# Quiz 1
(Deadline March 14, 2025)

## Problem 1

Please download `ciphertext.txt` from the new e3 platform.

A message has been encrypted, producing ciphertext characters with ASCII values ranging from 32 to 126.

**a)** (1 pt) Use frequency analysis to attempt to recover the original plaintext. Fill Table 1 below by mapping each ciphertext character to its corresponding plaintext character. **Include a snapshot of your filled table in your report.** (Leave an entry blank if there is no corresponding plaintext character.)

**Hint:** The plaintext spans a wide range of ASCII characters (32–126), including lowercase letters, uppercase letters, punctuation, and whitespace.
**Hint:** Refer to the frequency count information in Table 2 to guide your analysis.

Table 1: Ciphertext-to-plaintext mapping (ASCII 32–126)

| **Ciphertext** | (space) | ! | " | # | $ | % | & | ' | ( | ) | * | + | , | - | . |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ASCII** | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 |
| **Plaintext** | | | | | | | | | | | | | | | |
| **Ciphertext** | / | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | : | ; | < | = |
| **ASCII** | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 |
| **Plaintext** | | | | | | | | | | | | | | | |
| **Ciphertext** | > | ? | @ | A | B | C | D | E | F | G | H | I | J | K | L |
| **ASCII** | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 | 76 |
| **Plaintext** | | | | | | | | | | | | | | | |
| **Ciphertext** | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | [ |
| **ASCII** | 77 | 78 | 79 | 80 | 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 | 91 |
| **Plaintext** | | | | | | | | | | | | | | | |
| **Ciphertext** | \ | ] | ^ | _ | ` | a | b | c | d | e | f | g | h | i | j |
| **ASCII** | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 | 101 | 102 | 103 | 104 | 105 | 106 |
| **Plaintext** | | | | | | | | | | | | | | | |
| **Ciphertext** | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y |
| **ASCII** | 107 | 108 | 109 | 110 | 111 | 112 | 113 | 114 | 115 | 116 | 117 | 118 | 119 | 120 | 121 |
| **Plaintext** | | | | | | | | | | | | | | | |
| **Ciphertext** | z | { | \| | } | ~ | | | | | | | | | | |
| **ASCII** | 122 | 123 | 124 | 125 | 126 | | | | | | | | | | |
| **Plaintext** | | | | | | | | | | | | | | | |

Table 2: Typical letter frequency (%) in English

| E | A | R | I | O | T | N | S | L | C | U | D | P |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 11.16 | 8.5 | 7.58 | 7.54 | 7.16 | 6.95 | 6.65 | 5.74 | 5.49 | 4.54 | 3.63 | 3.38 | 3.17 |
| M | H | G | B | F | Y | W | K | V | X | Z | J | Q |
| 3.01 | 3.0 | 2.47 | 2.07 | 1.81 | 1.78 | 1.29 | 1.10 | 1.01 | 0.29 | 0.27 | 0.20 | 0.20 |

**b)** (1 pt) Assume the encryption uses the affine transformation

$$y = (ax + b) \mod 95 + 32,$$

where $y$ is the ciphertext and $x$ is the plaintext (both in the ASCII range). Determine the values of $a$ and $b$.

**c)** (1 pt) An attacker discovers that the plaintext contains the word `created`. How could this known plaintext be used to break the encryption? What is the name of the technique involved?

**d)** (1 pt) What is the size of the key space for this affine cipher on ASCII characters from 32 to 126? Why does this method provide relatively weak security?

**e)** (1 pt) Next, consider a Monoalphabetic Substitution Cipher over ASCII characters from 32 to 126. What is the size of its key space, and how does this size affect the feasibility of a brute-force attack in terms of computational limits?

**f)** (Bonus 1 pt) Propose an enhanced encryption method that is more resilient against frequency analysis. Your design should:

1. Include at least two transformation steps (e.g., affine plus a bitwise operation).
2. Make frequency-based attacks more difficult.
3. Remain fully reversible to allow for accurate decryption.

In your response, explain how your design meets each of these three criteria.

## Problem 2

The plaintext is encrypted via an affine cipher over $\mathbb{Z}_n$ where $n$ is a prime number satisfying

$$30 < n < 100.$$

The encryption is given by

$$y = ax + b \mod n,$$

with $y$ the ciphertext and $k_{\text{enc}} = (a, b)$ the encryption key.

**a)** (1 pt) For a given $n$, compute the size of the key space by determining:

1. The number of valid $a$ values.
2. The number of possible $b$ values.
3. The total number of possible keys.

Please use standard Discrete Mathematics functions to represent your answer.

**b)** (1 pt) List all elements in $\mathbb{Z}_{30}$ that have multiplicative inverses, and identify those inverses.

**c)** (1 pt) An attacker intercepts the following plaintext-ciphertext pairs.

| Plaintext $x$ | Ciphertext $y$ |
|---|---|
| 81 | 48 |
| 14 | 91 |
| 3 | 72 |

Determine the encryption key $k_{\text{enc}} = (a, b)$.

**d)** (1 pt) Find the decryption key $k_{\text{dec}} = (c, d)$ such that

$$x = cy + d \mod n.$$

**e)** (1 pt) After a recent attempted breach, Dr. Shieh changed the key $k_{\text{enc}} = (a, b)$ and the prime number modulus $n$ satisfying

$$30 < n < 100.$$

However, the attacker intercept a few plaintext-ciphertext pairs, albeit with some digits obscured. In the intercepted data, a missing digit is denoted by a "?" symbol.

| Plaintext $x$ | Ciphertext $y$ |
|---|---|
| 12 | 4? |
| ?3 | 72 |
| 45 | 23 |
| 2 | 39 |

Determine the encryption key $k_{\text{enc}} = (a, b)$.

## Submission Guidelines

1. Upload a **single PDF file** named `<student_id>.pdf` (where `<student_id>` is replaced by your actual student ID) to the new e3 platform.
2. Present your solutions in **numerical order**, clearly labeling each subproblem.

## Grading Policy

1. This quiz comprises 10 standard subproblems plus 1 bonus subproblem, for a total of up to 11 points (one point per subproblem).
2. **Late Submission Penalty:** A penalty of **0.5 points per day** will be applied for late submissions, up to a maximum of 20 days. Beyond 20 days, late submissions will be assigned zero.
3. All quizzes are **mandatory**. Failure to submit any quiz will result in an automatic failing grade for the course.