



Spies rely on good security to collect and distribute information covertly in a public world. Although this security often takes the form of physical concealment, codes and ciphers are also frequently used to encrypt and protect information. Examining codes and ciphers provides a fascinating hook for the fields of algebra, probability, and statistics. The Museum’s permanent exhibition contains several historic examples of famed codes and ciphers in **Earliest Espionage**, and **Code Breaking** provides computer interactives with which students can try their hand at decoding a variety of ciphers. The Museum is a great place to jumpstart your students’ thinking about symbolic representation in espionage.

IN THE MUSEUM

Exhibit areas in bold. See map for location.

Symbolic Representation—Algebra



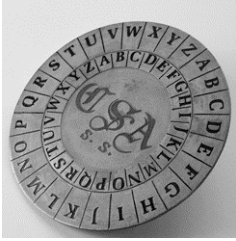
Spies use predetermined physical symbols to communicate with one another. A chalk mark on a mailbox or a newspaper on the ground may have great significance to the spies who intercept them. Explore the interactives in **Tradecraft Skills** and think about how spies’ symbols relate to the use of variables in the classroom. Just outside **Earliest Espionage**, the Rosetta Stone’s hieroglyphics, Demotic script, and Greek characters demonstrate three ways to represent a single message. In **Earliest Espionage**, examine Queen Elizabeth I’s “eyes and ears” dress, which symbolized her reliance on spy networks in order to govern successfully. In **D-Day**, listen to the recording of Paul Verlaine’s poem used as a code to signal the opening of the Second Front. In **Wilderness of Mirrors**, listen to Sandy Grimes and Jean Vertefeuille describe how Aldrich Ames’ body language helped them identify him as a mole.



To discuss with students:

- Look through the museum for other examples of symbolic communication. Can you find examples of:
 - symbols in the environment?
 - symbols in codes and ciphers?
 - symbols in dress or appearance?

Codes and Ciphers—Algebra, Probability, and Statistics



Check out three historic cipher devices in **Earliest Espionage**, and then examine the Enigma machine and code-breaking efforts in **Code Breaking**. Much like the evolution of calculus, each time a cipher is cracked, a whole new breed of cipher (and related mathematics) has to be developed to create a more sophisticated cipher. In any given discipline—algebra, statistics, number theory—students can trace the growth in complexity of ciphers and codes over time.

To discuss with students:

- What is the difference between a code and a cipher? What are some of the advantages and disadvantages of each?
- What is the significance of the key books? Which types of ciphers need keys? Which do not?
- What makes the Enigma code so complicated?
- The Enigma machine on display has three rotors of 26 letters each. How many permutations can the rotors alone produce? The Naval Enigma machine had four such rotors. How many permutations could this Enigma machine produce?



CLASSROOM CONNECTIONS

Artifacts in the Spy Museum are a great springboard for discussion and experimentation back in the classroom. Here are some ideas to get you started.

- Work with symbolic representation by designing codes and ciphers. Present the code and discuss its advantages and disadvantages.
- Test algebraic formulas and simple statistical analysis by constructing a cipher disk (<http://www.nsa.gov/kids/ciphers/ciphe00001.htm>). Work on encoding and decoding messages with the disk. Can you write an equation to find out what each letter maps to? Try using frequency analysis to break a cipher with an unknown key.
- Explore statistics and multi-variable systems by constructing your own Vigenere cipher (<http://www.trincoll.edu/depts/cpsc/cryptography/vigenere.html>). Try encoding and decoding messages using a simple keyword. How is this a better cipher than one produced by the cipher disk? How is it related to the cipher disk? How could this cipher be broken?
- Use bases, powers, and modular arithmetic to introduce the public key cipher now used as standard in internet transactions, etc. Refer to Simon Singh's *The Code Book* for a good introduction to the mathematics of this cipher. Go through the Alice, Bob, and Eve example in detail. What makes this cipher so powerful? Talk about the challenges mathematicians today face in solving the factoring problem.
- Think like a computer. Use binary and modular mathematics to symbolize the entire alphabet. A fun way to do this is with Skittles, M&Ms, or any multi-colored candy. Assign different color combinations to different letters, words, etc. Use a set of candies and try to make the simplest cipher to use and memorize, the one that uses the fewest candies, the one that uses both code and cipher concepts, etc.
- Explore combinations and permutations by exploring the mathematics of the Enigma cipher and its decryption. Simon Singh's *The Code Book* is an excellent resource for a clear breakdown of how the machine works and the bombes used to crack the code.
 - Which parts of the Enigma machine are static, and which are active? Why does this matter? What kind of code would the Enigma machine produce if all moving parts were taken out? Try cracking one of those codes.
 - Calculate the number of mappings possible for a three-rotor Enigma machine with a reflector and a five-pair plugboard. What about a four-rotor Enigma machine with a ten-pair plugboard? Examine the range of possibilities for a variety of configurations.
 - Polish codebreakers discovered that the initial settings of the rotors were the key to breaking the Enigma machine cipher. To determine the rotor settings they built simple pre-computers called bombes that checked every possible initial setting against known cipher text. How do you think a modern computer could find these settings?
 - Discuss looping functions. How do modern computers make the Enigma cipher a relatively easy cipher to crack?

BIBLIOGRAPHY

Kahn, David. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* (New York, NY: Scribner, 1996).

Singh, Simon. *The Codebook: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography* (New York, NY: Doubleday, 1999).