Affine Cipher Exercises (Daily Due Sept 2)

Katherine E. Stange, CU Boulder

Exercise 1

Suppose you have a known plaintex situation for affine cipher. The plaintext is HAHAHA and the ciphertext is NONONO. Determine the key. Hint: write down some equations modulo 26 that must be true and try to solve for the key. Use the Crypto Tools Sheet (addition and multiplication tables mod 26) in solving.

Solution. We have that H (7) encrypts to N (13) and A (0) encrypts to O (14). Therefore,

$$7\alpha + \beta \equiv 13 \pmod{26}, \quad 0\alpha + \beta \equiv 14 \pmod{26}.$$

From this, we obtain $\beta \equiv 14$ and, substituting into the other equation,

$$7\alpha + 14 \equiv 13 \pmod{26}.$$

Simplifying,

$$7\alpha \equiv -1 \pmod{26}.$$

Using the multiplication tables,

$$\alpha \equiv 11 \pmod{26}.$$

We've found the key $(11, 14)$.

Exercise 2

Suppose you have a known plaintext situation for affine cipher. The plaintext is III (that's 888, in case there's any confusion) and the ciphertext is QQQ. Explain why this is not enough information to determine the key.

Solution. From the pair, we know

$$8\alpha + \beta \equiv 16 \pmod{26}.$$

However, this is one equation in two unknowns; it's not enough information to solve.

Exercise 3

Suppose you have a known plaintext situation for affine cipher. The plaintext is BO and the ciphertext is OB. Explain why this is not enough information to determine the key.

Solution. From the pair, we know

$$\alpha + \beta \equiv 14 \pmod{26}, \quad 14\alpha + \beta \equiv 1 \pmod{26}.$$

If we try to solve this system of equations by subtracting, we obtain

$$13\alpha \equiv 13 \pmod{26}.$$

With reference to the multiplication table mod 26, this has a whopping 13 solutions (all the odds).

In fact, for any odd α,

$$13\alpha \equiv 13 \pmod{26},$$

so that

$$14\alpha \equiv 13 + \alpha \pmod{26}.$$

This implies that, for $\beta \equiv 14 - \alpha \pmod{26}$, we obtain a solution to the original system of equations!

Therefore the equations have many solutions, namely

$$(1, 13), (3, 11), (5, 9), \ldots$$

Exercise 4

I decide to make affine cipher more secure by encrypting first with one key, and then encrypting again using another key. Is there any reason this is more secure? Why or why not?

Solution. Suppose the first key is (α_1, β_1) and the second key is (α_2, β_2). Then encrypting by the first and then by the second is

$$p \mapsto \alpha_2(\alpha_1 p + \beta_1) + \beta_2 = \alpha_1\alpha_2 p + \alpha_2\beta_1 + \beta_2$$

so it is just like encrypting once with the key $(\alpha_1\alpha_2, \alpha_2\beta_1 + \beta_2)$.

So a double affine cipher is just a single affine cipher with a different key. Hence it is not more secure.