Tyler Huber
Prof. Bruff
Cryptography

Wheatstone-Playfair Cipher

The Wheatstone-Playfair cipher, more commonly known as the Playfair cipher, is a digraphic cipher that, while invented by Charles Wheatstone in 1854, was popularized by his friend, Baron Lyon Playfair. The cipher itself is a block cipher that enciphers every pair of letters, hence the term digraphic, and comes with three rules for encryption. (Barr 16) The Playfair cipher was introduced around the same time Charles Babbage first broke the Vigenère. The Playfair, however, did not go far in claiming the sort of notoriety the Vigenère achieved; probably because breaking the Playfair is comparable in difficulty to the Vigenère, yet it was invented much later. Still, The Playfair cipher was implemented in military use, since it was faster to encipher than the Vigenère, and still took a fair amount of time to decipher. (*Playfair Cipher*)

Charles Wheatstone, inventor of the Playfair, was born near Gloucester in 1802, the son of a musician. He was raised to make and play instruments, and was in charge of a musical instrument shop for a period of his life. Although he made improvements to various instruments during that time, he was always more interested in the sciences, specifically in sound. He was responsible for many breakthroughs in the field of sound, including designing a rough version of a microphone, and, most notably, playing a major role in the development of the telegraph. (*Charles Wheatstone - Definition*)
Wheatstone seems to have simply created his digraphic cipher in his free time. He initially presented his scheme to the British Foreign Office to use in the military. The Foreign Secretary initially rejected it, claiming that encipherment was too complex. When Wheatstone argued that he could teach the cipher to a group of boys at a nearby

school in fifteen short minutes, the Foreign Secretary famously replied, “That is very possible, but you could never teach it to attaches.” (Singh, 378) Luckily for Wheatstone, his friend and neighbor, Baron Lyon Playfair, was Deputy Speaker of the House of Commons, postmaster general, a commissioner on public health, and was determined to convince the British Foreign Office of the cipher’s value. (Singh, 378) Most likely due to Playfair’s connections to Prince Albert and future Prime Minister Lord Palmerston, the cipher eventually used for warfare purposes, and was named after the man who popularized it. (*Playfair Cipher*)

The Playfair Cipher was used by the British for practical warfare communications purposes in the second Boer War and the First World War, and was used until the Second World War by the Australian military. Unlike the Vigenère, the Cipher was never considered unbreakable. However, when it was introduced, breaking a Playfair encoded message was still extremely tedious, especially with shorter messages. Therefore, due to the time consuming nature of the cipher, it was used in the military for information that was important, but not absolutely crucial. (*Playfair Cipher*)

The most famous use of the Playfair Cipher involved John F. Kennedy Jr. in 1943, when he was a Lieutenant in the United States Naval Reserve. A Japanese destroyer in the Solomon Islands had rammed Kennedy, and he used the Playfair Cipher to encrypt a message to an Australian Coastwatcher. The Coastwatcher decrypted the message with the keyword “ROYAL NEW ZEALAND NAVY”, and soon thereafter rescued Kennedy and his crew. (*Playfair Cipher*)

The Playfair cipher is the first true example of a digraphic cipher, meaning that each pair of letters is enciphered together, unlike the previous mono and poly-alphabetic

ciphers, in which each letter is enciphered by itself. Encipherment begins with a 5 x 5 square alphabet, with I and J used in the same square, so as to make an entire alphabet available. Sender and receiver must previously agree upon a common cipher square, based upon either a keyword or a pattern. Using a keyword, the cipher square is constructed the same way as a keyword cipher in a monoalphabetic substitution cipher would be. The keyword is written from left to right and top to bottom, taking out repeated letters in the keyword and filling in the rest of the alphabet in the square after the keyword. For example, if the keyword agreed upon were "**PLAYFAIR**", the resulting cipher square would be as follows.

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

The cipher square can also be based upon a pattern. For instance, if the agreed upon cipher square were constructed by typing out the alphabet in a counter-clockwise fashion, starting in the bottom right corner and ending in the center, the cipher square would look like the one below:

I/J	**H**	**G**	**F**	**E**
K	**V**	**U**	**T**	**D**
L	**U**	**Z**	**S**	**C**
M	**X**	**Y**	**R**	**B**
N	**O**	**P**	**Q**	**A**

Once a cipher square has been agreed upon, the plaintext must be broken up into digraphs before encipherment can begin. The rule in separating plaintext into digraphs is as follows: if any digraph has the same two letters, then an **x** is placed in between the letters. (Any uncommon letter, **q** for instance, can be used instead of **x**, **x** is simply the most commonly used.) The reason a digraph cannot have the same two letters is because the rules for encryption assume that the two letters in the digraph are in different blocks of the cipher square. Finally, if the plaintext ends in a single letter, another **x** is added to the very end. For instance, if the plaintext, "Professor Bruff is super" is used, the digraphic plain text would be as follows.

Plaintext: professor bruff is super

Digraphic Plaintext: pr–of–es–so–rb–ru–fx–fi–sx–su–pe-rx

Now that the plaintext is in digraphs, encipherment can begin. There are three rules used in conjunction with the cipher square to encrypt text. First, if the two letters in the digraph appear in the same row, then each letter is enciphered as the letter directly to the right of itself. If one of the letters in the Digraphic Plaintext happens to be in the far right column, then it wraps around and is enciphered as the letter in the first column in the corresponding row. For example, with the Digraphic Plaintext above in combination with the cipher square with keyword "playfair", the digraph **so** would become **TQ**. Next, if the letters appear in the same column, then the each letter is enciphered as the letter directly below itself. Following the pattern in the first rule, if a letter in the Digraphic Plaintext appears at the bottom of a row, then it is enciphered as the letter in the top row of the same column. Using the same parameters as before, the digraph **pe** becomes **IN**, and **sx** becomes **XY**. Finally, if the letters in the digraph are neither in the same row or

column, the letters will make a rectangle following their respective rows and columns. Each letter in the digraph is therefore encrypted as the letter in the corner of the rectangle of its same row. That is to say, each letter is replaced by the letter in its respective row and the other letter's column. If the same cipher square and digraphic text is used, **ru** will become **IV,** and **rx** is enciphered as **CV**. Following these three rules, any digraph can be encrypted. In sum, the message, "Professor Bruff is super" is encrypted in the following way.

Cipher Square with keyword: PLAYFAIR

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

Plaintext: professor bruff is super

Digraphic Plaintext: pr–of–es–so–rb–ru–fx–fi–sx–su–pe-rx

Ciphertext: LITLKNTQBCIVYZPDXYNXINCV

(Barr, 17)(Singh, 378)(Singh, *The Playfair Cipher*)

Deciphering the ciphertext is simple enough, as long as the cipher square is available. Decryption follows the same rules as encipherment, but in reverse. First, break the encrypted text into digraphs; there will be no double letters, so consideration of extra **x**'s is unnecessary. Then, each digraph is decrypted by shifting each letter in the opposite direction that it would be encrypted. Letters in the same row shift left, the same column shift up. When the letters in the digraph aren't in the same row or column, the text is deciphered the exact way it would be enciphered (this is because the third rule of encipherment is symmetric. That is to say, if the rule were to be treated as a function of a and b; we could say that if F(a,b)=(c,d), then F(c,d)=(a,b) for each and every (a,b)).

The easiest way of knowing that a certain ciphertext was encrypted using a Playfair is if there are no double letters in the digraphs. As said before, the Playfair was

never considered impossible to crack. Yet for a long time, cryptanalysis was discouraged since it was extremely time consuming. One way of breaking the Playfair is to use a frequency analysis of digraphs. The most common digraphs in a message encrypted using Playfair will most likely represent the most common double letters in the English language; namely **th** and **ea**. (*Decrypting Text*) Once parts of the plaintext are decrypted, the rest always becomes easier. Eventually enough of the cipher square may be available to recognize the keyword or pattern used. A downside, however, of using frequency analysis of digraphs is that it demands a fairly lengthy amount of Ciphertext to work with, since there are (25!/(25-2)!)-25=575 possible digraphs.

Another way to crack the playfair is called the "Shotgun Hill Climbing" method. At its extreme, the way current computers would tackle a Playfair, is to assign a random cipher square to the ciphertext. Then, change any letters around; if the resulting text seems more likely to be the plaintext, the new cipher square is adopted. This process continues until the true cipher square is found. While this process is absurdly impractical for human use, computers can accomplish this in a very short time, even with limited ciphertext. (*Shotgun Hill Climbing Definition*)

While the Playfair Cipher itself has become obsolete as a practical method of encryption since introduction of the computer, it is still used in puzzle books and other decryption games. Additionally, the basic principles of the Playfair can still be seen in modern computer block ciphers (Goren, 1). Although the Wheatstone-Playfair cipher never received much notoriety even in the cryptographic world, it not only marks a definite step forward in the world of practical encryption, but was the basis of numerous expansions in cryptography, some still seen today.

Works Cited

Barr, Thomas H. *Invitation to Cryptology*. Upper Saddle River, NJ: Prentice Hall, 2002. Print.

"Charles Wheatstone - Definition." *Dictionary, Encyclopedia and Thesaurus - WordIQ Dictionary*. Web. 28 Oct. 2010. <http://www.wordiq.com/definition/Charles_Wheatstone>.

"Decrypting Text." *Richard Knights*. Web. 28 Oct. 2010. <http://www.richkni.co.uk/php/crypta/freq.php>.

Goren, Ben. "The Playfair Cipher." *Trumpetpower.com*. 18 Aug. 2004. Web. 27 Oct. 2010. <http://trumpetpower.com/Papers/Crypto/Playfair>.

"Playfair Cipher." *Practical Cryptography*. James Lyons, 2009. Web. 28 Oct. 2010. <http://practicalcryptography.com/ciphers/playfair-cipher/>.

Shotgun Hill Climbing Definition of Shotgun Hill Climbing in the Free Online Encyclopedia." *Encyclopedia*. Web. 28 Oct. 2010. <http://encyclopedia2.thefreedictionary.com/Shotgun hill climbing>.

Singh, Simon. "Playfair Cipher." *SimonSingh.net*. Web. 27 Oct. 2010. <http://www.simonsingh.net/The_Black_Chamber/playfaircipher.htm>.

Singh, Simon. *The Code Book: the Science of Secrecy from Ancient Egypt to Quantum Cryptography*. New York: Anchor, 2000. Print.