THE MATHEMATICAL ASSOCIATION OF VICTORIA

MATHS TREATS BY LUCIANA THE POSSUM

DATA SECURITY AND CRYPTOGRAPHY

Once the main concern of governments and military, data security is now important to everyone including businesses and individuals. The advent of increasing computational power has made it easier to decipher other people's data using analysis or a brute force attack. However, technology also enables us to create more complex encoding algorithms for data protection.

CLASSIC CIPHERS

Historically, cryptography was based on word and letter patterns. The classical way of encoding information was by rearranging the order of the letters of words (transposition cipher) or systematically swapping letters (substitution cipher). Statistical information such as letter frequency was used to break the encryption key.

ACTIVITY

What aspects of different human languages might make it harder to crack an encrypted message? Explore a few languages to test your theories. What strategies have been used historically to make encrypted messages more secure? Create a secret message using a transposition or substitution cipher and see if your friends can crack the code.

MODERN ENCRYPTION METHODS

Cryptographers now use mathematics rather than linguistics, and data can be represented in binary form. The main challenge is to create ciphers which are easy to encode but hard to break. Asymmetric-key schemes have evolved since the 1970s with a public key for encryption and a mathematically-related private key for decryption.

ACTIVITY

What benefits do number-based ciphers offer over alphabet-based ciphers? Write a short message and use random numbers to generate a random shift for each letter (e.g., 3 changes an A to a D). Can your friends crack this new code without the key? What are the limitations of this type of encryption? In what other ways could numbers or operations be used to create an encryption key? Can an unbreakable code be invented?

REFERENCES AND FURTHER READING

VIDEOS

Journey into cryptography series www.khanacademy.org/computing/computer-science/cryptography. Select the one-time pad. Is this the perfect code?

Cracking the 'perfect' code: the enigma machines
www.youtube.com/watch?v=Hb44bGY2KdU&feature=related
www.youtube.com/watch?v=QIrC-8T_hqk

ACTIVITIES

Kids' Zone: Beak the Code www.cia.gov/kids-page/games/break-the-code

Cryptography challenge www.khanacademy.org/computing/computer-science/cryptography/cryptochallenge/a/cryptochallenge-introduction

ARTICLES

Cryptography https://en.wikipedia.org/wiki/Cryptography

History of cryptography https://en.wikipedia.org/wiki/History_of_cryptography

Frequency analysis https://en.wikipedia.org/wiki/Frequency_analysis

The mathematics behind cryptography https://learncryptography.com/mathematics

A technical overview of cryptography www.garykessler.net/library/crypto.html

IMAGES

Leadbeater possum - Steve Kuiter. Other images - Pixabay