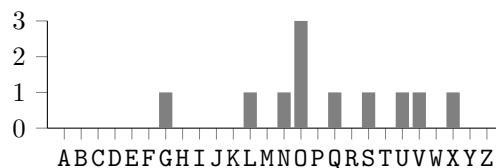


1. Here is the frequency of ciphertext symbols in an encryption of plaintext **abracadabra**:



(a) It is possible that the ciphertext was produced using the substitution cipher.

Solution: false. The plaintext is supported on the five letters **a, b, c, d, r**. If the substitution cipher was used the histogram would also have been supported on five symbols. Here there are nine.

(b) It is possible that the ciphertext was produced using the one-time pad.

Solution: true. It is possible that $m = \text{abracadabra}$ encrypts to, say, $c = \text{GLN000QSUVX}$. The one-time key would be the difference $c - m$ modulo 26.

2. This question is about the shift cipher. If you claim ciphertexts are distinguishable, describe a distinguisher.

(a) Encryptions of plaintexts **def** and **fed** are perfectly indistinguishable.

Solution: false. They are perfectly distinguishable. To distinguish, Eve checks that the ciphertext consists of three consecutive symbols like **XYZ**. This is always the case for encryptions of **def** but never for encryptions of **fed**.

(b) Encryptions of plaintexts **def** and **stu** are perfectly indistinguishable.

Solution: true. The p.m.f. of both encryptions is uniform over the 26 possible sequences of three consecutive symbols: **ABC** with probability $1/26$, **BCD** with probability $1/26$, up to **ZAB** with probability $1/26$.