1. Since key space is 26 in shift cipher, we can found the key with exhaustive search. This question was done by program that I wrote, you can find the programs in my submission folder. In program, we have nested for loops. First loop iterate over possible keys which are English letter in shift cipher. Other for loop iterate over each char of the cipher-text, and we apply current key to each character in the cipher. After second for loop (that iterate over cipher-text) is over, we print the key together with corresponding plaintext then we reset the plain text and try next key. When all of the possibilities were printed, I found that plaintext either “ROAD” with key 22(‘W’) or “DAMP” with key 10(‘K’).
2. Since the most frequent letter in the plaintext is given as ‘A’, we can easily found the beta. To find that, we should get the most frequent letter in the cipher-text. In program, we have letter counter dictionary that store characters with corresponding occurrences, to find the most frequent letter in cipher-text, we iterate over the cipher-text, and modify letter count dictionary accordingly. After that, we can obtain the most frequent letter in cipher-text with max() method of dictionary. We obtain ‘R’ as the most fret letter in the cipher-text. This means that our beta is 17(‘R’) - 0(‘A’) = 17. On the other hand, we are also know possible alpha keys because gcd(a, 26) should be 1. So that our possible alphas are [1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25]. Then we can find possible gamma keys with the inverse modulus of alphas. To this purpose, we can use given ‘modinv’ function. Then we obtain possible gammas are [1, 9, 21, 15, 3, 19, 7, 23, 11, 5, 17, 25]. Moreover, we can find theta, together with possible gammas and beta key. Since the key space is decreased importantly, now we can perform exhaustive search, there are 12 possible gamma and 1 theta decryption key, total of 12 pairs of decryption keys. Then, we can apply these decryption keys to each characterizer of the cipher-text and investigate the outputs. In our case, meaningful message was came with decryption key pair (gamma:3, theta:1), so that we can conclude that encryption key pair is (alpha:9, beta:17). The message is ‘ANYBODY CAN MAKE HISTORY. ONLY A GREAT MAN CAN WRITE IT. ’.

3. We have 31 letters in total, since 31 is prime the possible alphas are [1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30]. Again we know the the most frequent letter in the plaintext, so that we can find the one of encryption key beta and one of decryption key theta. With the same method that I described in question 2, the most frequent letter in cipher-text was found as ’N’. This means that beta is 16(’N’) - 0(‘A’) = 16. Since we know the possible alphas, we can obtain possible gammas. To find possible gammas, we iterate over each alpha keys and apply ‘modinv’ function such that modinv(alpha, 31). So that we can obtain gamma keys as [1,16,21,8,25,26,9,4,7,28,17,13,12,20,29,2,11,19,18,14,3,24,27,22,5,6,23,10,15,30]. Moreover, we can find theta, together with possible gammas and beta key. Then we can try each possible decryption key pairs in our cipher-text and evaluate the outputs. Decryption key pair (gamma: 4, theta: 29) gave “BENİ SÜZDÜ, ANLADI VE AYRILIĞIN ACISINI DAĞITMAK İÇİN ALAYCI BİR GÜLÜMSEYİŞLE SORDU NE ZAMANA KADAR NE…”
4. Since shift amount is uniformly randomly, we obtain 1/26 possibility for each possible shift amount. This means;

$$P(k = C) = 1/26, \quad C \in \{A,B,C,D\ldots,Z\}.$$

The plain text characters are not balanced;

P(m = ‘A’) = a, P(m = ‘B’) = b, P(m = ‘C’) = c, … , P(m = ‘Z’) = z, and a + b + c + … + z = 1.

5. We have 28 letters in total, so there exist 28*28 = 784 different bigrams. In order to be each encoded number unique, modulus should be 784. So that we obtain encryption function as;

$$y = (a*x + B) \bmod 784$$

in this equation, y is number for encoded bigram from cipher-text and x is number for encoded bigram from plaintext. In order to calculate possible alpha we should use Euler's phi function to find relatively prime integers according to 784 (like we did in original affine cipher). $\phi(784) = 336$. This means there exist 336 integer that relatively prime to 784. As a result we have 336 different option for alpha and 784 different option for beta, so the key space is

336*784 = 263 424

6. Since it is modified version of Affine Cipher which is Substitution Cipher, it shouldn't be secure against the frequency analysis.
7. I tried but I cannot implement
    1. - Firstly, all of the punctuation symbols and spaces were removed and all of the chars are uppered.

       - The maximum shift amount was determined as 20 and created array that stores num of coincidences.

       - Then we iterate over predetermined maximum shift amount times which is 20. Inside this for loop we first count the coincidences with the help of countLetters functions then we shift the cipher one character to the right. (functions are explained in the program)

       - Then we print the shift amount together with corresponding coincidences which were calculated and stored in countLetter function.

       - For shift amount 5, there are 40 coincidences compared to its adjacent which has about 20-25 coincidences. However there is some clear peeks in 7 and 10, but I tried 5 firstly.

       - I set key_length as 5

- Then clusters were created. Clusters are store the indexes of the sub-ciphers such as;

```
[0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, 65,
[1, 6, 11, 16, 21, 26, 31, 36, 41, 46, 51, 56, 61, 66,
[2, 7, 12, 17, 22, 27, 32, 37, 42, 47, 52, 57, 62, 67,
[3, 8, 13, 18, 23, 28, 33, 38, 43, 48, 53, 58, 63, 68,
[4, 9, 14, 19, 24, 29, 34, 39, 44, 49, 54, 59, 64, 69,
```

- Then we calculate the most repeated chars in the sub-ciphers

- The most repeated chars together with the corresponding the number of repetitions are stored under the array of dictionaries

- Then, dictionaries inside the arrays are sorted according to the max number of receptions, and we print array, it looks like that;

```
for cluster 0 : [('L', 28), ('A', 18), ('H', 14), ('U', 13), ('P', 12), ('V', 11),
for cluster 1 : [('E', 20), ('A', 18), ('T', 16), ('N', 16), ('O', 14), ('U', 13),
for cluster 2 : [('R', 22), ('C', 22), ('L', 18), ('G', 15), ('Y', 14), ('M', 12),
for cluster 3 : [('T', 20), ('I', 17), ('E', 17), ('O', 16), ('S', 11), ('U', 10),
for cluster 4 : [('S', 17), ('H', 17), ('F', 15), ('W', 14), ('B', 13), ('I', 11),
```

- So we obtain clue about the keys, for examples in the first sub-cipher the most repeated character was ‘L’ so, char ‘E’ (the most frequent letter in English alphabet) can be encrypted as ‘L’ with the first letter of the key. For the second sub-cipher, the most frequent char was ’E’, so the second char of the key can be A(‘0’)…

- Then I created possible keys by hand and I tried these keys for decrypting cipher-text. I found decryption key as ‘HAYAO’.

- After finding key, I put back the punctuation symbols, spaces and adjust characters (lower/upper) according to original cipher-text.

- Then I get;

“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. I'm no idealist to believe firmly in the integrity of our courts and in the jury-system that is no ideal to me, it is a living, working reality. Gentlemen, a court is no better than each man of you sitting before me on this jury. A court is only as sound as its jury, and a jury is only as sound as the men who make it up. I am confident that you gentlemen will review without passion the evidence you have heard, come to a decision, and restore this defendant to his family. In the name of God, do your duty."