Two More Examples of a Known Plaintext Attack

Here are two examples of cryptanalyzing a Hill cipher with a known plaintext attack. Each example is done by hand – without using *Mathematica*. In example one, there is no need to reduce the modulus; in example two the modulus must be reduced.

Example one:

Ciphertext: `FAGQQ ILABQ VLJCY QULAU STYTO JSDJJ PODFS ZNLUH KMOW`

We are assuming that this message was encrypted using a 2×2 Hill cipher and that we have a crib. We believe that the message begins "`a crib.`"

ac	ri
[1, 3]	[18, 9]
[6, 1]	[7, 17]
FA	GQ

We could either solve for the key or the key inverse. To solve for the key, we would solve

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 \\ 3 \end{bmatrix} = \begin{bmatrix} 6 \\ 1 \end{bmatrix}$$

and

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 18 \\ 9 \end{bmatrix} = \begin{bmatrix} 7 \\ 17 \end{bmatrix}$$

To solve for the key inverse, we would solve

$$\begin{bmatrix} e & f \\ g & h \end{bmatrix}\begin{bmatrix} 6 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \end{bmatrix}$$

and

$$\begin{bmatrix} e & f \\ g & h \end{bmatrix}\begin{bmatrix} 7 \\ 17 \end{bmatrix} = \begin{bmatrix} 18 \\ 9 \end{bmatrix}$$

We will solve for the key.

$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 \\ 3 \end{bmatrix} = \begin{bmatrix} 6 \\ 1 \end{bmatrix}$ represents two linear equations:

$$\begin{array}{ccc} a & +3b & = & 6 \\ c & +3d & = & 1 \end{array}$$

and $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 18 \\ 9 \end{bmatrix} = \begin{bmatrix} 7 \\ 17 \end{bmatrix}$ represents

$$\begin{array}{cccc} 18a & +9b & = & 7 \\ 18c & +9d & = & 17 \end{array}$$

Now we solve the following linear congruences mod 26.

$$\begin{cases} a & +3b & = & 6 \\ 18a & +9b & = & 7 \end{cases} \text{ and } \begin{cases} c & +3d & = & 1 \\ 18c & +9d & = & 17 \end{cases}$$

We will solve the pair of congruences $\begin{cases} a & +3b & = & 6 \\ 18a & +9b & = & 7 \end{cases}$ first.

To eliminate an unknown, multiply congruence 1 by 3

$$\begin{cases} 3a & +9b & = & 18 \\ 18a & +9b & = & 7 \end{cases}$$

and subtract congruence 2 from congruence 1.

$$-15a \quad = \quad 11$$

Modulo 26, -15 is 11.

$$11a = 11$$

Divide by 11 to obtain *a*.

$$a = 1$$

Now substitute this in congruence 1.

$$1 + 3b = 6$$

$$3b = 5$$

The multiplicative inverse of 3 is 9 modulo 26.

$$b = 9 \times 3b = 9 \times 5 = 45 = 19 \bmod 26$$

So, the key looks like

$$\begin{bmatrix} 1 & 19 \\ c & d \end{bmatrix}$$

Now solve the system $\begin{cases} c & +3d & = & 1 \\ 18c & +9d & = & 17 \end{cases}$

$$\begin{cases} 3c & +9d & = & 3 \\ 18c & +9d & = & 17 \end{cases}$$

$$15c = 14$$

$$c = 7 \times 15c = 7 \times 14 = 98 = 20 \bmod 26$$

$$20 + 3d = 1$$

$$3d = -19 = 7 \bmod 26$$

$$d = 9 \times 3d = 9 \times 7 = 63 = 11 \bmod 26$$

The key is $\begin{bmatrix} 1 & 19 \\ 20 & 11 \end{bmatrix}$.

Example two:

We are assuming that we have a ciphertext message was that encrypted using a 2×2 Hill cipher and that we have a crib. We believe that ciphertext `UKJN` corresponds to plaintext `word`.

$$\begin{array}{c|c} \text{wo} & \text{rd} \\ [23,\ 15] & [18,\ 4] \\ [21,\ 11] & [10,\ 14] \\ \text{UK} & \text{JN} \end{array}$$

The two systems of congruences are:

$$\begin{cases} 23a & +15b & = & 21 \\ 18a & +4b & = & 10 \end{cases} \text{ and } \begin{cases} 23c & +15d & = & 11 \\ 18c & +4d & = & 14 \end{cases}$$

We will solve the system on the left.

To eliminate an unknown, multiply congruence number 1 by 4 and congruence number 2 by 15 both modulo 26.

$$\begin{cases} 14a & +8b & = & 6 \\ 10a & +8b & = & 20 \end{cases}$$

Subtract the second congruence from the first.

$$4a = -14 = 12 \bmod 26$$

This congruence corresponds to the equation $4a = 12 + 26k$, $4a$ is 12 plus a multiple of 26. Notice that 2 divides the coefficient of *a*, the constant 12, and the modulus 26. We reduce the modulus by dividing by 2.

$$2a = 6 + 13k$$

and we have a congruence modulo 13.

$$2a = 6 \bmod 13$$

This congruence does not have a common factor among the coefficient, the constant, and the modulus.

Here are the multiplicative inverses of the integers modulo 13:

Number	1	2	3	4	5	6	7	8	9	10	11	12
Multiplicative inverse	1	7	9	10	8	11	2	5	3	4	6	12

To find *a*, multiply $2a = 6 \bmod 13$ by the multiplicative inverse of 2, which is 7.

$$a = 7 \times 2a = 7 \times 6 = 42 = 3 \bmod 13$$

So, *a* is 3 modulo 13. But, there are two integers mod 26 that are 3 mod 13, namely, 3 and 3 + 13 = 16. So, there are two possible values for *a*.

If *a* = 3,

$$18 \times 3 = 4b = 10$$

$$54 + 4b = 10$$

$$2 + 4b = 10$$

$$4b = 8 \bmod 26$$

$$2b = 4 \bmod 13$$

$$b = 7 \times 2b = 7 \times 4 = 26 = 2 \bmod 13$$

So, *b*=2 or *b* = 2+13 = 15 modulo 16.

If *a* = 16,

$$18 \times 16 + 4b = 10$$

$$288 + 4b = 10$$

$$2 + 4b = 10$$

which yields the same solutions for *b*.

Here are the 4 possible solutions for *a* and *b*.

$$\begin{array}{ll} a=3 & b=2 \\ a=3 & b=15 \\ a=16 & b=2 \\ a=16 & b=15 \end{array}$$

Now solve $\begin{cases} 23c & +15d & = & 11 \\ 18c & +4d & = & 14 \end{cases}$.

$$\begin{cases} 14a & +8b & = & 18 \\ 10a & +8b & = & 2 \end{cases}$$

$$4c = 16 \bmod 26$$

$$2c = 8 \bmod 13$$

$$c = 7 \times 2c = 14c = 7 \times 8 = 56 = 4 \bmod 13$$

So, *c* = 4 or *c* = 4 + 13 = 17 modulo 26.

If *c* = 4,

$$18 \times 4 + 4d = 14$$

$$20 + 4d = 14$$

$$4d = -6 = 20 \bmod 26$$

$$2d = 10 \bmod 13$$

$$d = 7 \times 2d = 7 \times 10 = 5 \bmod 13$$

So, *d* = 5 or *d* = 5 + 13 = 18 modulo 26.

If c = 17,

$$18 \times 17 + 4d = 14$$

$$20 + 4d = 14$$

and we are led to the same solutions for d.

$$\begin{array}{ll} c = 4 & d = 5 \\ c = 4 & d = 18 \\ c = 17 & d = 5 \\ c = 17 & d = 18 \end{array}$$

There are 16 possible 2×2 matrices that could be the key.

$$\begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix} \quad \begin{bmatrix} 3 & 2 \\ 4 & 18 \end{bmatrix} \quad \begin{bmatrix} 3 & 2 \\ 17 & 5 \end{bmatrix} \quad \begin{bmatrix} 3 & 2 \\ 17 & 18 \end{bmatrix}$$
$$\begin{bmatrix} 3 & 15 \\ 4 & 5 \end{bmatrix} \quad \begin{bmatrix} 3 & 15 \\ 4 & 18 \end{bmatrix} \quad \begin{bmatrix} 3 & 15 \\ 17 & 5 \end{bmatrix} \quad \begin{bmatrix} 3 & 15 \\ 17 & 18 \end{bmatrix}$$
$$\begin{bmatrix} 16 & 2 \\ 4 & 5 \end{bmatrix} \quad \begin{bmatrix} 16 & 2 \\ 4 & 18 \end{bmatrix} \quad \begin{bmatrix} 16 & 2 \\ 17 & 5 \end{bmatrix} \quad \begin{bmatrix} 16 & 2 \\ 17 & 18 \end{bmatrix}$$
$$\begin{bmatrix} 16 & 15 \\ 4 & 5 \end{bmatrix} \quad \begin{bmatrix} 16 & 15 \\ 4 & 18 \end{bmatrix} \quad \begin{bmatrix} 16 & 15 \\ 17 & 5 \end{bmatrix} \quad \begin{bmatrix} 16 & 15 \\ 17 & 18 \end{bmatrix}$$

In[1]:=

```
Solve[a + 3 b == 6 && 18 a + 9 b == 7, {a, b},
 Modulus → 26]
```

Out[1]=

```
{{a → 1, b → 19}}
```

In[2]:=

```
Solve[c + 3 d == 1 && 18 c + 9 d == 17, {c, d},
 Modulus → 26]
```

Out[2]=

```
{{c → 20, d → 11}}
```

In[3]:=

```
Solve[23 a + 15 b == 21 && 18 a + 4 b == 10,
 {a, b}, Modulus → 26]
```

Out[3]=

```
{{a → 3 + 13 C[1], b → 2 + 13 C[1]}}
```

In[4]:=

```
Solve[23 c + 15 d == 11 && 18 c + 4 d == 14,
 {c, d}, Modulus → 26]
```

Out[4]=

```
{{c → 4 + 13 C[1], d → 5 + 13 C[1]}}
```