Ahmedabad University

School of Arts and Sciences

CLCQCVZIPY VEQNCP ZRCAPY & SPYFZAMPIFRY (QIZ215)

Quiz 2, Date: 17 October 2025

Timing: 02:45 PM to 03:45 PM Monsoon 2025 Maximum points: 10

- **Question 1 is worth 0.5 point.**
- **Questions 2 and 3 are worth 1 point each.**
- **Questions 4, 5, and 6 are worth 2 points each.**
- **Questions 7 and 8 are worth 3 points each.**
- **Do at most questions totaling 10 points, anything above that will not be evaluated.**

1. A substitution cipher that permutes the 26 letters has a key space size 26!. Is this statement true or false?

2. Explain why the affine cipher $f_{a,b}(x) = ax+b \pmod{26}$ requires that $\gcd(a, 26) = 1$. What goes wrong if this condition is not met?

3. Suppose you use an affine cipher on the English alphabet (letters mapped to $0, 1, \ldots, 25$). The encryption function is $f_{a,b}(x) = ax + b \pmod{26}$ where $\gcd(a, 26) = 1$.

   (a) List all possible values of a.

   (b) If $a = 5$ and $b = 8$, encrypt the plaintext “HELLO”.

4. Show that if two affine ciphers (a, b) and (a', b') give the same mapping, i.e.

$$f_{a,b}(x) = ax + b \equiv a'x + b' \pmod{26} \quad \text{for all } x,$$

   then $a \equiv a' \pmod{26}$ and $b \equiv b' \pmod{26}$.

5. Given a substitution cipher, you intercept the ciphertext “XJQZ” and you also know that the plaintext is “GOOD.” Use this known plaintext–ciphertext pair to deduce the mapping for the four letters involved. Explain how this helps attack the rest of the cipher.

6. (a) What is the Vigenère cipher?

   (b) Use the Vigenère cipher with key “DOG” to encrypt the plaintext “ATTACKATDAWN.” (Use $A = 0, B = 1, \ldots, Z = 25$.)

   (c) Describe the Kasiski method for estimating the key length of a Vigenère cipher.

(d) A Vigenère ciphertext shows repeated trigrams "KDL" at distances of 12 and 18 letters apart. Use the *Kasiski method* to estimate the likely key length.

7. A cipher first applies a Caesar cipher with shift 3, then an affine cipher

$$f_{a,b}(x) = 5x + 8 \pmod{26}.$$

Write the combined encryption as a single affine function

$$f'_{a,b}(x) = a'x + b' \pmod{26},$$

and find a' and b'.

8. Explain why the existence of multiplicative inverses modulo n is directly related to Euler's φ function. Then, find all integers a with $1 \leq a \leq 12$ such that a has a modular inverse modulo 12.

9. **(Bonus)** Find the encryption system & function used for encrypting the course title at the top of the question paper.