Journey into cryptography

How have humans protected their secret messages through history? What has changed today?

Community Questions

ALL CONTENT IN "JOURNEY INTO CRYPTOGRAPHY"

Ancient cryptography

Explore how we have hidden secret messages through history.

- What is cryptography?
- The Caesar cipher
- Caesar Cipher Exploration
- Frequency Fingerprint Exploration
- Polyalphabetic cipher
- Polyalphabetic Exploration
- The one-time pad
- Perfect Secrecy Exploration
- Frequency stability property short film
- How uniform are you?
- Coin flip sequences
- The Enigma encryption machine
- Perfect secrecy
- Pseudorandom number generators
- Random Walk Exploration

Ciphers

Assess your understanding of the code breaking presented in the ancient cryptography lesson. This series of articles and exercises will prepare you for the upcoming challenge!

- Ciphers vs. codes
- Shift cipher
- Caesar cipher encryption
- Caesar cipher decryption
- Caesar cipher frequency analysis
- Vigenere cipher encryption
- XOR bitwise operation
- XOR and the one-time pad
- XOR exploration
- Bitwise operators
- Feedback

Modern cryptography

A new problem emerges in the 20th century. What happens if Alice and Bob can never meet to share a key in the first place?

- The fundamental theorem of arithmetic
- Public key cryptography: What is it?
- The discrete logarithm problem
- Diffie-hellman key exchange
- RSA encryption: Step 1
- RSA encryption: Step 2
- RSA encryption: Step 3
- Time Complexity (Exploration)
- Euler's totient function
- Euler Totient Exploration
- RSA encryption: Step 4
- What should we learn next?

Cryptography challenge 101

Ready to try your hand at real-world code breaking? This adventure contains a beginner, intermediate and super-advanced level. See how far you can go!

- Introduction
- The discovery
- Clue #1
- Clue #2
- Clue #3
- Crypto checkpoint 1
- Clue #4
- Checkpoint
- Crypto checkpoint 2
- Crypto checkpoint 3
- What's next?

Modular arithmetic

This is a system of arithmetic for integers. These lessons provide a foundation for the mathematics presented in the Modern Cryptography tutorial.

- What is modular arithmetic?
- Modulo operator
- Modulo Challenge
- Congruence modulo
- Congruence relation
- Equivalence relations
- The quotient remainder theorem
- Modular addition and subtraction
- Modular addition
- Modulo Challenge (Addition and Subtraction)
- Modular multiplication
- Modular multiplication
- Modular exponentiation
- Fast modular exponentiation
- Fast Modular Exponentiation
- Modular inverses
- The Euclidean Algorithm

Primality test

Why do primes make some problems fundamentally hard? To find out we need to explore primality tests in more detail.

- Introduction
- Primality test challenge
- Trial division
- What is computer memory?
- Algorithmic efficiency
- Level 3: Challenge
- Sieve of Eratosthenes
- Level 4: Sieve of Eratosthenes
- Primality test with sieve
- Level 5: Trial division using sieve
- The prime number theorem
- Prime density spiral
- Prime Gaps
- Time space tradeoff
- Summary (what's next?)

Randomized algorithms

Would access to coin flips speed up a primality test? How would this work?

- Randomized algorithms (intro)
- Conditional probability warmup
- Guess the coin
- Random primality test (warm up)
- Level 9: Trial Divison vs Random Division
- Fermat's little theorem
- Fermat primality test
- Level 10: Fermat Primality Test