**Practical Cryptology**

**Affine Cipher Cryptanalysis**

**The case C = AP (mod 26) (B = 0) is called Decimation Cipher.**

Example: Decipher the following text and find a key:

CFQGE KAZEMF ZMAGVMC NMO VYSV

Solution:

1. For each letter, count the number of times it appears in the ciphertext.

2. Choose the letter that appears the most.

In our example, M occurs 4 times in the ciphertext – the most.

3. Use the English frequency table below to make a following assumption:

Since E is the most common letter, we will make a tentative assumption that ciphertext M (12) corresponds to the plaintext E (4).

4. Solve equation:

C = AP (mod 26) to find A using 12 (M) instead of C and 4 (E) instead of P:

A\*4 ≡ 12 (mod 26)
there are 2 solutions in the range 1 to 25, A = 3 and A =16 (not good, not relatively prime with 26)

5. If our assumption was correct, the key A is 3.

6. To find the plain text we need to solve the following equations:

7. To find the plaintext we need to use the following decryption formula:

P = 3-1 C (mod 26) ,

 3-1 = 9 is multiplicative inverse of 3 mod 26.

8. Solving P = 9C (mod 26) for each ciphertext letter you will get the following plaintext:

Decrypted message: STOC MARKET REACHES NEW HIGH

**Frequency Table of English:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| frequiency 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 |
| Ciphertext | 8 | 7 | 3 | <1 | 8 | 6 | 9 | 3 | 1 | 1 | <1 | 1 | <1 |