

# 12 Days of Ghidra

Nathan R

[Twitter](#) | [Mastodon](#)

# Day 3 – More Crypto

# Cryptography Terminology

Plaintext      -> 'Normal' text

Ciphertext     -> Text passed through a cryptography algorithm

Encryption     -> Convert Plaintext to ciphertext

Decryption     -> Convert Ciphertext back into Plaintext

Key             -> Secret value that adds 'randomness'

# Types of Crypto Algorithms

## Encryption/Decryption

- Reversible
- Useful for hiding data

## Hashing

- One-way (Not reversible)
- Useful for verification of data, or to improve search efficiency

# Day 3 Binary

Improves the cryptography of the binary from yesterday

- No more XOR

Suggestions:

1. See if you can identify what the encryption scheme is
2. Reverse the encrypt algorithm and write the decryption function in a scripting language like Python

How might you find the encryption scheme?

- Variable names, any statically defined constants?