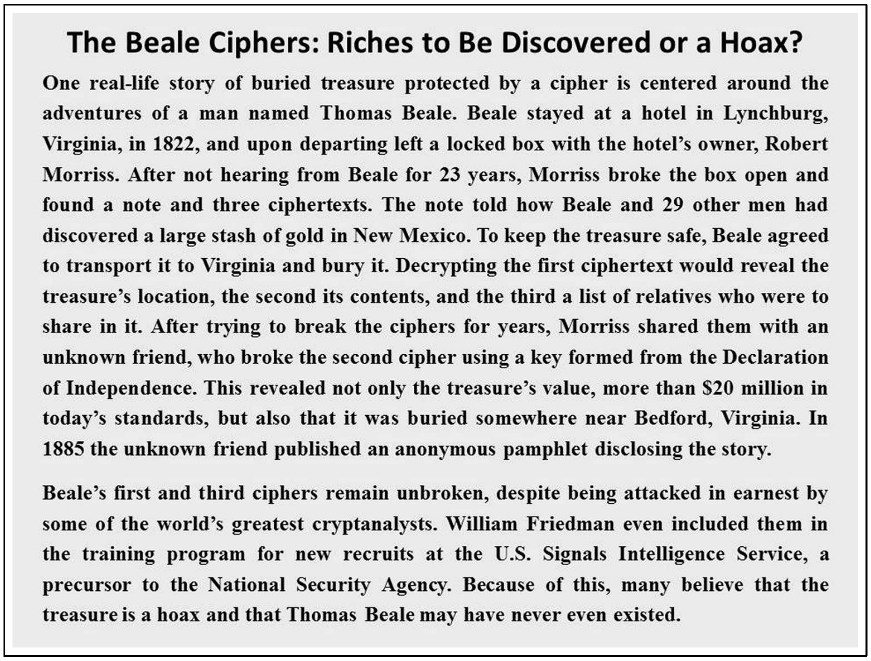
5. Find some information about the encrypted messages sent by the Zodiac killer to the San Francisco Bay area press in 1969–70, and write a summary of your findings.

2.3 Playfair Ciphers

Substitution ciphers would be less susceptible to attack by frequency analysis if plaintext characters were encrypted in pairs (i.e., digraphs). This is the basis for *Playfair* ciphers. Playfair ciphers were first described in 1854 by English scientist and inventor Sir Charles Wheatstone, but are named for Scottish scientist and politician Baron Lyon Playfair, Wheatstone's friend, who argued for their use by the British government. Although initially rejected because of their perceived complexity, Playfair ciphers were eventually used by the British military during the Second Boer War and World War I, and by British intelligence and the militaries of several countries, including both the United States and Germany, during World War II.

Playfair ciphers use one or more keywords. Spaces and duplicate letters in the keyword(s) are removed, and the resulting letters are then used to form an array of letters, similar to the array used in keyword columnar substitution ciphers, except that for Playfair ciphers this array must always



The Beale Ciphers: Riches to Be Discovered or a Hoax?

One real-life story of buried treasure protected by a cipher is centered around the adventures of a man named Thomas Beale. Beale stayed at a hotel in Lynchburg, Virginia, in 1822, and upon departing left a locked box with the hotel's owner, Robert Morriss. After not hearing from Beale for 23 years, Morriss broke the box open and found a note and three ciphertexts. The note told how Beale and 29 other men had discovered a large stash of gold in New Mexico. To keep the treasure safe, Beale agreed to transport it to Virginia and bury it. Decrypting the first ciphertext would reveal the treasure's location, the second its contents, and the third a list of relatives who were to share in it. After trying to break the ciphers for years, Morriss shared them with an unknown friend, who broke the second cipher using a key formed from the Declaration of Independence. This revealed not only the treasure's value, more than $20 million in today's standards, but also that it was buried somewhere near Bedford, Virginia. In 1885 the unknown friend published an anonymous pamphlet disclosing the story.

Beale's first and third ciphers remain unbroken, despite being attacked in earnest by some of the world's greatest cryptanalysts. William Friedman even included them in the training program for new recruits at the U.S. Signals Intelligence Service, a precursor to the National Security Agency. Because of this, many believe that the treasure is a hoax and that Thomas Beale may have never even existed.

have exactly five letters per row. Also, I and J are considered to be the same letter in Playfair arrays, so J is not included. The reason for this is so that Playfair arrays will always form perfect squares of size 5×5. (That is, Playfair arrays will always have exactly five rows and five columns.)

Example 2.5 Consider a Playfair cipher with keyword WHEATSTONE. Removing the duplicate letters in this keyword gives WHEATSON, and using these letters to form the array for a Playfair cipher yields the following.

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

We will use a Playfair cipher with this array to encrypt a message in Example 2.7. □

To encrypt a message using a Playfair cipher, spaces are removed from the plaintext, and the plaintext is then split into digraphs. If any digraphs contain repeated letters, an X is inserted in the plaintext between the first pair of repeated letters that were grouped together in a digraph, and the plaintext is again split into digraphs. This process is repeated if necessary and as many times as necessary until no digraphs contain repeated letters. Finally, if necessary, an X is inserted at the end of the plaintext so that the last letter is in a digraph.

Example 2.6 Consider the message IDIOCY OFTEN LOOKS LIKE INTELLIGENCE. To encrypt this message using a Playfair cipher, we begin by splitting the plaintext into digraphs. This yields the following.

ID IO CY OF TE NL OO KS LI KE IN TE LL IG EN CE

The seventh digraph is the first one that contains repeated letters. Thus, we insert an X between these letters and again split the plaintext into digraphs. This yields the following.

ID IO CY OF TE NL OX OK SL IK EI NT EL LI GE NC E

None of these digraphs contain repeated letters, but now we must insert an X at the end of the plaintext so that the last letter will be in a digraph. This yields the following.

ID IO CY OF TE NL OX OK SL IK EI NT EL LI GE NC EX

We are now ready to encrypt this message using a Playfair cipher, which we will do in Example 2.7. □

In a Playfair cipher, the 5 × 5 array of letters is used to convert plaintext digraphs into ciphertext digraphs according to the following rules.

- If the letters in a plaintext digraph are in the same row of the array, then the ciphertext digraph is formed by replacing each plaintext letter with the letter in the array in the same row but one position to the right, wrapping from the end of the row to the start if necessary. For example, using the array in Example 2.5, the plaintext digraph ID encrypts to the ciphertext digraph KF, and IK encrypts to KD.

- If the letters in a plaintext digraph are in the same column of the array, then the ciphertext digraph is formed by replacing each plaintext letter with the letter in the array in the same column but one position down, wrapping from the bottom of the column to the top if necessary. For example, using the array in Example 2.5, OF encrypts to FM, and EX encrypts to NE.

- If the letters in a plaintext digraph are not in the same row or column of the array, then the ciphertext digraph is formed by replacing the first plaintext letter with the letter in the array in the same row as the first plaintext letter and the same column as the second plaintext letter, and replacing the second plaintext letter with the letter in the array in the same row as the second plaintext letter and the same column as the first plaintext letter. For example, using the array in Example 2.5, IO encrypts to FB, and OX encrypts to NV.

Example 2.7 The Playfair cipher with keyword WHEATSTONE (for which the array is given in Example 2.5) encrypts the plaintext IDIOCY OFTEN LOOKS LIKE INTELLIGENCE as follows.

Plain: ID IO CY OF TE NL OX OK SL IK EI NT EL LI GE NC EX
Cipher: KF FB BZ FM WA SP NV CF DU KD AG CE WP QD PN BS NE

For decryption, the rules for encryption are reversed. (The first decryption rule is identical to the first encryption rule except letters one position to the left are chosen, wrapping from the start of the row to the end. The second decryption rule is identical to the second encryption rule except letters one position up are chosen, wrapping from the top of the column to the bottom. The third decryption rule is identical to the third encryption rule.) □

For cryptanalysis, because Playfair ciphers encrypt digraphs, single-letter frequency analysis is in general not helpful. (Note in Example 2.7 the plaintext letters I and O both correspond to four different ciphertext letters.) However, when used to encrypt long messages, it is sometimes possible to break Playfair ciphers using frequency analysis on digraphs, since identical plaintext digraphs will always encrypt to identical ciphertext digraphs.

Other weaknesses are that a plaintext digraph and its reverse (e.g., AB and BA) will always encrypt to a ciphertext digraph and its reverse, and that for short keywords the bottom rows of the array may be predictable.

2.3 Exercises

1. Consider a Playfair cipher with keyword SEINFELD.

   (a) Use this cipher to encrypt THE SMELLY CAR.

   (b) Use this cipher to encrypt THE BIZARRO JERRY.

   (c) Decrypt QMSHKZHCILKBXARBIY, which was formed using this cipher.

2. Consider a Playfair cipher with keywords CLINT EASTWOOD.

   (a) Use this cipher to encrypt DIRTY HARRY IS A CLASSIC.

   (b) Use this cipher to encrypt A FISTFUL OF DOLLARS IS GOOD TOO.

   (c) Decrypt ORAEZCABSNEWWUOSCAFSAFOCCOQZOC, which was formed using this cipher.

3. Create a Playfair cipher and use it to encrypt a plaintext of your choice with at least 20 letters.

4. In Walt Disney Pictures’ 2007 movie *National Treasure: Book of Secrets*, a man named Thomas Gates (the great-great-grandfather of treasure hunter Benjamin Franklin Gates, the main character in the movie) is asked by John Wilkes Booth and a colleague to decrypt the ciphertext MEIKQOTXCQTEZXCOMWQCTEHNFBIKMEHAKRQCUNGIKMAV, which was formed using a Playfair cipher with keyword DEATH. Decrypt this ciphertext.

5. On August 2, 1943, Japanese destroyer *Amagiri* rammed and sank American patrol boat PT-109, which was under the command of U.S. Naval Reserve Lieutenant and future President John F. Kennedy. After reaching shore, Kennedy sent the following ciphertext, which was formed using a Playfair cipher with keywords ROYAL NEW ZEALAND NAVY. Use the Playfair cipher Maplet to decrypt this ciphertext.

   ```
   KXIEYUREBEZWEHEWRYTUHEYFSKREHEGOYFIWUQUTQYOMUQYCAIPOB
   OTEIZONTXBYBNTGONEYCUZWRGDSONSXBOUYWRHEBAAHYUSEDQ
   ```

6. Find a copy of Dorothy Sayers’ novel *Have His Carcase*, and write a summary of how a Playfair cipher is integrated into the story and the steps described in it for breaking a Playfair cipher.

7. A description of cryptanalysis of Playfair ciphers can be found in U.S. Army Field Manual 34-40-2 [28]. Find a copy of this manual, and write a summary of how it describes Playfair cipher cryptanalysis.

8. Find some information about two-square and four-square ciphers, and write a summary of your findings.

9. Find some additional information about the Beale ciphers, and write a summary of your findings.

2.4 The Navajo Code

While simple substitution ciphers are not very secure, and even ciphers such as Playfair that substitute for digraphs can be broken through a type of frequency analysis on longer ciphertexts, not all ciphers based on substitution alone are easy to break. The Navajo code, a cipher famously created by Native Americans, primarily from the Navajo Nation that occupies a large region of Utah, Arizona, and New Mexico, and used effectively by the Americans throughout the Pacific Campaign during World War II, was essentially a substitution cipher. The Navajo language was at the time exclusively oral, very complex, and unknown to virtually everyone outside the Navajo Nation. The idea of using Navajos basically speaking their native language as a means for encrypting messages originated in 1942 with a man named Philip Johnston. Having grown up the son of a missionary to the Navajo, Johnston was very familiar with the Navajo culture, and was one of only a handful of non-Navajos who spoke the Navajo language fluently.

Johnston was a veteran of World War I, where he may have seen Native Americans, specifically from the Choctaw Nation, encrypting messages for the U.S. Army basically by speaking their native language. More likely, Johnston first read of the use of Choctaw by the U.S. Army during World War I shortly after the Japanese attack on Pearl Harbor that thrust the U.S. into World War II. Whatever the origin of his idea, Johnston recruited four Navajos to demonstrate to a group of U.S. Marine officers how they could quickly and flawlessly translate English messages into the Navajo language, communicate these messages to each other via radio, and then translate these messages back into English. Convinced of the potential of the Navajo language, the Marines ordered a pilot project in which an eight-week communications training course was completed by a group of 29 Navajos, who became the original Navajo code talkers. A graduation picture from this training course is shown in Figure 2.1 on page 23.

Before this training course could commence, the Marines had to figure out a way to overcome a problem that had plagued attempts at using Native American languages as a means for encrypting messages during World War