Research

A study of security standard encryption and hash algorithms.

Download Research

Project Roadmap

IDEA

Compare encryption algorithms.

ENCRYPTION

Identify encryption algorithms.

OBJECTIVES

Create encyption tests.

TESTS

Performs tests for data.

DISCOVERIES

Present findings & comparisons.

CONCLUSION

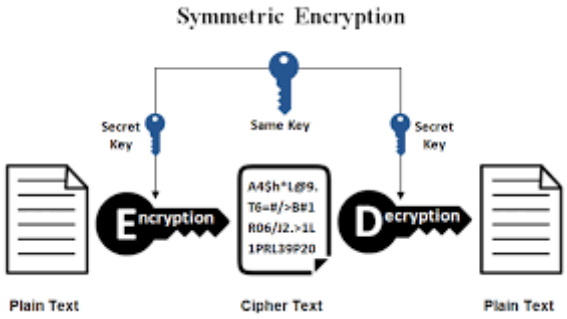
Determine the best encryption.

Two Kinds of Encryption

Symmetric, Asymmetric.

1. **Symmetric Encryption**
   - Algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.

2. **Asymmetric Encryption**
   - A cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner.



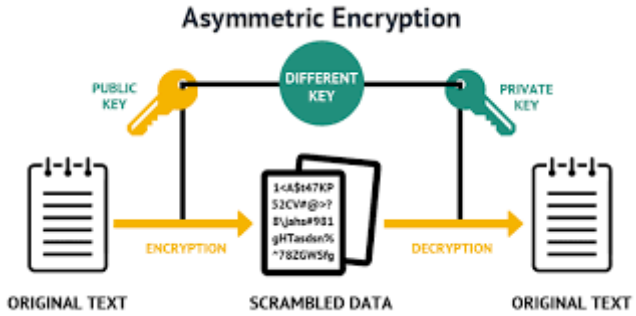
Symmetrical Key Encryption

The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption.

Encryption Stength: Relatively Weak : Single Point of Failure.

Asymmetrical Key Encryption

The generation of shared keys depends on cryptographic algorithms based on mathematical problems to produce one-way functions. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security.



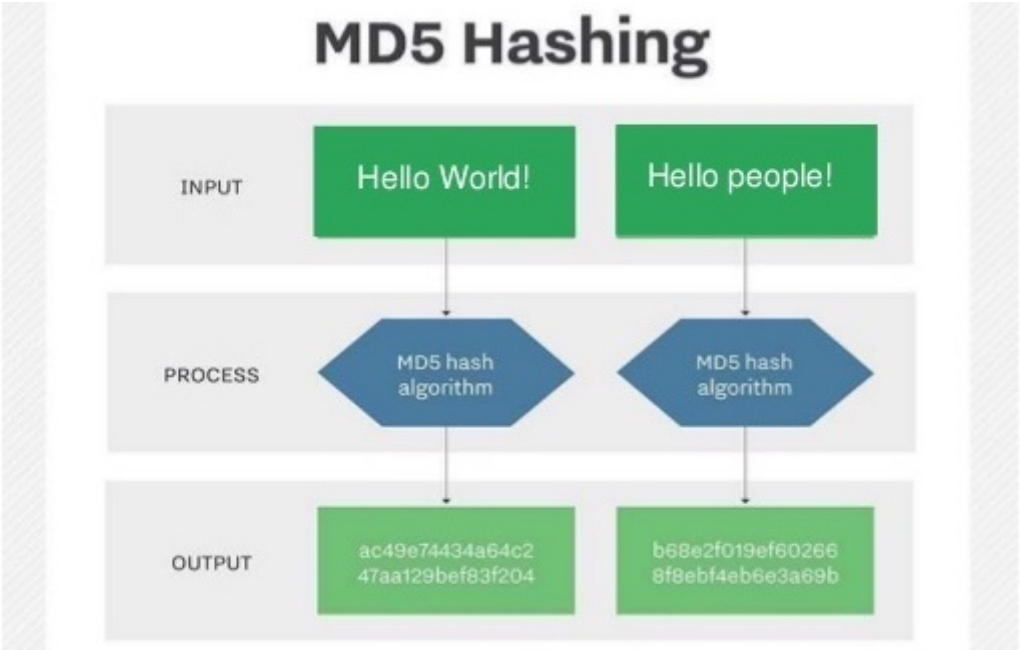
Encryption Stength: Relatively Strong : Still difficult to share private keys in secret, or keep them secret.

Types of Hash Algorithms

Message Digest, Secure Hash.

1. **Message Digests**
   - Cryptographic hash functions containing a string of digits created by a one-way hashing formula. (MD2, MD4, MD5, MD6)

2. **Secure Hash Algorithms**
   - Cryptographic hash functions which takes an input and produces a fixed-bit hash value known as a message digest – typically rendered as a hexadecimal number. (SHA-1, SHA-2, SHA-3)



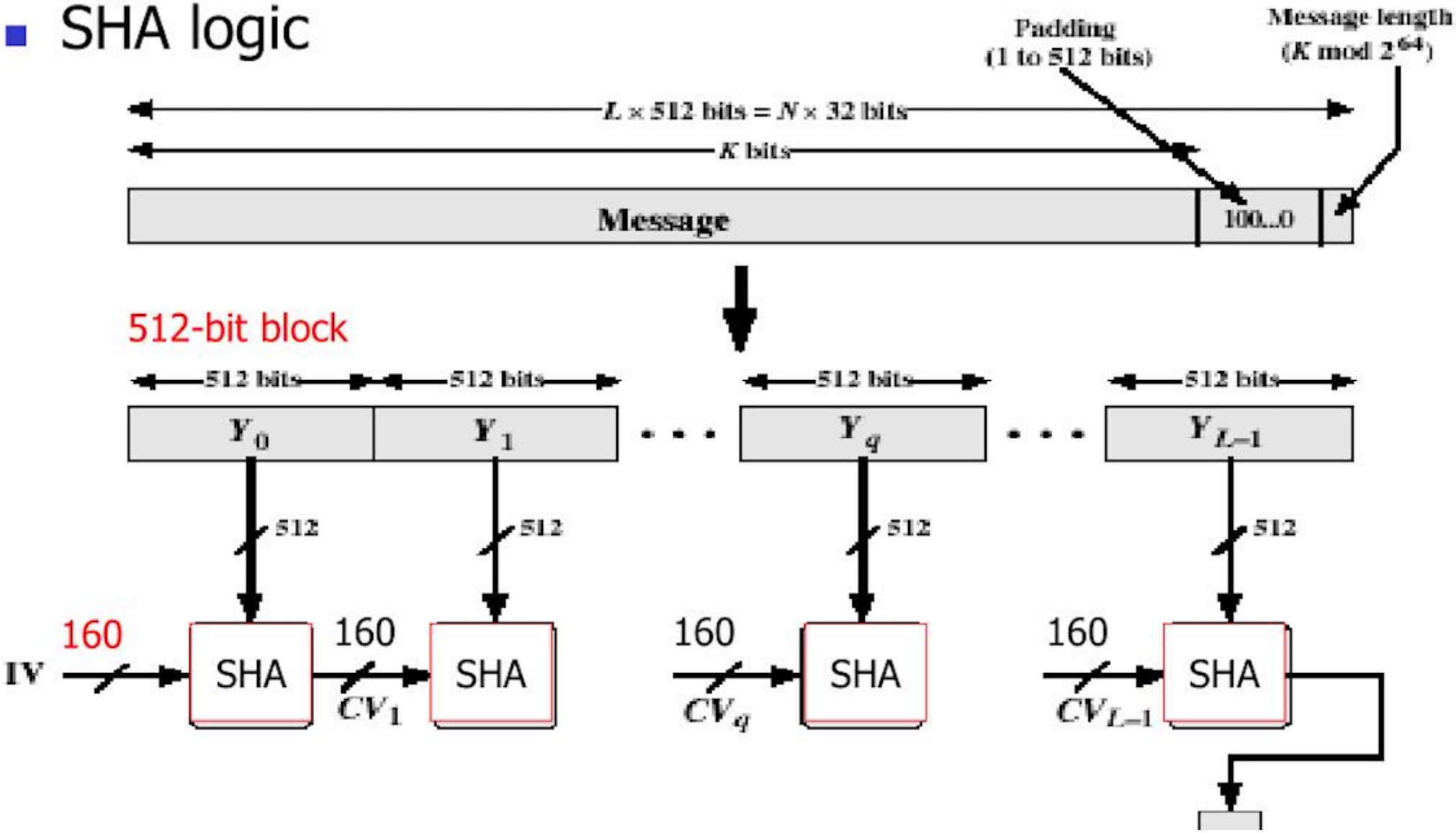
Message Digest

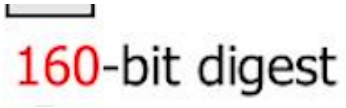
A message digest is a cryptographic hash function containing a string of digits created by a one-way hashing formula. Message digests are designed to protect the integrity of a piece of data or media to detect changes and alterations to any part of a message. They are a type of cryptography utilizing hash values that can warn the copyright owner of any modifications applied to their work.

Encryption Stength: Relatively Weak : Collision Attacks can be carried out in seconds for MD5 and lower.

Secure hash algorithm (SHA)

- SHA logic





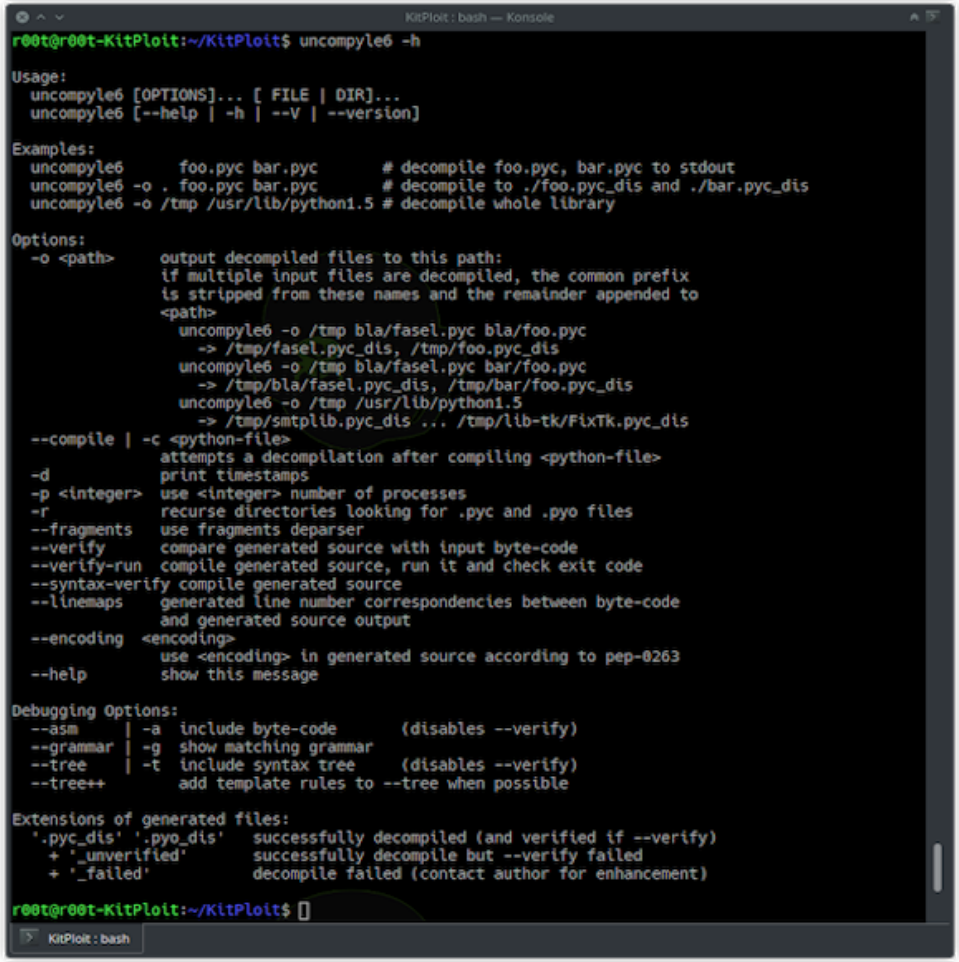
Secure Hash

A secure hash algorithm is a set of algorithms developed by the NIST along with other government and private parties. These secure encryption or "file check" functions are used to meet the top cybersecurity challenges of the 21st century. A number of public service groups work with federal government agencies to provide better online security standards for organizations and the public.

Encryption Stength: Relatively Strong : Google broke SHA-2 encryption using collision attacks in 2017.

Files on Github.

RESEARCH



IMPLEMENTATION

CONCLUSION

Closing Remarks.

There are only two kinds of companies:

1. Those that have been hacked.
2. Those that will be.

~ Robert Mueller

Best,

Brandon Rowe, Kyle Batson, and Josh Howard.