1) Probability and Statistics

1.1 Design an algorithm to simulate a discrete probability distribution using coin tosses. Illustrate it with an example simulating $\frac{1}{5}$ uniform probability distribution.

1.2 Come up with an algorithm to simulate a $\frac{1}{4}$ uniform distribution using the rolls of a standard six-sided die.

1.3 Compute the index of coincidence of the following string: "She sells seashells on the seashore". Compare this value with the index of coincidence of a random string of the English alphabet of the same length.

2) Modular Arithmetic

2.1 Given that $\gcd(32, 40) = 8$, express $8 = 32 \cdot x + 40 \cdot y$, where $x, y \in \mathbb{Z}$, show that the values of x, y are not unique by producing another pair $x', y' \in \mathbb{Z}$ such that $8 = 32 \cdot x' + 40 \cdot y'$. Comment on the time-complexity of the algorithm you used.

2.2 Compute 1/6 in $\mathbb{Z}_{17}$.

3) Historical Ciphers

3.1 We describe a Stream Cipher that is a modification of the Vigenère Cipher. Given a keyword $k_1, k_2, \ldots, k_m$ of length m, construct a keystream by the rule $z_i = k_i (1 \leq i \leq m)$, $z_{i+m} = (z_i + 1) \bmod 26 (i \geq 1)$. In other words, each time we use the keyword, we replace each letter by its successor modulo 26.

For example, if SUMMER is the keyword, we use SUMMER to encrypt the first six letters, we use TVNNFS for the next six letters, and so on.

- Describe how you can use the concept of the index of coincidence to first determine the length of the keyword, and then actually find the keyword.
- Test your method by cryptanalyzing the following ciphertext.:

```
JEJNGNXZWHHGWFSUKULJQACZKKJOAAHGKEMTAFGMKVRDO
PXNEHEKZNKFSKIFRQVHHOVXINPHMRTJPYWQGJWPUUVKFP
OAWPMRKKQZWLQDYAZDRMLPBJKJOBWIWPSEPVVQMBCRYVC
RUZAAOUMBCHDAGDIEMSZFZHALIGKEMJJFPCIWKRMLMPIN
AYOFIREAOLDTHITDVRMSE
```

3.2 Suppose that π is the following permutation of $\{1, 2, \ldots, 8\}$:

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	1	6	2	7	3	8	5

- Compute the permutation π^{-1}.
- Decrypt the following ciphertext, for a Permutation Cipher with $m = 8$, which was encrypted using the key π:

```
TGEEMNELNNTDROEOAAHDOETCSHAEIRLM.
```