I used two main functions to decipher the ciphertext, with as much modularity and abstraction as possible. The first part is finding the 5 most likely key lengths using the Chi squared method by taking the sum of the squares of the distribution for each potential key length. It finds the 10 largest sum of squares, sorting them each time so it only needs to sort a maximum of 10 instead of sorting for all potential K at the end. It then takes the 10, and sums the sum of squares for the first 10 substrings to make sure the order is correct before returning the top 5 most likely key lengths.

With potential key lengths known, we start the second part which is finding potential keys and scoring the potential keys. It isn't a full frequency distribution analysis, instead for each key on each substring, it counts how many characters in the potential plaintext are printable English characters and weights them based on how likely they are in English frequency distribution. It then takes the scores and weights them to find the smallest key instead of returning repeat keys. It's not as optimal efficiency wise as using the "magic number" but it was more consistently returning a perfect plaintext and the lack of efficiency was minimal since it only had to go through 5 potential key lengths.

Since the Key size was limited to 1000 the time complexity is O(N) however it is important to note that it would also be dependent on key size which in theory could get quite large.

Recovered Key: \xae"\x00\xaf/\xb8\x99\x11\xdd\x00

Plaintext: We stand today on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.\nThe development of computer controlled communication networks promises effortless and inexpensive contact between people or computers on opposite sides of the world, replacing most mail and many excursions with telecommunications. For many applications these contacts must be made secure against both eavesdropping and the injection of illegitimate messages. At present, however, the solution of security problems lags well behind other areas of communications technology. Contemporary cryptography is unable to meet the requirements, in that its use would impose such severe inconveniences on the system users, as to eliminate many of the benefits of teleprocessing.\n