Mathematics in CryptoClub

Many people enjoy solving cryptograms that are commonly found in newspapers. Those are almost always encrypted with some type of substitution cipher, in which one letter of the alphabet is replaced with another. They can usually be puzzled out by taking advantage of familiar patterns in English, such as common letters, three-letter words, double letters, and so on. Whatever patterns that might exist in the actual substitutions are rarely used to solve newspaper cryptograms.

In contrast, messages encrypted with authentic ciphers usually involve mathematical patterns. Using mathematics to encrypt a message makes it easier for the sender to communicate to the recipient how the message should be decrypted. However, it usually puts patterns into the encrypted text than an adversary could use to crack the code. The evolution of cryptography has historically involved a give and take between those who develop more complicated ciphers and those who develop sophisticated methods for breaking the ciphers. This has culminated in modern-day ciphers, such as RSA, which, for practical purposes, is currently not breakable. But the development of modern-day ciphers has spurred mathematical research into topics such as methods of factoring large numbers that could make it possible to crack them.

Exploring mathematical patterns is a core experience for CryptoClub students. In CryptoClub, students use mathematics to encrypt with some of the classical ciphers and they look for patterns in encrypted messages that can help them crack the ciphers used.

Key mathematics topics involved in CryptoClubs include:
- addition, subtraction, multiplication, division
- fractions, decimals, and percents
- negative numbers
- modular arithmetic, which is an important application of division with remainder
- multiples and factors, especially common factors
- functions
- multiplicative inverses
- solution of systems of linear equations

CryptoClub activities give students the opportunity to apply these topics, which they have usually encountered during their formal schooling. In the real-world setting of cryptography, students improve their understanding, reinforce their skills, and increase their appreciation of mathematics.

For more details, see the document, “CryptoClub Connections to the Common Core State Standards for Mathematics (CCSSM).”