Fall 2019
Chris Christensen
MAT/CSC 483
Section 9

Hill Cipher Cryptanalysis

A known plaintext attack means that we know a bit of ciphertext and the corresponding plaintext – a crib. This is not an unusual situation. Often messages have stereotypical beginnings (e.g., *to ..., dear ...*) or stereotypical endings (e.g, *stop*) or sometimes it is possible (knowing the sender and receiver or knowing what is likely to be the content of the message) to guess a portion of a message.

For a 2×2 Hill cipher, if we know two ciphertext digraphs and the corresponding plaintext digraphs, we can easily determine the key or the key inverse.

Example one:

Assume that we know that the plaintext of our ciphertext message that begins `WBVE` is `inma.` We could either solve for the key or the key inverse; let's solve for the key inverse.

Because `WB` corresponds to `in` $\begin{bmatrix} e & f \\ g & h \end{bmatrix}\begin{bmatrix} 23 \\ 2 \end{bmatrix} = \begin{bmatrix} 9 \\ 14 \end{bmatrix}$,

and because `VE` corresponds to `ma` $\begin{bmatrix} e & f \\ g & h \end{bmatrix}\begin{bmatrix} 22 \\ 5 \end{bmatrix} = \begin{bmatrix} 13 \\ 1 \end{bmatrix}$.

These result in two sets of linear congruences modulo 26:

$$\begin{array}{rcrcr} 23e & + & 2f & = & 9 \\ 22e & + & 5f & = & 13 \end{array}$$

and

$$\begin{array}{rcrcr} 23g & + & 2h & = & 14 \\ 22g & + & 5h & = & 1 \end{array}$$

We solve the systems modulo 26 using *Mathematica*.

```
In[5]:= Solve[23e+2f == 9 && 22e+5f == 13, {e, f}, Modulus -> 26]

Out[5]= {{e->1,f->19}}

In[6]:= Solve[23g+2h == 14 && 22g+5h == 1, {g, h}, Modulus -> 26]

Out[6]= {{g->20,h->11}}
```

Example two:

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:

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

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

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

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.

$$11a \quad = \quad 11$$

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

In[7]:= **Solve[a+3b == 6 && 18a+9b == 7, {a, b}, Modulus -> 26]**

Out[7]= {{a->1,b->19}}

In[8]:= **Solve[c+3d == 1 && 18c+9d == 17, {c, d}, Modulus -> 26]**

Out[8]= {{c->20,d->11}}

Example three:

Plaintext:

```
t h e p l a i n t e x t w o r d s a r e w r i t t e n i n s
m a l l l e t t e r s x
```

Ciphertext:

```
X P U V L A C B R A H N U K J N G C L S A Z O F R A H W B U
O E H D T U V X Y F C S
```

We are assuming that the plaintext was enciphered using a 2×2 Hill cipher.

We notice that ciphertext `UKJN` corresponds to plaintext `word`. We will use that relationship to solve for the key.

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

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.

$$\begin{cases} 23a & +15b & = & 21 \\ 18a & +4b & = & 10 \end{cases}$$

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.

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

We cannot “divide by 4” because 4 does not have an inverse modulo 26, but there is still hope for a solution.

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.

$$2a = 6 \bmod 13 \; 2a = 6 \bmod 13$$

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*.

Consider each case.

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.

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

When we check, only two of these are actually solutions of the system – all are solutions of the second congruence.

If we had substituted into the first congruence rather than the second, only two solutions would have resulted.

Using Mathematica:

```
In[9]:= Solve[23a+15b == 21 && 18a+4b == 10, {a, b}, Modulus -> 26]

Out[9]= {{a->3+13 C[1],b->2+13 C[1]}}
```

Notice that only two solutions resulted: a = 3 and b = 2 or a = 16 and b = 14.

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.

Consider each case.

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*.

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

Again, if we check these solutions, all are solutions of the second congruence, but only two are solutions of the system.

Using Mathematica:

```
In[1]:= Solve[23c+15d== 11 && 18c+4d == 14, {c, d}, Modulus -> 26]
```

```
Out[1]= {{c->4+13 C[1],d->5+13 C[1]}}
```

Again, Mathematica found only the two solutions of the system: c = 4 and d = 5 or c = 17 and s = 18.

So, there are 4 possible 2×2 matrices that could be the key.

First, calculate the determinant of each. Any matrix that does not have an invertible determinant modulo 26 (i.e., the determinant is not one of 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25 modulo 26) can be eliminated. (Two can be eliminated.)

Then calculate the inverse for each of the remaining two matrices and try to decipher the ciphertext with each of the inverses. The inverse that yields plaintext corresponds to the key.

Algebraic cipher

The Hill cipher is an algebraic cipher; there is an algebraic relationship between plaintext and ciphertext. That relationship can be exploited to determine the key.

To break a Hill cipher with a 2×2 key requires determining four entries – either the four entries of the key or the four entries of the key inverse. We can do that if we know the correspondence between plaintext and ciphertext for two digraphs because the correspondences will permit us to set up two systems of congruences – each system has two congruences of two unknowns.

To break a Hill cipher with a $n \times n$ key requires determining n^2 entries – the n^2 entries of the key or the n^2 entries of the key inverse. We can do that if we know the correspondence between plaintext and ciphertext for *n* *n*-graphs because the correspondences will permit us to set up *n* systems of congruences – each system has *n* congruences of *n* unknowns.

The reason that we can solve these systems of congruences is because they are linear and there is an efficient method for solving systems of linear equations – Gaussian elimination.