2.4 The Autokey cipher and cribs

2.4.1 Using a crib

One common tool in cryptanalysis is a *crib*, which is a known or guessed bit of plaintext corresponding to a ciphertext. (The term comes from the phrase "to crib notes" or "to crib an answer", meaning to copy or cheat on an assignment).

Often a crib can be used to dramatically simplify cryptanalysis. (In fact, frequency analysis is essentially an attempt to imitate a crib).

Cribs were famously used in Bletchley Park during World War II (where the term was coined). Many German Enigma operators used standardized terminology, including the regular use of the word *Wetter* ("weather") in weather reports, and one operator who repeatedly transmitted the message "Nothing to report".

Enigma operators were required to spell out all numbers, so Turing determined that the single most common word in messages was *eins*, meaning "one". Turing precomputed a catalog of what *eins* would look like encrypted in every possible position with various keys, which dramatically sped up decryption processes by seeing which of those were possible and judging them most likely.

You will notice that this is basically the same idea as frequency analysis: instead of taking common letters, we instead look for common words. *eins* was not enough to break messages on its own, but it could give substantial speedups and hints for other encryption messages.

2.4.2 Breaking the Autokey cipher

Cribs are an especially powerful tool in breaking the Autokey cipher, since the plaintext is *also* most of the keystream.

The basic idea is that we guess a word or phrase we expect to see in the plaintext. Since that word would also have to appear in the keystream, we try using that word as the key at every possible point, and see when the results are plausible English strings. We can extend this out to guess most or all of the message.

Example 2.14. Suppose we intercept the ciphertext:

`OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW`

We guess that it contains the word "the" somewhere. So we simply see what happens if we use "the" as the key at every possible position.

First we decrypt everything with an offset of zero:

Ciphertext:	O	O	F	I	K	A	A	Q	W	M	P	Q	U	M	X
Key:	T	H	E	T	H	E	T	H	E	T	H	E	T	H	E
Plaintext:	V	H	B	P	D	W	H	J	S	T	I	M	B	F	T
Ciphertext:	Z	X	Y	I	R	K	T	Z	S	P	G	M	G	P	K
Key:	T	H	E	T	H	E	T	H	E	T	H	E	T	H	E
Plaintext:	G	Q	U	P	K	G	A	S	O	W	Z	I	N	I	G
Ciphertext:	Q	M	I	P	L	C	N	W	X	K	E	N	Q	L	D
Key:	T	H	E	T	H	E	T	H	E	T	H	E	T	H	E
Plaintext:	X	F	E	W	E	Y	U	P	T	R	X	J	X	E	Z
Ciphertext:	I	R	F	S	N	I	J	A	M	G	P	W			
Key:	T	H	E	T	H	E	T	H	E	T	H	E			
Plaintext:	P	K	B	Z	G	E	Q	T	I	N	I	S			

A couple of these strings look like they might be English; we might notice "tim" or "aso". Let's see what happens if we assume "tim" is actually part of the plaintext. We now need to see what happens if we assume the original keyword is any of various lengths.

If the keyword has length four, we get

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW
--- --- --- --- --- --f bn- the -as o-- --- --- --- --- --- --- --- --- ---

--- --- --- --- --- --t he- aso -gu s-- --- --- --- --- --- --- --- --- ---
```

and while "gus" is possible, "fbn" probably is not.

If the keyword has length five, we get:

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW
--- --- --- --- --- -er e-- the --a so- --- --- --- --- --- --- --- --- ---

--- --- --- --- --- -th e-- aso --m ob- --- --- --- --- --- --- --- --- ---
```

This looks more promising, but if we continue building out we get:

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW
--- --- ono --m di- -er e-- the --a so- -mo b-- auo --- --- --- --- --- ---

--- --- mdi --e re- -th e-- aso --m ob- -au o-- ncj --- --- --- --- --- ---
```

which looks unlikely. With a key of length six we get

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW
--- --- --- --- --- gqu --- the --- aso --- --- --- --- --- --- --- --- ---

--- --- --- --- --- the --- aso --- gxw --- --- --- --- --- --- --- --- ---
```

Which again doesn't look like English. We can try longer keywords but nothing useful will show up. Similarly, we can try working with the "tim" but we won't really get anywhere.

So is this all the possibilities? No: the table we made started with "the" with an offset of zero from the ciphertext. We need to try again with offsets of one and two. If we build the table with an offset of two, we get

Ciphertext:	O	O	F	I	K	A	A	Q	W	M	P	Q	U	M	X
Key:	-	-	T	H	E	T	H	E	T	H	E	T	H	E	T
Plaintext:	-	-	M	B	G	H	T	M	D	F	L	X	N	I	E
Ciphertext:	Z	X	Y	I	R	K	T	Z	S	P	G	M	G	P	K
Key:	H	E	T	H	E	T	H	E	T	H	E	T	H	E	T
Plaintext:	S	T	F	B	N	R	M	V	Z	I	C	T	Z	L	R
Ciphertext:	Q	M	I	P	L	C	N	W	X	K	E	N	Q	L	D
Key:	H	E	T	H	E	T	H	E	T	H	E	T	H	E	T
Plaintext:	J	I	P	I	H	J	G	S	E	D	A	U	J	H	K
Ciphertext:	I	R	F	S	N	I	J	A	M	G	P	W			
Key:	H	E	T	H	E	T	H	E	T	H	E	T			
Plaintext:	B	N	M	L	J	P	C	W	T	Z	L	D			

We don't see anything terribly promising until we see past the wraparound; then we notice that the putative plaintext has "est" in it. So let's try assuming that's correct. With a keyword length of four we get

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW
--- --- --- -wj q-t he- est --- --- --- --- --- --- --- --- --- --- --- ---

--- --- --- -th e-e st- ezr --- --- --- --- --- --- --- --- --- --- --- ---
```

which doesn't look like English. So we try a key length of five:

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW
--- --- --- tim --t he- -es t-- --- --- --- --- --- --- --- --- --- --- ---
```

```
--- --- --- the --e st- -ns a-- --- --- --- --- --- --- --- --- --- --- ---
```

which looks like it could work. So we expand out another step, keeping in mind that we're guessing the keyword is length five so our keystream doesn't actually go earlier than the sixth character:

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW
--- --s o-- tim --t he- -es t-- nsa --- --- --- --- --- --- --- --- --- ---

so- --i m-- the --e st- -ns a-- com --- --- --- --- --- --- --- --- --- ---
```

This still looks good, so we fill out the rest:

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW
wa- --s o-- tim --t he- -es t-- nsa --c om- -ic a-- dan --h ea- -we r-- res

so- --i m-- the --e st- -ns a-- com --i ca- -da n-- hea --w er- -re s-- ple
```

At this point we just need to find any part of the message where we can make a guess to fill in the blanks, and we're done. We can try a few things, but perhaps we notice that the last part is "s– ple", which might be "simple". Guessing this and working backwards, we get:

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW
wat ers ome tim est heq ues tio nsa rec omp lic ate dan dth ean swe rsa res

som eti mes the que sti ons are com pli cat eda ndt hea nsw ers are sim ple
```

"Sometimes the questions are complicated, and the answers are simple."

3 Block Ciphers

Every encryption method we've studied so far has been a substitution cipher: that is, each letter is replaced by exactly one other letter. In fact, we've studied stream ciphers, which produce a keystream to add to the plaintext; there are substitution ciphers that don't work quite like that, but are still similar.

It is possible to make relatively secure substitution ciphers, but they are largely vulnerable

to the sorts of attacks we've been studying. But there is another class of cipher, called a *block cipher*, that behaves very differently. Rather than encrypting single letters, it encrypts entire blocks of letters at the same time.

3.1 Permutation Ciphers

Algorithm 3.1 (Permutation cipher)**.** *We choose a block size n, and as a key choose an element $k \in S_n$, which is a permutation on an alphabet of n letters.*

To encrypt, we break our plaintext into blocks of size n, padding the final block with nonsense characters if necessary. Then we permute each block according to the key k.

To decrypt, we take the inverse permutation k^{-1} and apply this to each ciphertext block.

Example 3.1. Suppose the plaintext is "Fourscore and seven years ago", and we choose a block length of 5 and a key of $k = (12345) \mapsto (23514)$. We write our message in blocks

`fours corea ndsev enyea rsago`

and then permute each block internally to get the ciphertext

`RFOSU ECOAR ENDVS EENAY GRSOA`.

To decrypt, we need to take the inverse permutation, which sends $(23514) \mapsto (12345)$ or $(12345) \mapsto (41253)$. Applying this inverse transformation returns to our original plaintext.

We can easily see that something like this approach is being used after conducting a frequency count: a frequency count on a message that has been encrypted by a permutation cipher will be the same as the frequency counts of the plaintext language.

Knowing even a small bit of the plaintext—that is, having a crib—is generally sufficient to break this cipher. (If I look through the above ciphertext, I see a place wehre one block has an "a" and the next has "n" and "d"; if I guess that this pieces together into "and", I can probably figure everything else out from there).

Without a crib, the most effective attacks involve looking for anagrams. In general, the cipher is not especially secure.

There are many variations on this idea, using more complex permutations and permuting between blocks as well as within them (which makes it no longer a true block cipher). We may return to that idea later, but for right now I want to discuss a more mathematically interesting cipher.

3.2 The Hill Cipher

3.2.1 Modular Arithmetic and Matrices

Before we can work with the Hill cipher, we need to recall a few extra facts about modular arithmetic.

Definition 3.2. Let m be a natural number. We write $\mathbb{Z}/m\mathbb{Z}$ for the set of all integers modulo m.

Definition 3.3. Given an integer a, an integer solution x to $ax \equiv 1 \mod m$ is called an *inverse of a modulo m.*

We're mostly going to concern ourselves with inverses modulo 26, since we're working in a 26-letter alphabet.

Example 3.4. What is the inverse of 5 modulo 26?

We notice that $5 \cdot 5 = 25 \equiv -1 \mod 26$, so $(5\cdot)^2 \equiv (-1)^2 \equiv 1 \mod 26$. Thus the inverse of 5 is $5^3 = 125 \equiv -5 \equiv 21 \mod 26$.

(Alternatively, we notice that $5 \cdot 5 \equiv -1 \mod 26$, so $5 \cdot (-5) \equiv 1 \mod 26$.

Fact 3.5. *An integer a has an inverse modulo m if and only if* $\gcd(a, m) = 1$.

Definition 3.6. A *matrix with coefficients in* $\mathbb{Z}/m\mathbb{Z}$ is a matrix all of whose entries are elements of $\mathbb{Z}/m\mathbb{Z}$. All operations are conducted modulo 26. We say such a matrix is an element of $M_n(\mathbb{Z}/m\mathbb{Z})$.

Recall that a matrix A over $\mathbb{R}$ is invertible if and only if $\det A \neq 0$. This is very nearly true for a matrix over $\mathbb{Z}/m\mathbb{Z}$, but the equivalent of "zero" is somewhat more common. What we actually need is a determinant that is invertible in $\mathbb{Z}/m\mathbb{Z}$.

Fact 3.7. *Let $A \in M_n(\mathbb{Z}/m\mathbb{Z})$. A is invertible if and only if* $\det A$ *has an inverse in $\mathbb{Z}/m\mathbb{Z}$, if and only if* $\gcd(\det A, m) = 1$.

There are two ways to find the inverse to a matrix. The first is to use a prepackaged formula. This formula for the inverse of a 2×2 matrix should be familiar:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \left(\det \begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}. \tag{3.1}$$

In this context, $\frac{1}{ad-bc}$ should be taken to be the inverse of $ad - bc$ modulo m. (And here we see why the determinant must have an inverse for the matrix to be invertible!)

The other alternative is to do a row reduction. We set up a block matrix $[A|I]$ with our matrix on the left and the identity on the right. We then row reduce; if we can row reduce until the left-side block is the identity, then our reduced matrix is $[I|A^{-1}]$ and the right-side block is our inverse. But again, all row operations should happen modulo m.

Example 3.8. Let's invert $A = \begin{bmatrix} 1 & 4 \\ 3 & 3 \end{bmatrix}$ modulo 26. We see the determinant is $3 - 12 = -9 \equiv 17 \mod 26$, and $\gcd(17, 26) = 1$, so this matrix is invertible.

The inverse of the determinant modulo 26 is $17^{-1} \equiv -3 \equiv 23 \mod 26$. (We can find this by counting up by 17s; we have 17, 34, 51, and notice that $51 \equiv -1 \mod 26$. Thus $17 \cdot 3 \equiv -1 \mod 26$ and so $17 \cdot (-3) \equiv 1 \mod 26$.) So we have

$$A^{-1} = 23 \begin{bmatrix} 3 & -4 \\ -3 & 1 \end{bmatrix} = \begin{bmatrix} 69 & -92 \\ -69 & 23 \end{bmatrix} \equiv \begin{bmatrix} 17 & 12 \\ 9 & 23 \end{bmatrix} \mod 26.$$

We can check that

$$\begin{bmatrix} 1 & 4 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} 17 & 12 \\ 9 & 23 \end{bmatrix} = \begin{bmatrix} 53 & 104 \\ 78 & 105 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mod 26.$$

Example 3.9. Let's invert $K = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 1 & 4 & 6 \end{bmatrix}$ modulo 26.

We don't have a formula here (we could look one up, but it's fiddly). We *can* compute the determinant:

$$\det K = 30 + 12 + 48 - (15 + 24 + 48) = 42 - 39 = 3$$

and so we see $\gcd(3, 26) = 1$ so the matrix is invertible.

To invert it we need to set up a block matrix.

$$\left[\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 4 & 5 & 6 & 0 & 1 & 0 \\ 1 & 4 & 6 & 0 & 0 & 1 \end{array}\right] \to \left[\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 0 & 2 & 3 & -1 & 0 & 1 \end{array}\right] \to \left[\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & 10 & -9 & 0 \\ 0 & 2 & 3 & -1 & 0 & 1 \end{array}\right]$$

$$\to \left[\begin{array}{ccc|ccc} 1 & 0 & -1 & -19 & 18 & 0 \\ 0 & 1 & 2 & 10 & -9 & 0 \\ 0 & 0 & -1 & -21 & 18 & 1 \end{array}\right] \to \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 2 & 0 & -1 \\ 0 & 1 & 0 & -32 & 27 & 2 \\ 0 & 0 & 1 & 21 & -18 & -1 \end{array}\right]$$

$$\to \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 2 & 0 & 25 \\ 0 & 1 & 0 & 20 & 1 & 2 \\ 0 & 0 & 1 & 21 & 8 & 25 \end{array}\right].$$

We can check that this is K^{-1}:

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 1 & 4 & 6 \end{bmatrix} \begin{bmatrix} 2 & 0 & 25 \\ 20 & 1 & 2 \\ 21 & 8 & 25 \end{bmatrix} = \begin{bmatrix} 105 & 26 & 104 \\ 234 & 53 & 260 \\ 208 & 52 & 183 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \mod 26.$$

Remark 3.10. Note, importantly, that we can't divide by numbers that don't have multiplicative inverses. So when working modulo 26 we can't divide by 2 or by 13, even if every number on the row is even.

3.2.2 The Cipher Algorithm

The Hill cipher was invented in 1929 by Lester Hill. It was implemented by a special machine that Hill had invented, using a complicated mechanical system to do all the linear algebra. It was a substantial advance at the time, but never achieved much use.

Algorithm 3.2 (Hill Cipher)**.** *We first choose a block size n. We choose a key, which is a $n \times n$ matrix K with entries in $\mathbb{Z}/26\mathbb{Z}$ (that is, integers modulo 26). We require that* $\gcd(26, \det K) = 1$.

We divide our message into blocks of length n. We write each plaintext block as a column vector $B \in (\mathbb{Z}/26\mathbb{Z})^n$. The corresponding ciphertext block is given by KB.

To decrypt, we compute K^{-1} in $\mathbb{Z}/26\mathbb{Z}$. Given a ciphertext block C, the corresponding plaintext block is $K^{-1}C$.

Example 3.11. Suppose we choose a block size of $n = 3$, and set our key to be the matrix we studied earlier:

$$K = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 1 & 4 & 6 \end{bmatrix}.$$

If we wish to encrypt the message `ABC` we first convert this to a column vector $[0, 1, 2]^T$. Then we compute

$$K \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 1 & 4 & 6 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 8 \\ 17 \\ 16 \end{bmatrix}$$

which corresponds to the ciphertext string `IRQ`.

To decrypt we need the matrix inverse of K, which fortunately we computed earlier:

$$K^{-1} = \begin{bmatrix} 2 & 0 & 25 \\ 20 & 1 & 2 \\ 21 & 8 & 25 \end{bmatrix}.$$

So to decrypt we compute

$$K^{-1}\begin{bmatrix}8\\17\\16\end{bmatrix} = \begin{bmatrix}2&0&25\\20&1&2\\21&8&25\end{bmatrix}\begin{bmatrix}8\\17\\16\end{bmatrix} = \begin{bmatrix}416\\209\\704\end{bmatrix} \equiv \begin{bmatrix}0\\1\\2\end{bmatrix}$$

which corresponds to our original plaintext of ABC.

Remark 3.12. Traditionally the ciphertext was written as a row vector and the encryption was computed as BK, which is effectively equivalent (but *not* interchangeable: $KB = (B^TK^T)^T$).

Example 3.13. For a longer example, let's take a block size of 2 and the key $K = \begin{bmatrix}3&1\\5&2\end{bmatrix}$. We have $\det K = 3\cdot 2 - 5\cdot 1 = 1$, and $\gcd(1,26) = 1$, so we know the matrix is invertible. We can in fact compute the inverse, either the long way:

$$\left[\begin{array}{cc|cc}3&1&1&0\\5&2&0&1\end{array}\right] \to \left[\begin{array}{cc|cc}1&9&9&0\\5&2&0&1\end{array}\right] \to \left[\begin{array}{cc|cc}1&9&9&0\\0&-43&-45&1\end{array}\right]$$
$$= \left[\begin{array}{cc|cc}1&9&9&0\\0&9&7&1\end{array}\right] \to \left[\begin{array}{cc|cc}1&0&2&-1\\0&9&7&1\end{array}\right]$$
$$\to \left[\begin{array}{cc|cc}1&0&2&25\\0&1&21&3\end{array}\right]$$
$$K^{-1} = \begin{bmatrix}2&25\\21&3\end{bmatrix} = \begin{bmatrix}2&-1\\-5&3\end{bmatrix}.$$

Or we can compute it the short way, by using equation (3.1), giving the same result.

Let's encrypt the message "It was a dark and stormy night." We first break the message up into blocks:

IT WA SA DA RK AN DS TO RM YN IG HT

Then we convert each letter into a number:

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

We read each pair as a column vector and multiply by K:

$$K\begin{bmatrix}8\\19\end{bmatrix} = \begin{bmatrix}43\\78\end{bmatrix} \equiv \begin{bmatrix}17\\0\end{bmatrix} \qquad K\begin{bmatrix}22\\0\end{bmatrix} = \begin{bmatrix}66\\110\end{bmatrix} \equiv \begin{bmatrix}14\\6\end{bmatrix}$$
$$K\begin{bmatrix}18\\0\end{bmatrix} = \begin{bmatrix}54\\90\end{bmatrix} \equiv \begin{bmatrix}2\\12\end{bmatrix} \qquad K\begin{bmatrix}3\\0\end{bmatrix} = \begin{bmatrix}9\\15\end{bmatrix} \equiv \begin{bmatrix}9\\15\end{bmatrix}$$

and repeating this process gives us the string

17-00 14-06 02-12 09-15 09-01 13-00 01-25 19-19 11-05 07-16 04-00 14-21

which gives the ciphertext string

`RA OG CM JP JA NA BZ TT LF HQ EA OV`.

3.2.3 Known-plaintext attacks

Unlike with a substitution or Vigenère cipher, it's not entirely trivial to recover the key even if you know a plaintext–ciphertext pair; but it is fairly easy. This makes cribs very powerful against a Hill cipher.

Suppose we again take a block size of two, and find that the plaintext message `how are you today` corresponds to the ciphertext `ZWS ENI USP LJVEU`. Converting this to numbers gives us the plaintext

07-14 22-00 17-04 24-14 20-19 14-03 00-24

and ciphertext

25-22 18-08 13-08 20-18 15-11 09-21 04-20

So how do we find the key $K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$?

We know the plaintext block 07-14 is sent to the ciphertext block 25-22. This gives us the equation

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 7 \\ 14 \end{bmatrix} = \begin{bmatrix} 25 \\ 22 \end{bmatrix}.$$

But this isn't, by itself, enough to find the matrix K.

If we look at the second pair, we get a similar equation

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 22 \\ 0 \end{bmatrix} = \begin{bmatrix} 18 \\ 4 \end{bmatrix}.$$

We can view this as a system of four linear equations in four variables; we can render this more compactly as

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 7 & 22 \\ 14 & 0 \end{bmatrix} = \begin{bmatrix} 25 & 18 \\ 22 & 4 \end{bmatrix}.$$

Unfortunately, we can't actually solve this system! In theory, we'd rearrange this to

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 25 & 18 \\ 22 & 4 \end{bmatrix} \begin{bmatrix} 7 & 22 \\ 14 & 0 \end{bmatrix}^{-1}.$$

But $\det \begin{bmatrix} 7 & 22 \\ 14 & 0 \end{bmatrix} = 0 - 14 \cdot 22 = -308$ and $\gcd(-308, 26) = 2 \neq 1$ so the matrix is not invertible. Thus in effect we have two equations in four variables, which isn't enough to solve

completely. (If somehow this was all the information you had, you could use it to seriously limit the space of possible keys to make any sort of brute-force search much easier).

But the problem is that these first two plaintext blocks happen to create a non-invertible matrix, which is relatively unlikely. So we can keep picking pairs of blocks until we find one that works.

We need to avoid determinants that are divisible by 2 or 13, which means we can't possibly use the second, fourth, or seventh blocks; we can't pair the first block with the third block either, but we can pair it with the fifth block. This gives us the equation:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 7 & 20 \\ 14 & 19 \end{bmatrix} = \begin{bmatrix} 25 & 15 \\ 22 & 11 \end{bmatrix}.$$

We compute

$$\begin{bmatrix} 7 & 20 \\ 14 & 19 \end{bmatrix}^{-1} = \frac{1}{7\cdot 19 - 14\cdot 20} \begin{bmatrix} 19 & -20 \\ -14 & 7 \end{bmatrix} = \frac{1}{-147} \begin{bmatrix} 19 & 6 \\ 12 & 7 \end{bmatrix} \equiv \frac{1}{9} \begin{bmatrix} 19 & 6 \\ 12 & 7 \end{bmatrix}$$
$$\equiv 3 \begin{bmatrix} 19 & 6 \\ 12 & 7 \end{bmatrix} = \begin{bmatrix} 57 & 18 \\ 36 & 21 \end{bmatrix} \equiv \begin{bmatrix} 5 & 18 \\ 10 & 21 \end{bmatrix} \mod 26.$$

Thus we have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 25 & 15 \\ 22 & 11 \end{bmatrix} \begin{bmatrix} 7 & 20 \\ 14 & 19 \end{bmatrix}^{-1} \equiv \begin{bmatrix} -1 & 15 \\ -4 & 11 \end{bmatrix} \begin{bmatrix} 5 & 18 \\ 10 & 21 \end{bmatrix} = \begin{bmatrix} 145 & 297 \\ 90 & 159 \end{bmatrix} \equiv \begin{bmatrix} 15 & 11 \\ 12 & 3 \end{bmatrix}.$$

Thus the key is $K = \begin{bmatrix} 15 & 11 \\ 12 & 3 \end{bmatrix}$. And we can check that indeed

$$\begin{bmatrix} 15 & 11 \\ 12 & 3 \end{bmatrix} \begin{bmatrix} 7 & 20 \\ 14 & 19 \end{bmatrix} = \begin{bmatrix} 259 & 509 \\ 126 & 297 \end{bmatrix} \equiv \begin{bmatrix} 25 & 15 \\ 22 & 11 \end{bmatrix} \mod 26.$$

3.2.4 Security

The Hill cipher is still vulnerable to frequency analysis-type attacks, but it makes them somewhat harder. Obviously single-letter frequencies are obscured; but if we take a Hill cipher with $n = 2$ then we can look for common bigraphs and run a frequency analysis on them; correctly identifying just two bigraphs will break the entire cipher. Similarly, to break a $n = 3$ Hill cipher we look at common trigraphs and need three to break the entire cipher.

Any "linear" cryptosystem is vulnerable to this sort of attack: if you can decrypt a small portion of the ciphertext, you can then decrypt the whole thing. For this reason, most cryptosystems are designed to be nonlinear.

3.3 Diffusion and Confusion

Claude Shannon gave two properties a good cryptographic method should have:

Definition 3.14. An encryption method has good *diffusion* if changing one character of the plaintext changes several characters of the ciphertext, and vice versa.

Definition 3.15. An encryption method has good *confusion* if the key does not relate straightforwardly to the ciphertext, but each part of the ciphertext depends on many parts of the key.

Thus diffusion means that changes in the plaintext are spread out through the ciphertext; while confusion means that changes in the key are spread out through the ciphertext. Each of these properties makes frequency analysis harder, since they increase the extent to which letters do not pair up one-to-one.

Simple substitution, Vigenère, and autokey ciphers have essentially no diffusion or confusion; each plaintext letter corresponds to one ciphertext letter, in a way mediated by one letter of the keyword. This makes them very susceptible to frequency analysis, as we saw in the homework.

The Hill cipher has better diffusion and confusion. Each letter of the ciphertext depends on an entire block of the plaintext, and an entire row of the key matrix. (It would be better if each letter of the ciphertext depended on the entire matrix).

This means that we had to do frequency analysis on n-grams instead of on individual letters, which is much harder. (We've mostly looked at cases where $n = 2$, but a realistic implementation would want much larger blocks). It also means that guessing "some" of the ciphertext doesn't actually give us any of the entries in the key.

Diffusion and confusion do have one major downside: error propagation. A small error in the ciphertext will make the decrypted plaintext drastically different, and possibly unreadable. But of course this is exactly the property that makes it hard to decrypt—that guessing it halfway doesn't give you enough information to finish the cryptanalysis.