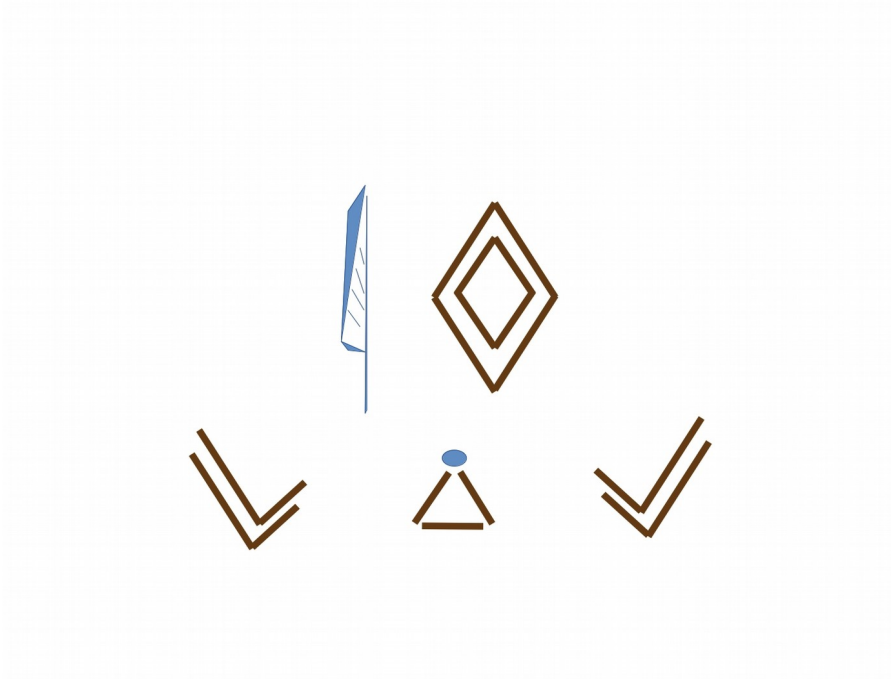
KryptoMagick



Services

- Ancient Egyptian Language Services
- Cryptologic Services
- Research and Development
- Language Services

Inventions

- Egyptian Star Code Generator
- Book of Mormon Cryptanalysis Tool
- Slip Public Key Algorithm
- Q’loQ Public Key Algorithm
- Cube Card Cipher

Inventions

- Purple Hand Cipher
- DarkCastle File Encryption Algorithm
- Kryptographic Music

Qualifications

- Technological skills
- Modular Arithmetic

Mission

- To research and discover hidden messages in the fabric of existence using ancient methods
- To decipher Ancient codes

Pitch

- KryptoMagick offers the chance to discover the connections between our past, present and nature
- Natural Magick is the key

Discoveries

- Supposed text of A the Moon Goddess
- Supposed text of Q the Dream Goddess
- Supposed additions to the Egyptian Book of the Dead

Egyptian Star Code Generator

- An algorithm to map the stars in the sky

Book of Mormon Cryptanalysis Tool

- A program to unmask the Egyptian history contained within the cipher text of the Mormon text
- 2 Nephi Chapter 25:1

Slip Public Key Algorithm

- Introduction of the concept of the Secret Modulus

Q’loQ Public Key Algorithm

- Introduction of the Modulus and the Mask

Cube Card Cipher

- Card Cipher resembling ciphering machines of the past

DarkCastle

DarkCastle

File Encryption Program

Application Purpose

- To help me learn how to construct cryptographic primitives
- Provide secure file storage against real world adversaries
- To allow secure communication between two parties

Design Goals

- To resist real world adversaries
- To allow fast file encryption arbitrary file sizes
- To detect tampering of messages
- To offer only Quantum safe key sizes for symmetric key algorithms
- To utilize no external libraries (sigh!)

Application Features

- Secure storage of files or transfer of messages
- Fast file encryption
- File tampering detection
- Sender/Receiver tampering detection

Language/Libraries

- Written in C
- OpenSSL BigNum Library and PRNG used for public key cryptography

Project History

- First commit in 2017
- Reached version 1.0 milestone in 2020

Project Phases

- Symmetric encryption of files + passphrase
- Symmetric encryption of files + message authentication + passphrase
- Symmetric encryption of files + message authentication + sender authentication + passphrase protected public keys

Symmetric Primitives Used

- Dark (Stream) 256-bit
- Uvajda (Stream) 256-bit
- Spock (Block) 256-bit
- Amagus (Stream) 256/512/1024-bit
- Q’apla (Stream) 256-bit
- ZanderFish2 (Block) 256-bit
- ZanderFish3 (Block) 256/512/1024-bit

Hash/HMAC/KDF Primitives Used

- Ganja 256-bit – Hash/HMAC
- Manja - KDF
- Spock (Block 128-bit block size) 256-bit
- Amagus (Stream) 256/512/1024-bit
- Q’apla (Stream) 256-bit
- ZanderFish2 (Block 128-bit block size) 256-bit
- ZanderFish3 (Block 256-bit block size) 256/512/1024-bit

Public Key Algorithm Used

- Q’loQ RSA 3072-bit

How Does It Work?

- Alice and Bob run `castle-keygen` to set a passphrase to with which to lock their private key and generate their public keys
- Alice and Bob exchange .pk files
- Alice and Bob agree to use the Uvajda cipher
- Alice types a letter to Bob and encrypts and signs it using DarkCastle `castle uvajda -e letter letter.encrypted Alice.pk Alice.sk`
- Bob receives the encrypted message and decrypts it using DarkCastle `castle uvajda -d letter.encrypted message.from.alice Bob.sk Bob.pk`

What about Evil Eve?

- If Eve intercepts the message between Alice and Bob and attempts to alter the message body. The alteration will be detected by Manja before decryption is attempted.
- If Eve attempts to forge a digital signature from Bob, DarkCastle will defend you and inform you that the message is not from who you think it is.

Statistical Testing

- All DarkCastle algorithms pass industry standard statistical tests including tests from NIST

Cryptanalysis

- No publicly known attacks

Research Resources

- Coursera
- IACR
- Christof Parr Course Videos on Youtube
- RSA Conference Videos
- Lectures by Dan Boneh
- MIT OpenCourseWare, lectures by Rivest, Goldwasser and Vaikunatunathan

Research Resources (Books)

- Applied Cryptography
- Handbook of Applied Cryptography
- The Design of Rijndael