Basic block ciphers

Bro. David E. Brown, BYU–Idaho Dept. of Mathematics. All rights reserved.

Version 0.21, of May 9, 2013

Introduction

In today’s world, information is more important than ever. Since much information needs to be kept private (or even secret), the business of keeping information secure is also more important than ever. The process of putting information in a (hopefully) secure form is called encryption\(^1\). Encrypted information can be stored (as when you back up your computer’s data) or shared with others (as it is in electronic commercial transactions). Either way, it has to be possible to decrypt\(^2\) the encrypted information, so as to return it to a readily usable form, when desired.

In this document, we will encrypt simple messages using matrix multiplication. Decrypting messages ought therefore to involve division, but since matrix division is not defined, we’ll multiply by inverse matrices, instead. So we’ll need invertible matrices.

Encryption

Let’s start with the simple message “encrypt this”. (For simplicity, we’re going to use all lower-case letters and ignore punctuation.) If we’re going to use matrices, we’ll need to convert our message to numbers. Here’s a quick way to do so:\(^3\)

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
<th>g</th>
<th>h</th>
<th>i</th>
<th>j</th>
<th>k</th>
<th>l</th>
<th>m</th>
<th>n</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>o</th>
<th>p</th>
<th>q</th>
<th>r</th>
<th>s</th>
<th>t</th>
<th>u</th>
<th>v</th>
<th>w</th>
<th>x</th>
<th>y</th>
<th>z</th>
<th>&lt;space&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
</tr>
</tbody>
</table>

Table 1: Converting letters (characters) to numbers

So the message “encrypt this” converts to “5 14 3 18 25 16 20 27 20 8 9 19”. This message has 12 numbers in it. Let’s arrange them in blocks\(^4\) of three (which divides evenly into 12), like so:

5 14 3 | 18 25 16 | 20 27 20 | 8 9 19.

(To distinguish the original message from its representation as a list of numbers, the original message is called the plaintext message.)

To be able to use matrix multiplication, let’s turn the blocks into column matrices:

\[
\begin{bmatrix}
5 \\
14 \\
3 \\
\end{bmatrix}
\quad
\begin{bmatrix}
18 \\
25 \\
16 \\
\end{bmatrix}
\quad
\begin{bmatrix}
20 \\
27 \\
20 \\
\end{bmatrix}
\quad
\begin{bmatrix}
8 \\
9 \\
19 \\
\end{bmatrix}
\]
Now we need an invertible matrix. Since the columns are all $3 \times 1$, we need an invertible $3 \times 3$ matrix. Here’s one: $E = \begin{bmatrix} 2 & 3 & 3 \\ 1 & 1 & 1 \\ 2 & 2 & 3 \end{bmatrix}$. This is where matrix multiplication comes in; it effects the actual encryption.

Let’s do it. We encrypt the letters “enc” at the beginning of the message by multiplying $E$ by the column
$$
\begin{bmatrix} 5 \\ 14 \\ 3 \end{bmatrix}
$$ and getting
$$
\begin{bmatrix} 61 \\ 22 \\ 47 \end{bmatrix}.
$$ Let’s do the same for the rest of the columns:
$$
\begin{align*}
E \begin{bmatrix} 18 \\ 25 \\ 15 \end{bmatrix} &= \begin{bmatrix} 159 \\ 59 \\ 134 \end{bmatrix} \\
E \begin{bmatrix} 20 \\ 27 \\ 20 \end{bmatrix} &= \begin{bmatrix} 181 \\ 67 \\ 154 \end{bmatrix} \\
E \begin{bmatrix} 9 \\ 19 \end{bmatrix} &= \begin{bmatrix} 100 \\ 36 \\ 91 \end{bmatrix}
\end{align*}
$$

Transposing the results and concatenating them gives us
$$
61 \ 22 \ 47 \ 159 \ 59 \ 134 \ 181 \ 67 \ 154 \ 100 \ 36 \ 91,
$$ which is the encrypted message.

**Decryption**

Decrypting a message that has been encrypted with this type of block cipher is pretty straightforward. Just undo what was done above. That is, take the encrypted message
$$
61 \ 22 \ 47 \ 159 \ 59 \ 134 \ 181 \ 67 \ 154 \ 100 \ 36 \ 91,
$$ break it up into columns (blocks) of three numbers each:
$$
\begin{bmatrix} 61 \\ 22 \\ 47 \end{bmatrix} \quad \begin{bmatrix} 159 \\ 59 \\ 134 \end{bmatrix} \quad \begin{bmatrix} 181 \\ 67 \\ 154 \end{bmatrix} \quad \begin{bmatrix} 100 \\ 36 \\ 91 \end{bmatrix},
$$

and then multiply the inverse $E^{-1}$ of the encryption matrix by each column. (Using the inverse matrix here exactly undoes that which multiplying by the encryption matrix did in the first place.) Well,

$$
E^{-1} = \begin{bmatrix} -1 & 3 & 0 \\ 1 & 0 & -1 \\ 0 & -2 & 1 \end{bmatrix},
$$

so multiplying gives us
$$
\begin{align*}
E^{-1} \begin{bmatrix} 61 \\ 22 \\ 47 \end{bmatrix} &= \begin{bmatrix} 5 \\ 14 \\ 3 \end{bmatrix} \\
E^{-1} \begin{bmatrix} 159 \\ 59 \\ 134 \end{bmatrix} &= \begin{bmatrix} 18 \\ 25 \\ 16 \end{bmatrix} \\
E^{-1} \begin{bmatrix} 181 \\ 67 \\ 154 \end{bmatrix} &= \begin{bmatrix} 20 \\ 27 \\ 20 \end{bmatrix} \\
E^{-1} \begin{bmatrix} 100 \\ 36 \\ 91 \end{bmatrix} &= \begin{bmatrix} 8 \\ 9 \\ 19 \end{bmatrix}
\end{align*}
$$

Transposing the results and concatenating them gives “5 14 3 18 25 16 20 27 20 8 9 19”. We can use Table 1 to recover the plaintext “encrypt me”.

**Comments:**

1. Because the message “encrypt me” had 12 characters in it (including the space) our encryption matrix could just as easily have been of size $4 \times 4$ or $6 \times 6$ as $3 \times 3$. But $5 \times 5$ would not have been so convenient: To disassemble a 12-character message into blocks of length 5 would give two blocks, with two characters left over. You can salvage such a situation by “padding” the message with extra characters, thus: “enxrcrypt qm”. Now there are fifteen characters in the message, so you can use a $5 \times 5$ encryption matrix, if desired. Padding messages like this has the advantage of allowing everyone involved to agree ahead of time on the size of encryption matrix to use, rather than letting the length of the message govern such things.
2. Basic block ciphers, as described above, are very easy to crack. In real life, people use far more sophisticated encryption methods than this one. However, matrix multiplication is so powerful that it is at the heart of almost all of the cryptographic methods in use today. Especially the most popular ones. Including those used to secure your electronic commercial transactions. And your bank account info. And your medical records. And your college transcript. And the files on your hard drive. And the codes needed for firing nuclear missiles. And so on.

3. How do you crack a basic block cipher? The chosen method depends on things we can’t go into, in this document. To keep this simple, we’ll assume you have acquired—by legal means—a message in both its encrypted and its numeric unencrypted forms.\(^5\)

(a) Determine the block size (maybe by trial and error). Let’s call the block size \(n\).

(b) Break up unencrypted version of the message into blocks of length \(n\). Do the same with the encrypted version.

(c) Fill an \(n \times n\) matrix with unknowns—as in \(E = \begin{bmatrix} a & p & x \\ b & q & y \\ c & r & z \end{bmatrix}\), for example.

(d) Take any \(n\) unencrypted blocks \(U_1, U_2, \ldots, U_n\) and their encrypted versions \(E_1, E_2, \ldots, E_n\), and set up the following systems of linear equations: \(EU_1 = E_1, EU_2 = E_2, \ldots, EU_n = E_n\). These systems all involve the entries of the unknown encryption matrix. This is different than what we’re used to doing, because the unknowns are in the coefficient matrix, instead of being in some column matrix.

(e) Your collection of \(n\) systems of \(n\) linear equations in \(n^2\) unknowns is really one big system. After all, you need to solve simultaneously all of the equations in all of those systems. So solve the big system to find all the unknown entries of the encryption matrix.

To do this, you might (say) multiply out the systems \(EU_1 = E_1, EU_2 = E_2, \ldots, EU_n = E_n\) to get \(n^2\) equations in \(n^2\) unknowns, rewrite this system as a single matrix multiplication, and then use the inverse of the \(n^2 \times n^2\) coefficient matrix to solve the system. (Other methods such as Gaussian elimination or the LU decomposition are acceptable in my classes, but I do require my students to use matrices. And save us both a lot of work by using a CAS!)

(f) Check your work in one or more of the following ways:

- Encode some of the unencoded blocks and compare your results to the corresponding known encoded blocks.
- Verify that your matrix \(E\) is invertible. (If it isn’t invertible, you can’t decode messages!)
- Having verified that \(E\) is invertible, use \(E^{-1}\) to decode some encoded blocks and compare your results to the corresponding unencoded blocks.

(g) Decode to your heart’s content.

4. If you use the above to crack a basic block cipher you got no business cracking, I’ll disown you mathematically, at the very least!

---

\(^5\) We’re leaving out significant details here, such as the fact that there are many ways to convert characters into numbers.