CA01 Cryptography Exercise
Spring 2014

Please implement encryption software based on the following description:

Input: Input to the software consists of a text file (.txt). The first line of the file specifies an encryption key. Successive lines in the file contain the plaintext message that is to be encrypted.

Encryption: The encryption algorithm is based on a Vigenere tableau. The key is repeated over the plaintext as many times as is needed to cover the entire message. Each character of plaintext is enciphered by shifting it down the alphabet by the amount specified by the corresponding letter in the key and the amount specified by the enciphered character to the immediate left. The very first letter of the plaintext is the exception to this: because it has no characters preceding it, it should be shifted by the amount of its corresponding key character alone.

Put more formally,

Let

- d(w) be the offset of character w from the beginning of the character set.
- p_i is the ith letter of plaintext
- k_i is the ith letter of the key after it has been repeated the appropriate number of times
- e_i is the ith letter of the enciphered text
- c(d) is the character at an offset of d from the beginning of the character set
- m is the modulus of the character set to ensure enciphered characters wrap around.

$c_1 = c((d(p_1) + d(k_1) + 0) \bmod m)$
$c_2 = c((d(p_2) + d(k_2) + c_1) \bmod m)$
$c_3 = c((d(p_3) + d(k_3) + c_2) \bmod m)$
…
$c_n = c((d(p_n) + d(k_n) + c_{n-1}) \bmod m)$

The key/plaintext/ciphertext character set consists of the space character, followed by the uppercase letters in alphabetic order, followed by the digits in numerical order, followed by period:

_ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789.

Output: Write the plaintext message, the key, and encrypted text to a text file named result.txt as in the example below:

```
Plain text: AUBURN UNIVERSITY
Key:        WAREAGLEWAREAGLEW
Encrypted:  XH1P8R3RQ02ATH2PZ
```

Submission details: Implement this algorithm in C, C++, Java, or Python. Read the key and plaintext from a file called plain.txt (supplied as part of the assignment). Write the plaintext message, the key, and encrypted text to a text file named result.txt

Submit a single .zip file containing your source code and result.txt. Your .zip file should be named <username>CA01.zip (e.g., umphrdaCA01.zip).

Additional work for COMP6730/COMP6736 Sections:

How would you suggest trying to break this cipher? Please be explicit as possible. An answer of "look for patterns" is not sufficiently detailed. (Hint: see the cryptoanalysis of the Vigenere Cipher shown in section 8.2.2.1 of your textbook.) Please submit your answer in a .pdf file in addition to the zip file described above.