2.13.5 The following ciphertext was encrypted by an affine cipher mod 26:

\[ CRWWZ \]

The plaintext starts with ha. Decrypt the message.

Sol.

Since the ciphertext corresponding to the plaintext "ha" \((7, 0)\) is "CR" \((2, 17)\) and the cipher is an affine cipher, we immediately have the following two equations:

\[
2 \equiv \alpha \cdot 7 + \beta \pmod{26} \\
17 \equiv \alpha \cdot 0 + \beta \pmod{26}
\]

The second equation says that \(\beta = 17\). Substitute back to the first equation, we have \(2 \equiv \alpha \cdot 7 + 17 \pmod{26}\), i.e. \(7 \cdot \alpha \equiv 11 \pmod{26}\).

Since \(\gcd(7, 16) = 1\), 7 has inverse in \(\mathbb{Z}_{26}^*\), i.e. \(7 \cdot 15 \equiv 1 \pmod{26}\).

Thus, \(\alpha \equiv 15 \cdot 11 \equiv 9 \pmod{26}\).

The encryption formula is \(Y \equiv 9 \cdot x + 17 \pmod{26}\).

The decryption formula is \(x \equiv 3 \cdot (Y - 17) \equiv 3Y + 1 \pmod{26}\).

Ciphertext W \(\rightarrow 22\), \(x \equiv 3 \cdot 22 + 1 \equiv 15 \pmod{26}\) \(\rightarrow\) plaintext p

Ciphertext Z \(\rightarrow 25\), \(x \equiv 3 \cdot 25 + 1 \equiv 24 \pmod{26}\) \(\rightarrow\) plaintext y

Plaintext: happy

2.13.8 Suppose that you want to encrypt a message using an affine cipher. You let \(a = 0, b = 1, \ldots, z = 25\), but you also include ? = 26, ; = 27, " = 28, ! = 29.

Therefore, you use \(x \mapsto ax + \beta \pmod{30}\) for your encryption function, for some integers \(a\) and \(\beta\).

(a) Show that there are exactly eight possible choices for the integer \(a\) (that is, there are only eight choices of \(a\) (with \(0 < a < 30\)) that allow you to decrypt).

(b) Suppose you try to use \(a = 10, \beta = 0\). Find two plaintext letters that encrypt to the same ciphertext letter.

Sol.
(a) Basically, the only usable values of $\alpha$ must satisfy $\gcd(\alpha, 30) = 1$ such that each ciphertext can be decrypted. Therefore, the number of possible values are those $\alpha$ being relatively prime to 30.

In terms of the Euler’s totient function, the number of possible values is $\phi(30) = \phi(5) \cdot \phi(6) = \phi(5) \cdot \phi(3) \cdot \phi(2) = 4 \cdot 2 \cdot 1 = 8$.

These values include $\{1, 7, 11, 13, 17, 19, 23, 29\}$.

(b) The encryption formula is $Y \equiv \alpha x + \beta \equiv 10x \pmod{30}$.

Note that $\gcd(30, 10) = 10$ implies that there must be 10 plaintext letters that map to the same ciphertext letter.

E.g.

For the plaintext ‘a’, $x = 0$, $Y \equiv 10 \cdot 0 \equiv 0$, ciphertext is ‘A’

To find the plaintext letters that map to the ciphertext ‘A’, we solve the congruence relation $0 \equiv 10 \cdot x \pmod{30}$

$\Rightarrow 0 \equiv x \pmod{10}$

$\Rightarrow x = 0, 3, 6, 9, 12, 15, 18, 21, 24, 27$ all satisfy $0 \equiv 10 \cdot x \pmod{30}$

For the plaintext ‘b’, $x = 1$, $Y \equiv 10 \cdot 1 \equiv 10$, ciphertext is ‘K’

To find the plaintext letters that map to the ciphertext ‘K’, we solve the congruence relation $10 \equiv 10 \cdot x \pmod{30}$

$\Rightarrow 1 \equiv x \pmod{10}$

$\Rightarrow x = 1, 4, 7, 10, 13, 16, 19, 22, 25, 28$ all satisfy $10 \equiv 10 \cdot x \pmod{30}$

For the plaintext ‘c’, $x = 2$, $Y \equiv 10 \cdot 2 \equiv 20$, ciphertext is ‘U’

To find the plaintext letters that map to the ciphertext ‘U’, we solve the congruence relation $20 \equiv 10 \cdot x \pmod{30}$

$\Rightarrow 2 \equiv x \pmod{10}$

$\Rightarrow x = 2, 5, 8, 11, 14, 17, 20, 23, 26, 29$ all satisfy $20 \equiv 10 \cdot x \pmod{30}$

2.13.17 Suppose the matrix $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ is used for an encryption matrix in a Hill cipher.

Find two plaintexts that encrypt to the same ciphertext.

Sol.

First, this is a block cipher scheme, the plaintext always means a block of plaintext letters (i.e. a pair of plaintext letters).

The determinant is $d = 4 - 3 \cdot 2 = -2$, is coprime to the modulus 26.

It can be expected that for each ciphertext block, there are $\gcd(26, 2) = 2$ plaintext blocks that map to it.

The encryption equation is

$$(Y_1, Y_2) \equiv (x_1, x_2) \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \pmod{26}$$

That is,

$$\begin{cases} Y_1 \equiv x_1 + 3x_2 \pmod{26} \\ Y_2 \equiv 2x_1 + 4x_2 \pmod{26} \end{cases}$$
Assuming that the second pair of plaintext that satisfies the same equation is \((x'_1, x'_2)\). Then,

\[
\begin{align*}
(x_1 - x'_1) + 3(x_2 - x'_2) &\equiv 0 \pmod{26} \\
2(x_1 - x'_1) + 4(x_2 - x'_2) &\equiv 0 \pmod{26}
\end{align*}
\]

Multiply the first equation by 2 and subtract the second equation from it, we obtain

\[2(x_2 - x'_2) \equiv 0 \pmod{26}\]

i.e. \(x_2 = x'_2\) or \(x_2 = x'_2 + 13\). If \(x_2 = x'_2\), then from the first equation, \(x_1 = x'_1\). This is a trivial case.

If \(x_2 = x'_2 + 13\), then from the first equation, \(x_1 = x'_1 + 13\).

From the above discussion, we note that any pair of plaintexts such that \(x_1 = x'_1 + 13\) and \(x_2 = x'_2 + 13\) would encrypt to the same ciphertext block. For example, \((a, b) \rightarrow (N, O), (b, i) \rightarrow (O, V), (s, k) \rightarrow (F, X), \ldots\)

2.14.7 The following was encrypted using the Vigenere method using a key of length at most 6. Decrypt it and decide what is unusual about the plaintext. How did this affect the results?

hdsfgemkoowawfweectenfthskacuhilgjofmaqgswatexqbyrsecfmrwsvr\nvnqszanoradgsakmlupsaffnudncyzyoaoqscacjkbrsevbelebkarsl\ncdsraannwryswxqvevlyeulwwwveaafgelaowafojdlhsfiksepoqymafo\nwbfcoseylqqxzygkmfegrgrgokfmgmhlnejabsjvymlnrqzcrgrchqegw\npcyfgtydycjkhqluhxgjzhqswpvdnbsffsenbxaaspqazmyuqhsfhmftayjxm\nwznrsafaoqgwaarmfitqsmahvqecv

(The ciphertext is stored in the downloadable computer files (see the Appendices) under the name hdsf. The plaintext is from Gadsby by Ernest Vincent Wright.)

\textbf{Sol.}

Using the MATLAB programs, you can estimate the length of the key, the key, the decipher the ciphertext.

(a) execute ciphertexts.m to define the hdsf

(b) for \(i = 1:12\)

\[
\text{coincidence}(i) = \text{coinc}(hdsf, i);
\]

end

\[
\text{coincidence} = 11 \ 14 \ 15 \ 25 \ 14 \ 15 \ 23 \ 15 \ 11 \ 6 \ 27
\]

Therefore, the length of key is very likely to be 4.

(c) for \(i = 1:4\)

\[
[y, key(i)] = \text{max}(vigvec(hdsf, 4, i));
\]

end

\[
key = key - [1 \ 1 \ 1 \ 1];
\]

\[
\text{keytext} = \text{int2text}(key)
\]
(d) The plaintext can be calculated by

\[ \text{plaintext} = \text{vigenere}(\text{hdsf}, [26 26 26 26] - \text{key}); \]

With this code, we can find out that the key is “noes”.

The decrypted ciphertext is:

\[ \text{uponthisbasisiamgoingtoshownowabunchofbrightyoungfolksd} \]
\[ \text{idfindachampionamanwithboysandgirlsofhisownamanof sodominating} \]
\[ \text{andhappyindividualitythatyouthisdrawntohimasisa flytoasu} \]
\[ \text{garbowlitisastoryaboutasmalltownisnotagossipyarnnorisit} \]
\[ \text{drymonotonousaccountfullofsuchcustomaryfillinsasromanticm} \]
\[ \text{oonlightcastingmurkysdownalongwindingcountryroad} \]

Let’s insert some spaces, punctuation and capitalize some characters for easier reading of this paragraph:

Upon this basis, I am going to show you how a bunch of bright young folks did find a champion aman.

With boys and girls of his own aman.

Of so dominating and happy individuality that you this drawn to him as is a fly to a sugar bowl.

It is a story about a small town.

It is not a gossipy yarn nor is it a dry monotonous account full of such customary fillins as romantic moonlight casting murky shadows down along winding country road.

You can use \textit{frequency(plaintext)} to further explore the letter frequency of the plaintext. The result is

\[ 35 6 9 14 0 9 12 15 34 0 2 13 12 31 41 5 0 13 28 25 15 1 10 0 14 0. \]

Notice that in this poem/prayer style English paragraph, the letter ‘e’ did not occur at all in these 344 character paragraph. This is different from a normal English paragraph. This implies that had we not used the correlation analysis in the crytanalysis of the key but used the first method treating the most frequently occurred letter as ‘e’, we would run into deep troubles.