**Practical Cryptology**

**Affine Cipher Summary and Cryptanalysis**

1. Encryption: C ≡ ( AP + B ) (mod 26)
2. Decryption: P ≡ (A-1 (C – B )(mod 26)
3. Conditions:
   * A is relatively prime to 26: GCD (A, 26) = 1
   * B any number between 0 and 25

**Cryptanalysis based on two known plaintext letters – known plaintext attack**

Suppose you know the cipher text, C1C2C3….CN and you know two plaintext letters, for simplicity, suppose that you know P1 and P2 that corresponds to the C1 and C2.

Based on this information, in certain situations you will be able to find the keys of the Affine Cipher: A and B.

Method of finding A and B:

1. Substitute C1, C2, P1 and P2 intro encryption formula:

C1 ≡ (AP1 + B)(mod 26)

C2 ≡ (AP2 + B)(mod 26)

1. To solve this system, use the following steps:

**Step 1 - Finding D using the formula below:**

D ≡ (P1 – P2)(mod 26)

**Pay Attention! D should be relatively prime to 26, in order to the system to have a unique solution. If D is not relatively prime you would not be able to find the keys based on the pair of the plaintext that you have.**

**Step 2 – Finding** D-1 **– multiplicative inverse of D mod 26**

If D is relative prime to 26, find D-1 – multiplicative inverse of D mod 26

D\*D-1 ≡ 1 (mod 26)

**Step 3 – Finding keys A and B using formulas below:**

A ≡ (D-1 \*(C1 – C2)) (mod 26)

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

**Example 1:**

Suppose you know two first plaintext letters and corresponded ciphertext letters and they are: P1 = 4, P2 = 19, C1 = 2, C2 = 20. To find keys, we need to solve the following system of equations:

2 ≡ 4A + B (mod 26)

20 ≡ 19A + B (mod 26)

Step 1: D ≡ 4 – 19 (mod 26) = -15 (mod 26) = 11 – relatively prime to 26

Step 2: D-1 = 19

Step 3: A ≡ 19 \* (2 – 20) ≡ -19\*18 ≡ - 342 (mod 26) = 22

(since 342 % 26 = 4, 26 – 4 = 22)

B ≡ 19 \* (80 – 38) ≡ 19\*42 ≡ 798 (mod 26) = 18

The keys are: A = 22 and B = 18

**Example 2:**

Suppose the plaintext starts with **if** and the corresponding ciphertext is **PQ**. Find the keys.

Solution: Numeric values of known letters: i = 8, f = 5, P = 15, Q = 16

Using Affine Cipher encryption formula we obtain 2 equations:

15 = (A\*8 + B) (mod 26)

16 = (A\*5 + B)(mod 26)

**1: Subtracting equations:**

-1 = A\*3 (mod 26), pay attention, - 1 ≡ 25 (mod 26)

25 = 3\*A mod 26

A = 25 \* (multiplicative inverse of 3 mod 26) (mod 26) = 25

A = 25 \* 9 (mod 26) = 17

**2: Substitute A = 17 into the first equation to find B:**

15 = (17\*8 + B)(mod 26)

B = (15 – 17\*8)(mod 26) = (15 – 136)(mod 26) = (-121)\*(mod 26) =

26 – (121%26) = 9

**Final answer: A = 17 B = 9**

**Example 3:** go – plaintext TH – ciphertext

19 = (6\*A+B) (mod 26)

7 = (14\*A+B)(mod 26)

**1: Subtracting:**

12 = (-8\*A) (mod 26) = (18 \* A)(mod 26) – this equation doesn’t have unique solution since 18 and 26 are not relatively prime

There are 2 solutions: A = 5 and 18

**2: for each A find B**

In both cases B = 15

**Final answer**: there are 2 possible pairs of keys (5, 15) and (18, 15)

Since 18 is not relatively prime to 26, the final answer is **A = 5 B = 15**