Homework 1

Cryptography

CS 435

Ritvik Upadhyaya

Solution 1

We know that the length of the ciphertext = 17.
Since the contents of the plain text are only two days of the week, let's start by looking at the length of each day.

Table 1: Day Length Table

Day	Length
Monday	6
Tuesday	7
Wednesday	9
Thursday	8
Friday	6
Saturday	8
Sunday	6

The only combination that will work should have a plain text of length 17. Assuming that there are no spaces in between, the only combinations that will work are:

Wednesday and Thursday
OR
Wednesday and Saturday

(The order of the two days can be reversed from what written above.)
Next, we know that all the days end with the phrase 'day' so we can use that as our repititive phrase in the Kasiski's method. And we know that irrespective of the order of the words, the last three letter of the plain text have to be 'day' as well. Therefore using the formula

$$m_i = (c_i - k_i) \bmod 26$$

d = 3, a = 0, y = 24.
r = 17, v = 21, c = 2.

From the equation:

$3 = 17 - k_{14} \bmod 26 \Rightarrow k_{14} = 26n + 14$
$0 = 21 - k_{15} \bmod 26 \Rightarrow k_{15} = 26n + 21$
$24 = 2 - k_{16} \bmod 26 \Rightarrow k_{16} = 26n - 22$

The last three letters of the key are OVE.
Using the same equations over the entire plaintext combinations and the given cipher text, we see that the possible keys are:

Table 2: Key to Combinations

Plaintext	Key
WednesdayThursday	DOCTORSTRZGFHKOVE
ThursdayWednesday	GLLPAGVVTOKMUKOVE
WednesdaySaturday	DOCTORSTRANGELOVE
SaturdayWednesday	HSMMBGVVTOKMUKOVE

So we see that the plain text is wednesdaysaturday as the key is a combination of english words - *Doctor, Strange, Love.*

Solution 2

Part A

If the attacker knows that the password is either abcd, or bedg and that the user has encrypted the password using shift cyper, it is easy for the attacker to nd out which password is actually the correct one. Because in shift cypher, the shift is constant for all the characters in the ciphertext, if the ciphertext has characters progressing by only 1 i.e something like pqrs, it is almost positive that the password is 'abcd'.

If its not abcd, then we know that the password is 'bedg'. To con rm, the attacker can look at the di erence in the characters in the ciphertext. For example, the attacker can check if the character in ciphertext for e is 3 more than that for the character for b in ciphertext and so on. If all the checks are valid, then we can say for sure that the password was 'bedg'.

Part B

Period 2

In this case, the rst and the third character in the ciphertext will be o by the same amount since the key will only be of length two. SO the attacker can look at the ciphertext and see if the rst and the third character are o by 2 (the di erence between 'a' and 'c' of 'abcd'). If so, then the password is indeed 'abcd' or else it is 'bedg'.

Period 3

Like with period 2, the attacker can see what the password is if the plaintext is crypted using vigenere cipher. The di erence would just be that the attacker will have to look at the rst and the 4th characters in the ciphertext. If the two are o by 3 ('d'-'a' = 3). thee to lookwillit is 'bedg'.