Introduction: The idea behind encryption is to take a message, called plaintext and encrypt (encode) it into a form called cipher-text so that if the cipher-text is intercepted, it cannot be read. Only the intended recipient has the means to correctly decrypt (decode) the cipher-text into plaintext. Plaintext should be easy to encrypt but for security reasons, cipher-text should be nearly impossible to decrypt without knowledge of the decryption algorithm.

What follows is a number of encryption systems.

Mono-alphabetic Substitution: A substitution is made for each plaintext letter. This can be easily seen by lining up the cipher alphabet under the plaintext alphabet.

```
plain alphabet  abcdefghijklmnopqrstuvwxyz
cipher alphabet JLPAXIQBCTRZYESKFGUXHNVM
```

The Caesar Shift Cipher: A form of monoalphabetic substitution where each plaintext letter is replaced by a cipher-text letter which is n positions away. For example, if n = 3, you substitute D for A, E for B, F for C etc (A for X, B for Y, C for Z).

```
plain alphabet  abcdefghijklmnopqrstuvwxyz
cipher alphabet DEFGHIJKLMNOPQRSTUVWXYZABC
```

Keyphrase Mono-alphabetic Substitution: Another variant is to use a key word or keyphrase to generate the cipher alphabet. For example, if JULIUS CAESAR is used as the key phrase, remove all spaces and repeated characters to obtain JULISCAER then beginning with the last letter (R) append the rest of the alphabet in their correct order, skipping over letters which already appear.

```
plain alphabet  abcdefghijklmnopqrstuvwxyz
cipher alphabet JULISCASRTVWXYZBDEFGHKMNOP
```

Mono-alphabetic substitutions are easy to implement but are not very secure since frequency analysis of cipher-text can be used to identify letters like ‘e’ and ‘s’ that occur more frequently in messages.

Poly-alphabetic Substitution - the Vigenère Cipher:

Blaise de Vigenère (b. 1523) French diplomat, Traité des Chiffres ("A Treatise on Secret Writing") pub 1586

One way to defeat the frequency analysis attack on mono-alphabetic substitution is to use multiple cipher alphabets. For example, if two cipher alphabets were used, substitutions would be made by alternating between cipher alphabets. Blaise de Vigenère in 1586 published a poly-alphabetic substitution method based on 26 cipher alphabet arranged into the so-called Vigenère Square. Each row is the alphabet shifted n place to the left with n being the row number.
### The Vigenère Square

<table>
<thead>
<tr>
<th></th>
<th>plain a b c d e f g h i j k l m n o p q r s t u v w x y z</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>B C D E F G H I J K L M N O P Q R S T U V W X Y Z A</td>
</tr>
<tr>
<td>2</td>
<td>C D E F G H I J K L M N O P Q R S T U V W X Y Z A B</td>
</tr>
<tr>
<td>3</td>
<td>D E F G H I J K L M N O P Q R S T U V W X Y Z A B C</td>
</tr>
<tr>
<td>4</td>
<td>E F G H I J K L M N O P Q R S T U V W X Y Z A B C D</td>
</tr>
<tr>
<td>5</td>
<td>F G H I J K L M N O P Q R S T U V W X Y Z A B C D E</td>
</tr>
<tr>
<td>7</td>
<td>H I J K L M N O P Q R S T U V W X Y Z A B C D E F G</td>
</tr>
<tr>
<td>8</td>
<td>I J K L M N O P Q R S T U V W X Y Z A B C D E F G H</td>
</tr>
<tr>
<td>9</td>
<td>J K L M N O P Q R S T U V W X Y Z A B C D E F G H I</td>
</tr>
<tr>
<td>10</td>
<td>K L M N O P Q R S T U V W X Y Z A B C D E F G H I J</td>
</tr>
<tr>
<td>12</td>
<td>M N O P Q R S T U V W X Y Z A B C D E F G H I J K L</td>
</tr>
<tr>
<td>13</td>
<td>N O P Q R S T U V W X Y Z A B C D E F G H I J K L M</td>
</tr>
<tr>
<td>14</td>
<td>O P Q R S T U V W X Y Z A B C D E F G H I J K L M N</td>
</tr>
<tr>
<td>15</td>
<td>P Q R S T U V W X Y Z A B C D E F G H I J K L M N O</td>
</tr>
<tr>
<td>16</td>
<td>Q R S T U V W X Y Z A B C D E F G H I J K L M N O P</td>
</tr>
<tr>
<td>17</td>
<td>R S T U V W X Y Z A B C D E F G H I J K L M N O P Q</td>
</tr>
<tr>
<td>19</td>
<td>T U V W X Y Z A B C D E F G H I J K L M N O P Q R S</td>
</tr>
<tr>
<td>20</td>
<td>U V W X Y Z A B C D E F G H I J K L M N O P Q R S T</td>
</tr>
<tr>
<td>22</td>
<td>W X Y Z A B C D E F G H I J K L M N O P Q R S T U V</td>
</tr>
<tr>
<td>23</td>
<td>X Y Z A B C D E F G H I J K L M N O P Q R S T U V W</td>
</tr>
<tr>
<td>25</td>
<td>Z A B C D E F G H I J K L M N O P Q R S T U V W X Y</td>
</tr>
<tr>
<td>26</td>
<td>A B C D E F G H I J K L M N O P Q R S T U V W X Y Z</td>
</tr>
</tbody>
</table>

To encrypt a message, choose a sequence of rows which are used to define the substitution of cipher letters for plaintext letter. The sequence of rows can be based on a key word or phrase. For example, the key word COMPSCI uses the rows beginning with C, O, M, P, S, C, and I to encrypt a message. For example

```plaintext
key phase  C O M P S C I C O M P S C I C O M P S C
plain text  w i t t e n b e r g u n i v e r s i t y
cipher text Y W F I W P J G F S J F K D G F E X L A
```

Decrypting is easy to do. In the row beginning with the key phase letter, locate the cipher-text letter. The corresponding plaintext letter is at the head of that column.

The advantage of the Vigenère cipher, unlike mono-alphabetical substitution, is that frequency analysis cannot be used to compromise the cipher. However, the Vigenere cipher can be broken. In 1854, Charles Babbage (called the **grandfather of computer science** because of his design of the **Analytic Engine**, a 19th century calculator which anticipated the modern computer) and in 1863 Friedrich Wilhelm Kasiski independently developed techniques to crack the Vigenere cipher. Kasiski published his work in *Die Geheimschriften und die Deschiffir-kunst* in 1863. Babbage's earlier work only came to light in the 20th century when his papers were examined. It's not clear why he failed to publish his results.

**Suggested Readings**

- *Code Breaking* by Rudolf Kippenhahn, Overlook Press 1999