**Practical Cryptology**

**Find the keys and decrypt the message. We will use frequencies of English to solve the problem.**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| E | A | V | R | W | F | R | V | M | R | A | Z | E | W | T | M | T | J | Z | F | L | Y | H | I |
| P | R | A | C | T | I | C | A | L | C | R | Y | P | T | O | L | O | G | Y | I | S | F | U | N |

E A V R W F R V M R A Z E W T M T J Z F L Y H I

1. Count the number of times each letter appears in the ciphertext

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A2 | B0 | C0 | D0 | E2 | F2 | G0 | H1 | I1 | J1 | K0 | L1 | M2 | N0 | O0 | P0 | Q0 | **R****3** | S0 | T2 | U0 | V2 | W2 | X0 | Y1 | Z2 |

1. Most frequent ciphertext letters: R, A, E, F, M, T, V, W, Z
2. Using Table below, the most frequent plaintext letters are: E, T, (I, N, R), (A, O), S..

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Letter | A 0 | B 1 | C 2 | D 3 | E 4 | F 5 | G 6 | H 7 | I 8  |  J 9 | K 10 | L 11 | M 12 |
| frequency in % | 7 | 1 | 3 | 4 | 13 | 3 | 2 | 3 | 8 | < 1 | < 1 | 4 | 3 |
| Plaintext | N 13 | O 14 | P 15 | Q 16 | R 17 | S 18 | T 19 | U 20 | V 21 | W 22 | X 23 | Y 24 | Z 25 |
| frequency in % | 8 | 7 | 3 | <1 | 8 | 6 | 9 | 3 | 1 | 1 | <1 | 1 | <1 |

1. At this point you would need to start making assumptions, say

C1 = R(17) corresponds P1 = E(4) (most frequent)

C2 = A(0) corresponds P2 = T(19).

And then for this pair of C1, C2 and P1, P2 follow the algorithm of finding D and then keys A and B.

In this case we will have:

D=(P1-P2)%26 = (4-19)%26 = -15 % 26 = 11% 26 = 11

D\_Inverse = 19

The possible keys are:

A ≡ (D-1 \*(C1 – C2)) (mod 26) = 11

B ≡ (D-1 \*(P1\*C2 – P2\*C1)) (mod 26) = 25

1. If you will try to decrypt the message using A = 11 and B = 25 you will get the following plaintext: RTCEVKECNETARVQNQIAKUHWP which is not an English sentence, so we need to continue the process
2. You have to make a next assumption. Since, in this case the ciphertext is small but we do know the plaintext, I will take pairs of letters that I know will work out, but in general case, you will continue to make assumptions, and for each pair of plain and cipher text letters you will find possible keys A and B. Try to decrypt using these keys and decide whether the plaintext you received make sense or not.
3. In our case, we know the plaintext, see below, so I will make the following assumption:

P1 = T(19) C1 = W(22)

P2 = I(8) C2 = F(5)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| E | A | V | R | W | F | R | V | M | R | A | Z | E | W | T | M | T | J | Z | F | L | Y | H | I |
| P | R | A | C | T | I | C | A | L | C | R | Y | P | T | O | L | O | G | Y | I | S | F | U | N |

D = (19 - 8) % 26 = 11, D\_Inverse = 19

A ≡ (D-1 \*(C1 – C2)) (mod 26) = 19\*(22 - 5) % 26 = 11

B ≡ (D-1 \*(P1\*C2 – P2\*C1)) (mod 26) =19\*(19\*5 - 8\*22) % 26 = 21

1. Using A=11 and B=21 will produce correct plaintext