# An extended affine cipher

On the surface this problem seems to be asking us to solve a system of polynomial equations, and there may not be a solution or there could be multiple solutions. This is clearly outside the scope of this course, so there must be something that I missed. Let's first have a look at the provided ciphertext and the partial plaintext (`hint.txt`). Using a simple python script, I extracted all the pairs of known plaintext-ciphertext (see the appendix for the python code I used). The numbers in the parentheses correspond to the numerical encoding of the characters. The characters to the left of the arrows are the plaintext, and the ones to the right are ciphertexts.

```
i=40: g (16) --> n (23)
i=50: 8 (8) --> E (40)
i=51: J (45) --> i (18)
i=53: y (34) --> g (16)
i=64: t (29) --> G (42)
i=314: q (26) --> A (36)
```

Recall that the encryption function is given by the formula:

$$e_k(x, i) = a^i x + bi \mod 67.$$

So, for example, the first plaintext-ciphertext pair would give us the following equation:

$$\begin{array}{rcll} 23 & = & a^{40} \cdot 16 + b \cdot 40 \mod 67 & (E_1) \\ 40 & = & a^{50} \cdot 8 + b \cdot 50 \mod 67 & (E_2) \\ 18 & = & a^{51} \cdot 45 + b \cdot 51 \mod 67 & (E_3) \\ 16 & = & a^{53} \cdot 34 + b \cdot 53 \mod 67 & (E_4) \\ 42 & = & a^{64} \cdot 29 + b \cdot 64 \mod 67 & (E_5) \\ 36 & = & a^{314} \cdot 26 + b \cdot 314 \mod 67 & (E_6) \end{array}$$

The degrees of the resulting polynomials are too high to be solved directly. So we turn to the provided hint (on using Fermat's Little Theorem) to see if we can simplify the equations to a solvable (linear) form.

Recall that Fermat's Little theorem states that

$$a^{p-1} \equiv 1 \mod p$$

when $p$ is prime. The modulus for the affine cipher in this case (67) is a prime number, so we can apply Fermat's Little Theorem to simplify the equation $(E_6)$ above to:

$$\begin{array}{rrcll} & 36 & = & a^{314} \cdot 26 + b \cdot 314 & \\ \Rightarrow & 36 & = & a^{4*(67-1)} \cdot a^{50} \cdot 26 + b \cdot 314 & \\ \Rightarrow & 36 & \equiv & a^{50} \cdot 26 + b \cdot 314. & (E_7) \end{array}$$

We immediately notice that the degree of $a$ in $(E_7)$ is the same as the degree of $a$ in $(E_2)$. We could thus eliminate the term containing $a$ from these equations as follows: First multiply the equation $(E_2)$ with $26$:

$$\begin{array}{rcl} (E_2) \times 26 & \Rightarrow & (26 \cdot 40) \equiv a^{50} \cdot 8 \cdot 26 + b \cdot 50 \cdot 26 \mod 67 \\ & \Rightarrow & 35 \equiv a^{50} \cdot 7 + b \cdot 27 \mod 67. \qquad (E_8) \end{array}$$

Note that we simplify the second equation by performing the remainder calculation modulo 67, so for example, $26 \cdot 40$ simplifies to $26 \cdot 40 = 1040 \equiv 35 \mod 67$.

Next, we multiply both sides of the equation $(E_7)$ with 8 to get:

$$20 \equiv a^{50} \cdot 7 + b \cdot 33 \mod 67 \qquad (E_9)$$

We can now subtract $(E_9)$ from $(E_8)$ to obtain:

$$\begin{array}{rrcl} & (35 - 20) & \equiv & b \cdot (27 - 33) \mod 67 \\ \Rightarrow & 15 & \equiv & -6 \cdot b \mod 67 \\ \Rightarrow & 15 & \equiv & 61 \cdot b \mod 67 \\ \Rightarrow & b & \equiv & 15 \cdot 61^{-1} \mod 67 \\ \Rightarrow & b & \equiv & 31 \mod 67 \end{array}$$

Substituting the value of $b$ to $(E_2)$ we get the value of $a^{50} \mod 67$ as follows:

$$\begin{array}{rrcl} & 40 & = & a^{50} \cdot 8 + b \cdot 50 \mod 67 \\ \Rightarrow & 40 & = & a^{50} \cdot 8 + 31 \cdot 50 \mod 67 \\ \Rightarrow & a^{50} & = & (40 - 31 \cdot 50) \cdot 8^{-1} \mod 67 \\ \Rightarrow & a^{50} & = & 29 \end{array}$$

*Instructor notes: At this point we could try to find the 50th-root of $a^{50} \mod 67$ to find the value of $a$, but this would involve techniques that are beyond the scope of this course. So a different solution would be required.*

Notice that in the equation $(E_3)$, the degree of $a$ is 51, i.e., one more than $a^{50}$. So we could turn that equation into a linear equation by substituting the value of $a^{50}$ we found above, resulting in:

$$\begin{array}{rrcl} & 18 & = & a^{51} \cdot 45 + b \cdot 51 \mod 67 \\ \Rightarrow & 18 & = & a^{50} \cdot a \cdot 45 + b \cdot 51 \mod 67 \\ \Rightarrow & 18 & = & 29 \cdot 45 \cdot a + 31 \cdot 51 \mod 67 \\ \Rightarrow & 18 & \equiv & 32 \cdot a + 40 \mod 67 \\ \Rightarrow & a & \equiv & (18 - 40) \cdot 32^{-1} \equiv 37 \mod 67. \end{array}$$

So we have recovered the key: (37, 31). Using this key and the provided `affine.py`, we decrypt the ciphertext to obtain:

# Appendix: source code

The following was used to extract the plaintext-ciphertext pairs from `hint.txt` and `cipher.txt`.

```python
#!/usr/bin/env python3

import affine

map = affine.map

with open('hint.txt','r') as f:
    pt = f.read()

with open('cipher.txt','r') as f:
    ct = f.read()

for i in range(len(ct)):
    if pt[i] != '_':
        print("i=%d: %s (%d) --> %s (%d)"
            % (i,pt[i],map[pt[i]], ct[i], map[ct[i]]))
```