersecurity expert finds counterfeit diodes in critical security hardware. Discuss how a diode behavior analysis can help forensic teams identify and mitigate risks associated with counterfeit components. [6 Marks]

QUESTION FIVE **[20 MARKS]**

(a) A forensic team is investigating a secure voice communication system suspected of being tampered with. Explain how Op-Amp integrators and differentiators can be analyzed to detect unauthorized signal alterations. [6 Marks]

(b) A malicious actor has altered an ATM's Op-Amp-based sensor to approve unauthorized transactions. Explain how forensic analysis of Op-Amp circuits helps in detecting and reversing fraud. [8 Marks]

JOOUST OBSERVES ZERO TOLERANCE TO EXAM CHEATING

(c) A malware-infected skimmer installed in ATMs uses Op-Amp-based signal amplification to capture card data. Explain how forensic analysis of Op-Amp circuits can reveal the attack's mechanism. [6 Marks]

- **END –**

JOOUST OBSERVES ZERO TOLERANCE TO EXAM CHEATING