

This assignment was marked out of a total of 35.

1. Note that an affine cipher has a key $K = (a, b)$ where $a, b \in \mathbb{Z}_{26}$ and $\gcd(a, 26) = 1$, with encryption given by $e_K(x) = ax + b$.

(a) (1 mark) In \mathbb{Z}_{26} we have $k - x = 25x + k$. Thus since $\gcd(25, 26) = 1$, an inversion cipher is an affine cipher with key $K = (25, k)$.

(b) (2 marks) For $a, b, c \in \mathbb{Z}_{26}$, we have $a(x + c) + b = ax + (ac + b)$ and $ac + b \in \mathbb{Z}_{26}$. Moreover, we have $\gcd(a, 26) = 1$ as given in the question, so a two-step cipher is an affine cipher with key $K = (a, ac + b)$.

(c) (5 marks) Proposition: Applying a sequence of n affine cipher encryptions is equivalent to applying a single affine cipher encryption.

The proposition is certainly true for $n = 1$.

Assume that the proposition is true for $n = m$, and then use this to prove that it is true for $n = m + 1$. Suppose that applying m affine ciphers is equivalent to the single affine cipher with key $K = (a, b)$ where $a, b \in \mathbb{Z}_{26}$ and $\gcd(a, 26) = 1$. Consider applying the $(m + 1)^{\text{st}}$ affine cipher with key $K = (c, d)$ where $c, d \in \mathbb{Z}_{26}$ and $\gcd(c, 26) = 1$. Then the encryption of the plaintext character $x \in \mathbb{Z}_{26}$ would give

$$e(x) = c(ax + b) + d = acx + (cb + d).$$

Since $\gcd(a, 26) = \gcd(c, 26) = 1$ we have $\gcd(ac, 26) = 1$. Also $cb + d \in \mathbb{Z}_{26}$. Thus the effect of applying $m + 1$ affine ciphers is equivalent to one affine cipher with key $(ac, cb + d)$.

Thus the proposition is true for all integers $n \geq 1$.

- (2) (17 marks) Keys are attached. The explanation of the method is worth 15 marks. Decryption and finding the correct key (correct plaintext) is worth 2 marks. The solution should include:

- Calculation of the gcd of some of the distances between the beginnings of repeated substrings and the guess for the value of m based on the gcd.
- Calculations of the index of coincidence for m columns for at least one guess of the key length m .
- An estimate for the key length m based on the formula

$$m = \frac{0.027n}{(n-1)I_c - 0.038n + 0.065} \quad \text{or the approximation} \quad m = \frac{0.027}{I_c - 0.038}.$$

- A comment on any differences between the above three estimates for m and a deduction of the correct key length m .
- Applying the method of mutual index of coincidence to find the relative shift between each pair of columns. This should include the calculation of

$$\sum_{g=0}^{25} \frac{f_g f'_{g+s}}{n n'}$$

for at least one reasonable guess for s for at least $m - 1$ pairs of columns (probably columns $(0, 1), (0, 2), \dots, (0, m - 1)$).

- Deducing the keyword from the above information.

- (3) (a) (3 marks) Answers are attached.
(b) (3 marks) Answers are attached.
- (4) (a) (2 marks) Answers are attached.
(b) (2 marks) Answers are attached.