Cryptology

Overview

This activity introduces the field of cryptology. People who sometimes use cryptology in their work include archaeologists trying to decipher ancient languages, computer scientists devising ways of keeping information secure on the internet, and cryptanalysts who work for governments and large corporations. During this activity, participants will make a cipher wheel and decode a message using a key. Then they will use statistics to crack messages sent with a cipher wheel even if they do not know the key.

William and Elizebeth Friedman were the first cryptanalysts to use statistical techniques to decipher messages. They were able to crack ciphers that were considered unbreakable before. William analyzed enemy codes for the United States armed forces during World War I and World War II. Elizebeth helped the Coast Guard catch smugglers and spies who sent enciphered messages to each other. She provided crucial testimony in many high-profile criminal trials.

Levels Grades 1 through 6

Topics Data Analysis and Statistics

Goals

- Participants will learn to perform substitutions using a cipher wheel.
- Participants will learn about the relative frequencies of letters in the English language.
- Participants will analyze messages to determine what letters are used most frequently and will use that information to guess the encryption key.

Pre-requisite Knowledge Participants must be able to distinguish capital and lower case letters and work systematically.

Preparation Time 5 minutes

Activity Time 30 minutes

Materials and Preparation

- 1 code wheel copied on colored cardstock for each person
- 1 pair of scissors for each person
- 1 half-inch brass fastener for each person
- 1 paperclip for each person
- 1 pencil for each person
- 1 Cryptology handout for each person
- 1 piece of scrap paper for each person
- 1 page about William and Elizabeth Friedman for each person
- Frequency tables for several languages

Primary Source *The National Cryptologic Museum Activities Book.* Center for Cryptologic History, National Security Agency.

Activity Instructions

1. Participants should cut out their code wheels and fasten them with brass fasteners. People sometimes like to swap one of the circles on their sheets with someone else so that they can have two colors for their wheel.

2. Pass out the cryptology handouts and have them decipher my message to them. Participants may find it helpful to use a paperclip to fix the cipher wheel in the proper alignment so that it does not shift while they are decoding the message. It is easy to get confused about how to use the upper and lower case rings on the cipher wheel. Tell participants that the real English words are in capital letters and the secret message uses lower case letters.

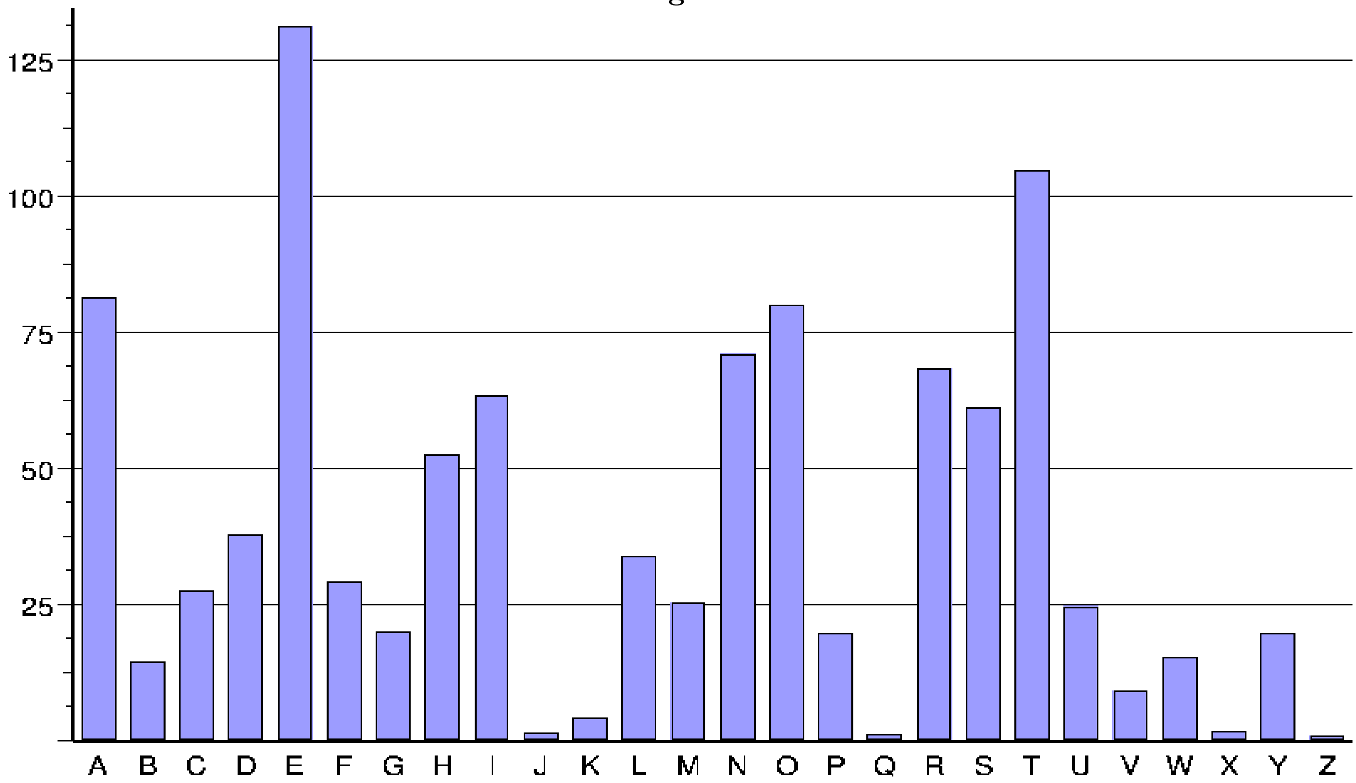
3. Talk about the frequency distribution on the handouts. Show participants that the frequency distributions in different languages are different, so that each language has its own "fingerprint".

4. Have participants tally the number of times each letter appears in the first message on the back of the handout. Have them guess which letter might be 'E' and use this to try to decode the message.

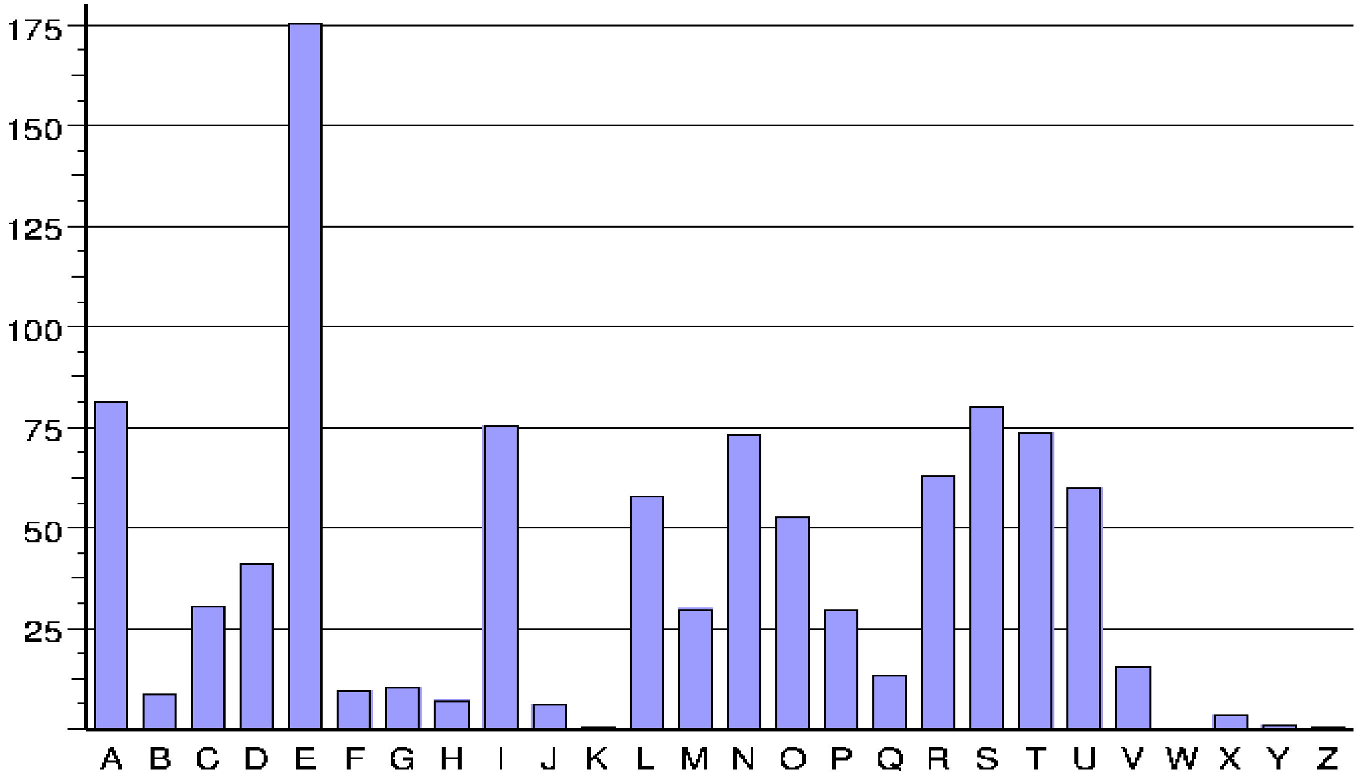
5. Participants can work together in teams to make the work shorter. They can divide and conquer to tally the letters in the longer messages.

6. Some of the later messages are more challenging to crack. In other words, sometimes the most frequent letter is not 'E' but is one of the other frequent letters in the alphabet.

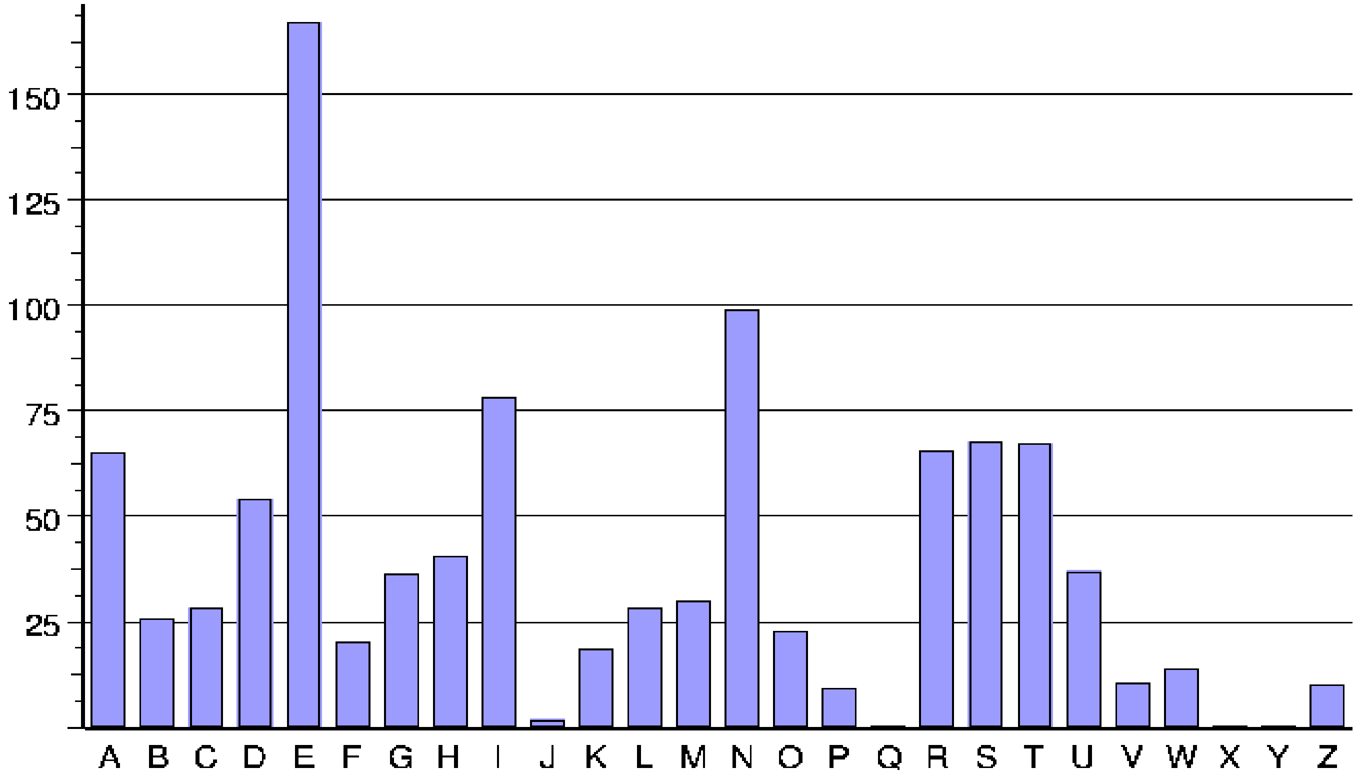
7. Some participants might like to write their own secret messages.

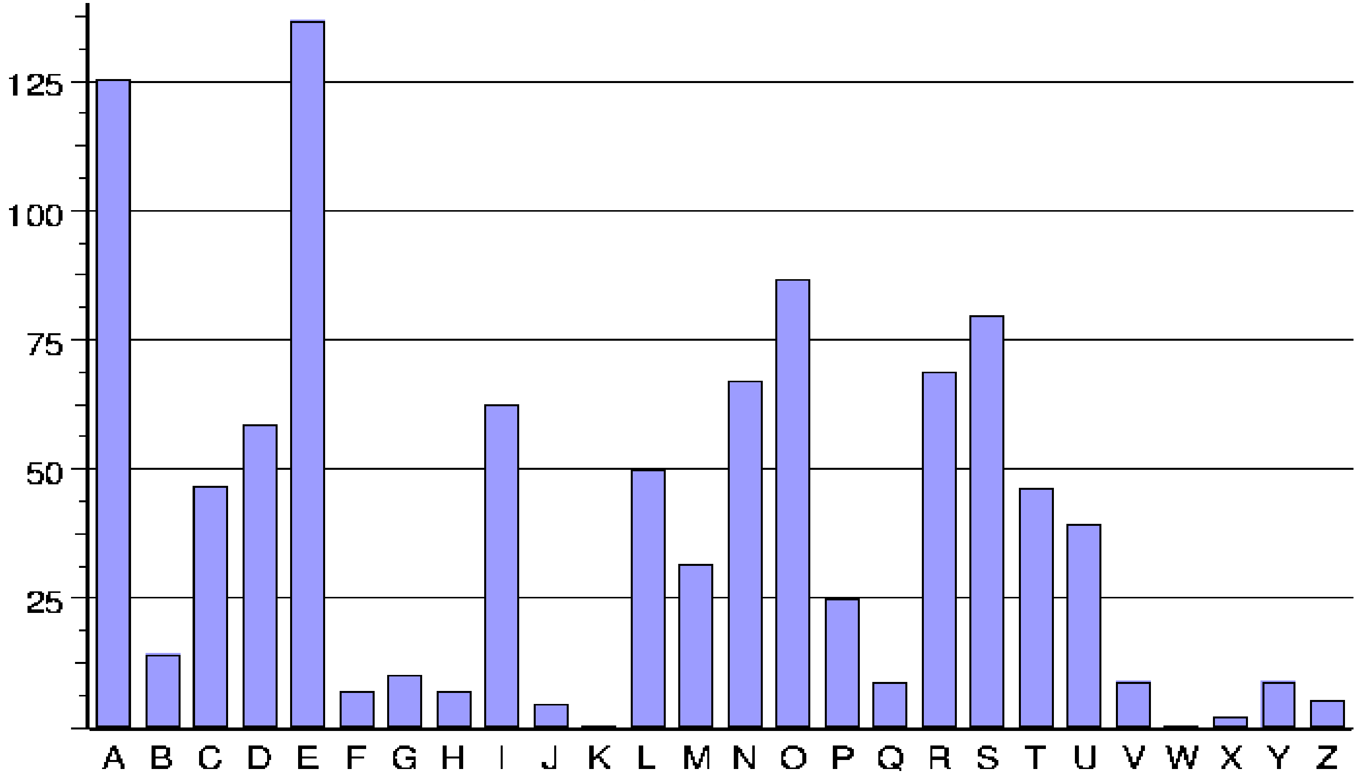


English



French


German


Spanish

William and Elizebeth Friedman and Cryptology

William Friedman (1891 – 1969) and Elizebeth Friedman (1892 – 1980) were a husband and wife team who were pioneers in the field of cryptology. William was the chief cryptanalyst of the United States War Department during the First and Second World Wars. He was responsible for developing the first military cryptology departments in the United States. Elizebeth was the first cryptanalyst hired by the U.S. Coast Guard. During a career spanning more than fifty years, she deciphered many thousands of encrypted messages by smugglers, rumrunners, drug dealers, and spies. Together they transformed the field of cryptology into a science based on sophisticated statistical techniques.

William and Elizebeth stumbled into cryptology by accident. In college, William studied genetics and Elizebeth studied English literature. They met when they were hired to work at Riverbank, a private research institute owned by an eccentric millionaire. They assisted a woman who believed that Sir Francis Bacon had written the works usually attributed to Shakespeare. It was known that Bacon had invented a cipher that could be used to hide a secret message in any text. Their boss thought that she had discovered this cipher in early Shakespeare manuscripts and wanted her research group to help decipher the message.

William and Elizebeth began working together to gather and study the few books that had been written on cryptology. They found that they made a great team and got married in 1917. In the meantime, the United States became involved in the First World War. At that time, the research group at Riverbank was the only one in the country capable of deciphering encrypted messages. The U.S. government asked the group to crack ciphers and train military officers in cryptanalysis. Elizebeth later recalled, “We had a lot of pioneering to do. Literary ciphers may give you the swing of the thing, but they are in no sense scientific. There were no precedents for us to follow. We simply had to roll up our sleeves and chart a new course.” Elizebeth and William began developing new statistical techniques to transform cryptology from an obscure art into a robust science.

In 1921, the Friedmans moved to Washington, D.C. to work as cryptanalysts for the United States government. William first worked in the American Black Chamber where he was responsible for developing new codes and code breaking techniques. William was also responsible for developing cryptology units for several branches of the military and government intelligence agencies. William played an especially important role in code breaking during the Second World War. After their first child was born in 1923, Elizebeth became a special agent for the Coast Guard. This position allowed her to work mostly at home so that she could be with her children. In the first three years alone, she deciphered over 12,000 messages written in many different languages. Elizebeth frequently traveled around the country to give courses on cryptanalysis to law enforcement officers and to testify at trials which hinged on her deciphered messages.

After retiring from their work for the government, Elizebeth and William returned to the subject that launched their careers, publishing *The Shakespearean Ciphers Examined* in 1957. In this book, they considered each of the claims of ciphers found in the works of Shakespeare, including the claims of their former boss. They argued that none of the claims are legitimate and explained carefully why the techniques used in each case were not reliable.

The information on this page comes from

- *Cryptology, Elizebeth Friedman and the United States Coast Guard Thwart the Rumrunners* by Patrick D. Weadon, http://www.nsa.gov/prohibition/about.pdf
- *The Man Who Broke Purple*, by Ronald Clark, published in 1977.

Written by Amanda Katharine Serenevy (amanda@riverbendmath.org), March 2003.