Sam Mallick

Dr. Bruff

MATH 115-F: FYWS Cryptography

October 5, 2010

The Great Paris Cipher:
Napoleon's *Grand Chiffre*

In 1809, battle raged in the Iberian Peninsula between Napoleon's armies and the united forces of the British army, Portuguese army, and Spanish guerrillas. As the war went on with neither side gaining a clear advantage, the British and the French realized that there was a need to reform their respective message-sending systems. In this pursuit of better communication, the British and the French chose different methods of concealing sensitive information. The British created a corps of communications specialists, the Army's Guides, under the command of Captain (later promoted to Major) George Scovell. The British system relied on meticulously keeping track of their own messages while trying to obtain and interpret French messages. The French, on the other hand, were rather careless with their message carrying and compensated for this vulnerability by adopting ciphers. Most formidable of these was the Great Paris Cipher, introduced in 1811. The Great Paris Cipher was based on Louis XIV's *grand chiffre*, adapted for use by the military, relying on identical copies of a table containing many numbers in the possession of both the sender and the receiver. It should be noted that the "Cipher" was actually a hybrid between a code and a cipher. Technically, a cipher is symbol-for-symbol replacement while a code is word-for-word replacement. The Great Paris Cipher used numbers to replace words, individual letters, bigrams, and syllables (in this paper, I will refer to the encryption simply as a cipher to avoid complications). Such a cipher is much stronger than a monoalphabetic substitution cipher and easier to use than a polyalphabetic Vigenère with a constantly-changing keyword, making it seem ideal for military communications. In its implementation, however, the Great Paris Cipher was much less effective than the *grand chiffre* of Louis XIV, which was not broken for around 200 years.[1] Though the Great Paris Cipher was a theoretically strong cipher, there were inherent weaknesses that the French military built into its implementation which allowed Scovell to break it easily.

The French army under Napoleon was very formidable, but it did not make secrecy of information a high priority. It was not until General Jean Baptiste Franceschi was captured by Spanish guerrillas and an unencrypted letter he carried fell into the hands of the British that the French army considered introducing a Peninsula-wide cipher system.[2] While Napoleon is generally regarded as one of the greatest military leaders of all time, he was notoriously lacking in one important area of the military—cryptography. In *The Codebreakers*, David Kahn writes, "That military genius [Napoleon], though not quite the cryptologic moron that it has been the fashion to portray him as being, certainly did not fully appreciate the importance of a tough cryptography. He depended upon a single, easy-to-solve system during most of his campaigns."[3] The simplicity of Napoleon's usual ciphers allowed his enemies to easily break them. Russian cryptographers under Czar Alexander I broke the ciphers Napoleon used in his Russian campaign,[4] and until the capture of Franceschi in the Peninsular wars, Napoleon's Army of Portugal had no cipher that was

[1] Singh, Simon, *The Code Book* (New York: Anchor Books, 2000), 57.
[2] Urban, Mark, *The Man Who Broke Napoleon's Codes: The Story of George Scovell* (London: Faber and Faber, 2001), 59.
[3] Kahn, David, *The Codebreakers: The Story of Secret Writing* (New York: Scribner, 1980), 617.
[4] Kahn, *The Codebreakers*, 618.

common to all regiments. Marshall Maramont, who took command of the Army of Portugal in May of 1811, introduced a cipher, known simply as the Army of Portugal Cipher, to streamline communication amongst his forces. The cipher table consisted of 150 numbers. Because of the small size of the cipher table, the Army of Portugal Cipher was known as a *petit chiffre*; its simplicity allowed Scovell to break it relatively easily.

The Great Paris Cipher, however, proved to be much more formidable. After the failure of the Army of Portugal Cipher, Napoleon's armies adapted a 1,200-number diplomatic cipher, forming a 1,400-word military cipher. This was the first time that the most scientifically advanced and well-organized military force in the world used a cipher table with over 200 numbers.[5] The strength of this new cipher, however, indirectly gave the British more access to French mail. A major weakness in communication of the French armies in general was carelessness with messages; French messages had a habit of falling into British hands, and after the introduction of the Great Paris Cipher, Napoleon became overconfident in the strength of his encryption, sending messages "of the utmost importance in the hands of some local peasant."[6] As with any form of cipher, access to more ciphertext creates a greater chance of successful frequency analysis. Thus, the British benefitted from each captured message. Even with copious ciphertext, however, the Great Paris Cipher was very difficult to break.

For the sake of simplicity, we will use a hypothetical cipher in English to create a picture of what the Great Paris Cipher looked like. The cipher table contained 1,400 numbers. Of these, the last 200 were assigned to words specifically related to the Peninsular War. The rest of the numbers were assigned in a few different categories. Some were

[5] Urban, *The Man Who Broke Napoleon's Codes*, 128.
[6] Urban, *The Man Who Broke Napoleon's Codes*, 129

common words, such as “the,” “and,” and “or.” Relevant names and words, for instance “Napoleon,” “Britain,” or “artillery” would also have numbers assigned to them. In addition, common syllables and frequently appearing bigrams (also called digraphs), such as “th” and “el” would have individual numbers. We would not assign any meaning to some numbers, which could be placed randomly throughout the cipher to throw off the cryptographer; the rest of the cipher table was composed of single letters, each letter appearing multiple times in proportion to its frequency. In our hypothetical cipher, we might pick 15 random numbers for “e,” 12 for “a” and “t,” ten for “o,” “i,” and “n,” and so on until we get to two numbers each for “x,” “z,” and “q/qu.” While it might seem tedious to use a cipher table to encipher and decipher large quantities of text, the benefits of such a cipher are great. If the sender encrypts properly, using different numbers randomly to encipher the same letter, frequency analysis becomes very difficult because each number will appear roughly the same number of times. Thus, instead of seeing 30 occurrences of a single symbol that represents “e,” the decipherer sees two occurrences of 15 different symbols, with no way of knowing that they all represent the same letter.

Another great benefit of the cipher is the ability to encipher one word many different ways. For instance, say we wanted to use our hypothetical cipher to encipher a message containing information about Mississippi. It is very likely that the word “Mississippi” will appear multiple times in the document, so we want to encipher it differently every time. The *grand chiffre* gives us many options. Using the single-number code:

1253
"Mississippi"

The word can also be enciphered letter-by-letter:

10.42.300.428.69.808.746.478
"m" "i" "s" "s" "i" "p" "p" "i"

Or we can encipher it using bigrams and single letters:

```
820.5.203.19.746.553
“mi” “ss” “is” “si” “p” “pi”
```

If “m” can be enciphered with three different numbers, “i” with ten, “s” with eight, and “p” with two, we can calculate the number of ways the whole word can be ciphered using just single-letter substitutions:

3 x 10 x 8 x 8 x 10 x 8 x 8 x 10 x 2 x 2 x 10 = 491,520,000

This is the number of unique ways to encipher “Mississippi” using only single letters. However, we do not need to include this word so many times, and doing so would create some form of repetition if we used the same numbers too frequently. In reality, we have fewer feasible options but still enough to confuse the cryptographer, especially if we use bigrams and syllables. If the cipher is used properly, meaning numbers spread out evenly and randomly, a cryptographer’s only way in is to take an educated guess based on some discrepancy in frequency. Even if the cryptographer should guess that a certain number represents “s,” which he has an 8/1,400 chance of doing correctly, he still does not know which other seven numbers represent “s” or what the numbers around his deciphered “s” mean. Furthermore, as long as the cryptographer has no reason to suspect that the message is about Mississippi, he has no crib, or idea of what the cipher text is meant to say.

Such a crib was exactly what Scovell needed; without something to latch onto, he had little hope of breaking the cipher. The French army, however, gave him many cribs in each message because it was standard practice to only partially encipher messages. The French senders included strings of plaintext in their messages to make the ciphering and deciphering process faster. This, however, gave Scovell a very important tool in his cryptanalysis: context. By using what he knew from the plaintext in the message, Scovell could extrapolate the meaning of other parts of the message. It would be as if we sent our encoded message about Mississippi and did not encode references to Jackson, the state capitol. Such a crib may be enough to allow a cryptanalyst to break a cipher, no matter how great the table. The ability to make an educated guess as to the meaning of the ciphertext gave Scovell a good place to begin his assault on the cipher, which would have otherwise been next to impossible: "It would seem at first sight that to interpret such a dispatch would be a perfectly hopeless task, to any one who had not the key to the cipher before him...[Scovell] was started on the track by the fortunate circumstance that most of the intercepted dispatches were only *partly* in cipher."[7] Solely by using the context of the message and information gathered by British intelligence, Scovell was able to discern parts of messages: "I received your letter of – July: it is unfortunate that you were not able to attack 1214.609.656.803. occupied 58.850.112.1168.13.1388.1153.820." became "I received your letter of – July: it is unfortunate that you were not able to attack the English army while they were occupied with the siege of 1168 of Salamanca."[8] Such a breakthrough was possible because of the partial enciphering of the message. Scovell's ability to decipher this and other messages came not from frequency analysis or mathematical calculation but from his knowledge of the French language.[9] Using his understanding French syntax and grammar, Scovell could determine what the code numbers represented in context.

[7] Oman, Charles, *A History of the Penninsular War* (New York: AMS Press, 1996), 613.
[8] Urban, *The Man Who Broke Napoleon's Codes*, 202.
[9] Urban, *The Man Who Broke Napoleon's Codes*, 163.

A cipher that does not include any plaintext is much more effective than one that does. Decryption of such a cipher would, however, require much guessing based on the frequency of letters, syllables, and whole words in the French language in the context of a war in Iberia. This would be exceedingly difficult for a cryptanalyst on a battlefield and would have ensured the safety of the Great Paris Cipher much longer. Cryptography is a battle of information—the cryptographer is trying to conceal information, the cryptanalyst is trying to discover it. When the cryptographer gives away information about his cipher system or his ciphered message, the cryptanalyst has more power to break the cipher. Essentially, the French military created cribs in what should have been an incredibly successful cipher, allowing it to be broken. With the plaintext revealed, Wellington used the information to aid in his defeat of the French in Iberia. In one message, Wellington was alerted that the French armies were in no position to launch an offensive, alerting Wellington that he would be able to plan his own; in another message, the British learned that the specifics of the French position near the Duero and Tagus rivers.[10] Though the exact extent of the effect of Scovell's information through the course of the campaigns cannot be known (due to lack of recorded information as well as an historical trend of cryptographers who do not receive proper recognition for their work) Scovell certainly helped Wellington's war efforts. "[Scovell's codebreaking's] influence on Wellington's strategy is obvious at times, even explicit in some of his dispatches."[11]

The success of Scovell's cryptography became somewhat short-lived, though, when a group of Spaniards attacked a French caravan and discovered a copy of the large cipher table.[12]

[10] Urban, *The Man Who Broke Napoleon's Codes*, 248.
[11] Urban, *The Man Who Broke Napoleon's Codes*, 287.
[12] Urban, *The Man Who Broke Napoleon's Codes*, 242.

The capture of such a table merely confirmed the work Scovell had done over the past months and ultimately helped the French; they realized that their cipher had been taken and was no longer secure.[13] Scovell's skills proved useful again, however, when he came up with a system that was nearly impregnable for the British army to use. He gave the same edition of a pocket dictionary to two headquarters; the code would be based on the location of words in these dictionaries, so 134A18 translates to page 134, column A, row 18.[14] While a substantial amount of frequency analysis could be used to break such a code, the British had less need to send messages than the French and were much more careful with the messages they did send. Therefore, the French were less likely to obtain enough ciphertext to perform successful frequency analysis.

Ultimately, the French Army's poor implementation of a strong cipher was detrimental to their cause. Napoleon's belief that his cipher was impregnable led him to send messages freely and carelessly; overconfidence in a cipher's strength can be worse than no cipher at all. The British system of communication proved to be much more effective than the French; The British were very careful with their messages and put a high priority on intercepting and interpreting information sent by the French. The failure of French cryptography in the Peninsular Wars is an example of how overconfidence and generally careless communication can change the outcome of a war. The Great Paris Cipher is only one of many examples of ciphers broken because of carelessness and overconfidence. While a cipher may be theoretically strong, it is only practically as strong as the sender makes it. While the Great Paris Cipher was indeed a strong method of encryption, the British proved that strength of a cipher system is not as important as proper implementation of that cipher.

[13] Crowdy, Terry, *The Enemy Within: A History of Espionage*, (New York: Osprey, 2006), 156.
[14] Urban, *The Man Who Broke Napoleon's Codes*, 233.

Works Cited

Crowdy, Terry. *The Enemy Within: A History of Espionage*. New York: Osprey, 2006. Accessed October 26, 2010. http://books.google.com.

Kahn, David. *The Codebreakers: The Story of Secret Writing*. New York: Scribner, 1996.

Oman, Charles. *A History of the Peninsular War*. New York: AMS Press, 1980.

Singh, Simon. *The Code Book*. New York: Anchor Books, 2000.

Urban, Mark. *The Man Who Broke Napoleon's Codes: The Story of George Scovell*. London: Faber and Faber, 2001.