**Cipher Text 3**

Having solved all the other encryptions first I have determined by process of elimination this one is the stream cipher.

**Cipher Text 8**

Cipher for this text is Vigenère with a key of “APP”. To decrypt this text, I applied a test for the shift and permutation ciphers, neither of which resulted in a likely candidate. Testing the text for repeated sequences indicated groupings of repeated trigrams with intervals of 9 and 15 between repeats. The common denominator between these is 3, so I grouped the letters into every third letter, looked at the letter frequencies, and applied the appropriate shift to align with English letter frequencies. In this case, the first grouping aligned with English, so a shift of 0(A), and the other two groups had similar frequencies peaking on the shifted “T”, so a shift of -14 (P) to revert to plaintext was applied. The resulting text clearly describes a Japanese amphibious assault on Java. Plaintext is in the cipherText-8-decrypted.txt file.

**Cipher Text 13**

Plaintext selection:

“at lexingtons cxam radar detected the inbound japanese aircraft at a range of nmi mi km and vectored nine wildcats to intercept expecting the japanese torpedo bombers to”.

Full decrypted plaintext will be attached in file cipherText-13-decrypted.txt.

The cipher for text 8 is the shift method with a key of 14.

To aid in decryption the text was ran through a python script to provide the frequency of each letter occurring in the cipher text. As the result was close to a normal distribution of English texts with mismatched letters, the text was decrypted through a shifting algorithm for all 25 key possibilities with correction for wrapping outside the normal alphabet ASCII range.

**Cipher Text 18**

Transform, 10 rows by 8 columns permutation cipher. To decrypt this text, I built a test sentence – “THEQUICKBROWNFOXJUMPSOVERTHELAZYDOG”. I then encrypted the text by hand and devised an algorithm to return the text to its plaintext state. I then applied a loop to run through each possible combination of transform from 2x2 and up, as anything smaller than a 2x2 is trivial to recognize a pattern by hand. Applying the algorithm and testing for multiple English words present in the results indicated either a 10x4 or 10x8 transform. The 10 row by 8 column transform was the only one that was not still garbled in some way.

**Cipher Text 23**

Transform, reversed by decrypting 8x3 column transformation results in an article about the USS Archerfish. This selection was decrypted with the same methods as Cipher Text 18.

**Cipher Text 28**

Plaintext selection:

“more than any documented attack peter benchleys best selling novel jaws”

Cipher for this text was Vigenère. A frequency analysis of the text resulted in letter frequencies ranging from ~2-4 and ~5-7. The change in letter frequency suggested either not an English alphabet or the use of a substitution cipher. Since we know the text is from English Wikipedia articles, the text must have been encrypted using a substitution cipher. In order to test if the text was Vigenère, I used a function to search the text for repeated letter sequences and the spacing between them. Spacings for cipher text 28 were mostly 16 and 32 spaces apart. I decided to start testing for a key length of 2,4,8, or 16. By using a function to take each letter position in groupings of key length and performing a frequency analysis, a key length of 8 most closely matched English letter frequencies.

After finding the potential key length, I aligned the letter frequencies for each group superimposed with English letter frequencies and counted the amount of alignment shifts until they best aligned with English, accounting for A and E being common and X,Y, and Z being most uncommon. Using a function to shift each letter position by a potential key I adjusted each letter in the key starting with all “A” and running possible letters to find a key of “UFYUVSFE”, resulting in text about the movie JAWS. The text is from the Wikipedia article on the great white shark.