Cryptology

Assignment 1: Vigenere

JH Darbyshire and Bengu Erenler

Part B

The following are the results of our decryptions:

Part C

Extended Alphabets

We believe extending the number of characters from 26 to 32 in general makes a cipher more difficult to break, particularly from a brute force point of view. Similarly would we expect the level of difficulty to diminish if the number of characters was reduced.

Indirectly, extending the number of characters may make, however, a cipher easier to break if those additions brought about strong statistical elements. For example our methods rely on letter frequencies being a signature. If an alphabet of 26 characters existed with equal probability of character appearance in the plaintext then this would likely be more difficult to break than a 32 character alphabet statistically favouring some characters more than others.

A mathematical argument for this can be made in terms of entropy: suppose a random character (X_2) from a two character alphabet has equal letter frequency then the entropy is:

$$H(X_2) = -\sum P(x_i) log_2(P(x_i)) = 1 \quad \text{where} \quad P(x_i) = 0.5 \quad \forall\, i\ .$$

The entropy for a similar character X_3in a similarly distributed set of three letters is:

$$H(X_3) = 1.58\ .$$

Whereas the entropy for a character X_{3*} three character set with probability density $\{0.1, 0.1, 0.8\}$ is:

$$H(X_{3*}) = 0.92\ .$$

In this final example we would consider the unpredictability of any given character less than in the original case with two characters.

Cipher Adjustments

(a)

This is not sensible