CS411-507 CRYPTOGRAPHY HOMEWORK 1

Name: Elif Cemre Durgut

ID: 26493

Note: I added the code implementations for each question in different files.

1. “DAMP” and “ROAD” are the two meaningful words, the encryption keys are 10 and 20 respectively. You can see my code in question1.py, I tried all the possible keys from 0 to 26.
2. The plain text is "ANYBODY CAN MAKE HISTORY. ONLY A GREAT MAN CAN WRITE IT."Encryption key is (9, 17). Decryption key is (3, 1) using the encryption key. My code is available at question2.py. Firstly, I found the most frequent letter in the cipher text which is R. This means A is encrypted as R meaning that the beta is 17. Because

E(0) = alpha\*26 + beta = 17. Then I tried the possible alpha values ( gcd(alpha, 26) should be 1) and found the meaningful text among them.

1. My code is at question3.py file. Answer is:

“ONA ÖZGÜ HİÇBİR ŞEY İÇİMDE ÖLMÜŞ DEĞİL, SANKİ ZORBAYA AİT OLAN HER ŞEY ÖLÜMSÜZLEŞMİŞ, FAKAT ŞU GÜNLERDE ANİ BİR HUZURSUZLUK BENİ SARSIYOR İKİ YILDIR ONDAN MEKTUP ALMADIM, ARTIK YETMİŞİNİ AŞMIŞ OLMALI BELKİ DE SON GÜNLERİNİ YAŞIYORDUR KESİNLİKLE SON GÜNLERİNİ YAŞIYORDUR, YOKSA ONA AİT OLAN HER ŞEYİ TOPARLAMAK, BANA NE SÖYLEMİŞ VE NE YAPMIŞSA HATIRLAMAK VE KAÇMASINLAR DİYE HEPSİNİ KAĞIDA YANSITMAK KONUSUNDA BANA EGEMEN OLAN ÖNÜ ALINMAZ İSTEĞİ BAŞKA TÜRLÜ AÇIKLAYAMAZDIM SANKİ ÖLÜMÜ, ONUN ÖLÜMÜNÜ KAÇIRMAK İSTİYOR GİBİYİM KORKARIM BUYAZDIĞIM, BİR KİTAP DEĞİL, BİR GÜZELLEME OLACAK VE ŞIMDİ GÖRÜYORUM Kİ BU KİTAP, BİR GÜZELLEMENİN BÜTÜN BELİRTİLERİNİ TAŞIMAKTADIR TEPSİ, KOLİVA VE KALIN BİR ŞEKER TABAKASIYLA SÜSLENMİŞ, ONUN ÜZERİNE DE, TARÇINI VE BADEMLE ALEKSİ ZORBA ADI YAZILMIŞ”

A is given as the most frequent letter in the plain text and I found the most frequent letter as Ğ. This means A is encrypted as Ğ so beta value must be 8. The modulus is 31 (prime) so alpha can take all the values between 0 and 31. When the alpha is 6, the text is meaningful. Enc. Key = (6, 8). Dec. Key = (26, 9).

(P.S. You can see the corresponding results for each alpha value if you uncomment the commented lines.)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ki | probability | mi | Prob. | ci | Prob. |
| 0 | 1/26 | 0 | a | 0 | a/26 |
| 0 | 1/26 | 1 | b | 1 | b/26 |
| 0 | 1/26 | 2 | c | 2 | c/26 |
| … | … | … |  | … | … |
| 0 | 1/26 | 25 | 1-(a+b+c+..) | 25 | (1-(a+b+c..))/26 |
| 1 | 1/26 | 0 | a | 1 | a/26 |
| 1 | 1/26 | 1 | b | 2 | b/26 |
| … | … | … |  | … | … |
| 2 | 1/26 | 0 | a | 2 | a/26 |
| 2 | 1/26 | 1 | b | 3 | b/26 |
| … | … | … | … | … | … |

For example let’s have a look at the probability of i’th letter of the ciphertext being 2. P(ci = 2) = c/26 + b/26 + a/26 + …. + (1-(a+b+c))26 = 1/26

And this is the case for any letter of the ciphertext. So the ciphertext is random.

1. Modulus is 784 because the encrypted bigram can take 28x28 values. The size of the key space is the multiplication of the number of alpha and beta values that can take. Beta can take any value between 0 and 784. For alpha, this condition must be met: gcd(alpha, 784) = 1. There are 336 values satisfying this. Key space is 784\*336=263424
2. The frequency analysis can still work but in this case we need to know the most common bigrams in English instead of only a letter. We can divide the ciphertext into bigrams and record their frequencies.
3. Based on the given hints, the last two letters of the text must be “.X” and it is encrypted as “BE”. This means (751 \* alpha + beta)mod784 = 32. I tried all the possible alpha values(gcd(alpha, 28) = 1). The encryption key is (121, 105). The plain text is “IT DOES NOT DO TO DWELL ON DREAMS AND FORGET TO LIVE.”
4. First thing to do is finding the key length. So I shifted the text to right in different amounts and recorded the number of coincidences (same letter). The maximum number of coincidences is 67 when the shift amount is 50. However I realized a pattern that the number of coincidences are higher when the shift amount is multiple of five. So I started trying 5 as key length. Then I divided the text into group of 5 letters and made the frequency analysis. The key is “hayao”. The plain text is:

“But there is one way in this country in which all men are created equal-there is one human institution that makes a pauper the equal of a Rockefeller, the stupid man the equal of an Einstein, and the ignorant man the equal of any college president. That institution, gentlemen, is a court. It can be the Supreme Court of the United Etates or the humblest J.P court in the land, or this honorable court which you serve. Our courts have their faults, as does any human institution, but in this country our courts are the great levelers, and in our courts all men are created equal.”