**PROGRAMME: DIPLOMA IN INFORMATION & COMMUNICATION TECHNOLOGY**
**SCHOOL: SCIENCE ENGINEERING AND HEALTH**
**ACS 332/MIS 412 Computer Systems Security**

**Semester: September 2024**
**Lecturer: Harriet Ratemo**
**Day:** November 2024

---

**Instructions**: Attempt all Questions
**NOTE: Please submit physical copies**

## TAKE AWAY CAT 1 (50 Marks)

1. Using the theorem divisibility, prove the following
   a) If a|b , then a|bc $\forall a, b, c \in \mathbb{Z}$ (5 marks)
   b) If a|b and b|c , then a|c (5 marks)
2. Using python, implement the Modular exponentiation algorithm (. Show the output code. (5 marks)
3. Let m be the gcd of 117 and 29. Find m using the Euclidean algorithm (5 marks)
4. Write a program in Python that implements the Euclidean Algorithm. Show your output (5 marks)
5. Modify the Euclidean Algorithm above such that it not only returns the gcd of a and b but also the Bezouts coefficients x and y, such that $ax + by = 1$ . Show output for your code. (10 marks)
6. Find the integers p and q, solution to $1171p + 89q = m$ (5 marks)
7. Determine whether the equation $486x + 222y = 6$ has a solution such that $x, y \in Z_p$ If yes, find x and y. If not, explain your answer. (5 marks)
8. Using Fermat's Little Theorem, compute $11^{345}\ mod\ 23$ (5 Marks)