MAKERERE UNIVERSITY
DEPARTMENT Of COMPUTER SCIENCE

Name: **Azamuke Denish** Assignment Number: **1**
Course: **Demo Template for Msc. CS** Date: April 25, 2021

Problem 1

Given that **Airqo**, *Africa's leading air quality monitoring, research and analytics network company* has used its public RSA key (n, e) for years. After a security check they had to change it to (n, e'), with the same n but with a different number e' which is relatively prime to e. A customer had previously sent his message $\overline{a}$ which was encoded with the old key. After he got the news of the security check he encodes this same message $\overline{a}$ with the new public key.
How can an attacker get $\overline{a}$ from the knowledge of the old and new encrypted message $\overline{c_1}$ and $\overline{c_2}$ respectively using only the public keys? You are required to evaluate this for the example where $n = 247, e = 11, e' = 17, c_1 = 24, c_2 = 93$.

References

[1] Bitter, R., Mohiuddin, T., & Nawrocki, M. (2017). LabVIEW: *Advanced programming techniques.* CRC press.