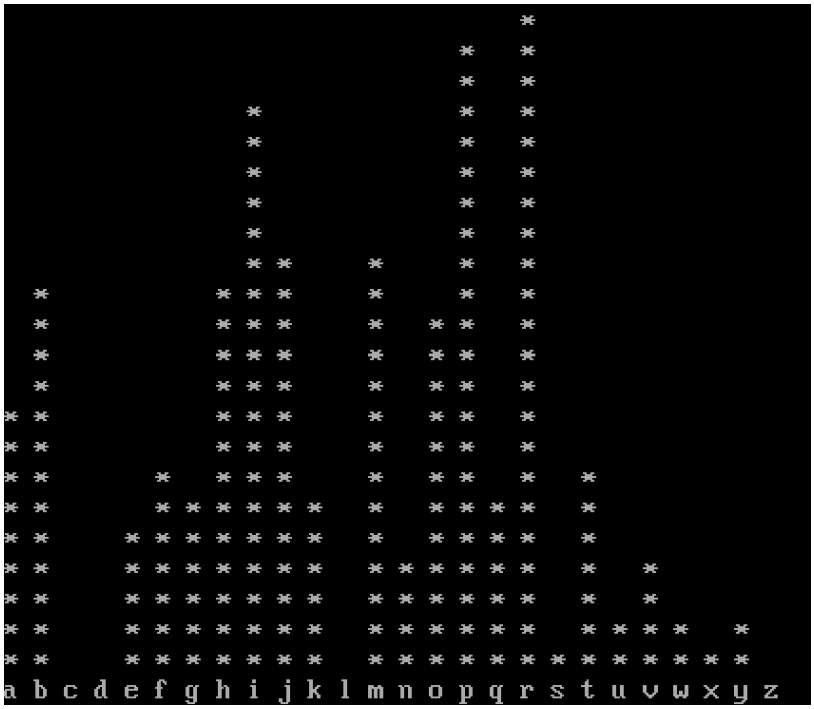
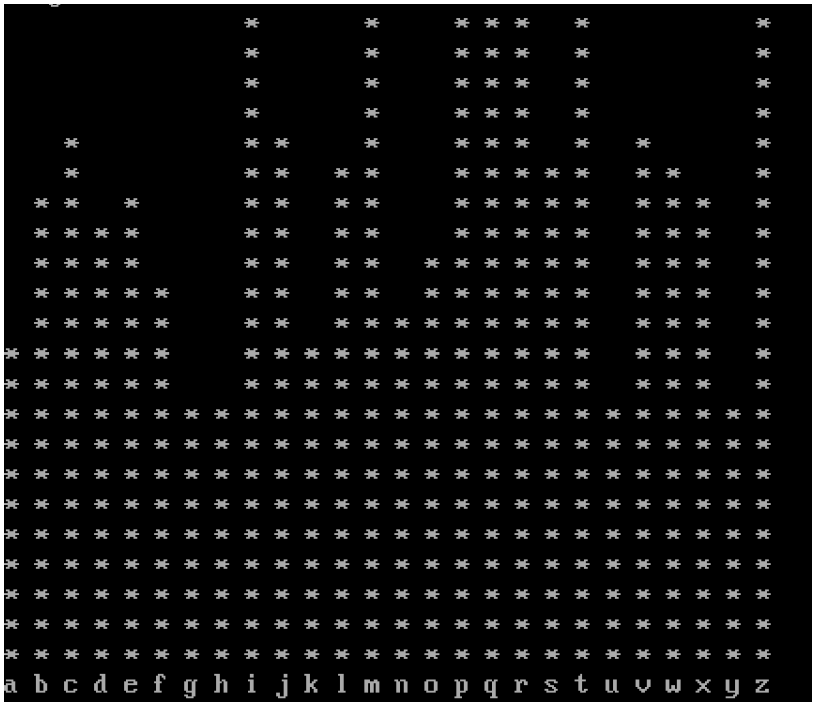
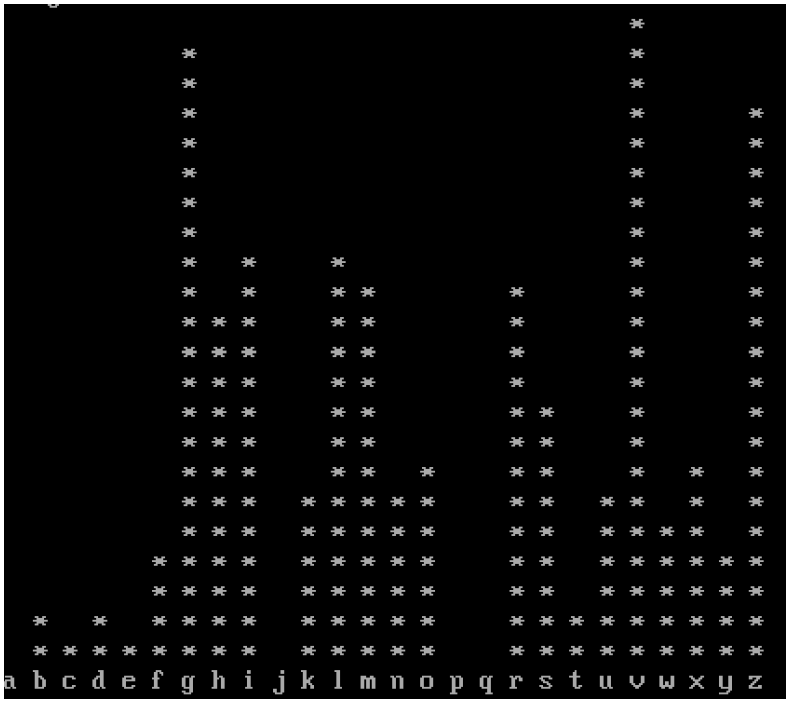


CText-1 frequency distribution graph



CText-2 frequency distribution graph



CText-3 frequency distribution graph

Discussion of statistical properties of Ctext-1, Ctext-2 and Ctext-3

From the frequency distribution graphs above, Ctext-1 and Ctext3 doesn't have a relatively flat frequency distribution while the frequency distribution graph of Ctext-2 remains relatively flat.

While Ctext-1 and Ctext-3 may originate from the same plain text, their raw ciphertext frequencies will differ due to different substitution mappings. A relatively flat distribution of Ctext-2 indicates that the plaintext is effectively encrypted and do not immediately reveal the plaintext through simple frequency analysis.

Decrypting the Kama Sutra cipher (Ctext-3) without using the key

An effective strategy to decrypt Ctext-3 without having a key, is that the two ciphertexts Ctext-1 and Ctext-3 share the same plaintext and can leverage a common plaintext phase. A good candidate for such a common plaintext phase is “encyclopedia metropolitana” because of its length and its distinct letter sequence.

We observe this phrase in Ctext-1 as:

rhtytfjkrebi grpmjkjfbpihi

and in Ctext-3 as:

vmxbxolkvwrz nvgilklorgzmz

By aligning these ciphertexts segments with the presumed plaintext, we can directly deduce most of the characters of the substitution of Ctext-3.

From this alignment, we can have the following key mappings for Ctext-3:

V = E

M = N

X = C

B = Y

O = L

L = O

K = P

W = D

R = I

Z = A

N = M

G = T

I = R

After getting the above mappings, we can substitute the mappings to the ciphertext and derive the mappings for other characters in the ciphertext by doing pattern recognition.

Observe the phase,

dsrxs r dzh

With d = w, r = i and s as potentially h, this phase looks like

which i was

Conclusion on decryption strategy

The strategy to decrypt Ctext-3 without the key is through a crib-based attack by exploiting the shared plaintext with Ctext-1. In this ciphertext “encyclopedia metropolitana” serves as a powerful plaintext allowing the derivation of a partial substitution key. The rest of the decryption involves:

- Applying the initial key mappings
- Identifying common English patterns
- Making educated guesses for unknown letter mappings based on partial decryptions
- Iteratively refining the key as more plaintext is revealed and checking for consistency