CS410 / CS591
Computer Security
Homework #2
60 pts

Programming with Python

Write a script in Python that is an implementation of a version of the ***Vigenere cipher*** for English text. Your script should distinguish lowercase and uppercase letters (i.e., the encryption key and the plaintext are allowed to be composed of lowercase and uppercase letters but the ciphertext should be uppercase).

In addition to letters, there will be four other characters in the plain text: comma (26), dot (27), dash (28), underscore (29) changing the encryption function to be under mod 30. Your script should read from standard input and write to standard output. It should prompt the user for the encryption key of size k. Then key is not allowed to be repeated as in the standard Vigenere cipher. Instead, we will follow a block cipher-based idea. Basically, the plaintext and ciphertext will have blocks of size k which is same as the key size. If the key length is shorter than the plaintext, the ciphertext of block size k of the previous block is concatenated to the key.

Here is an example:

When the keyword is “Carbondale” with k = 10:

Plaintext : SIU_CS-Department_is_the_best
Key : CarbondaleUIHAQBBDPTUZ,MUOUCX
Ciphertext: UIHAQBBDPTUZ,MUOUCXHTODQTPYUM