DarkTomb

(Authenticated File Encryption Program)

by Karl Zander

DarkTomb is an authenticated file encryption program designed to allow two parties to exchange a file message using the public key algorithm QloQ and the symmetric algorithm AKMS in CBC mode (Advanced KryptoMagick Standard). It works on Unix and Unix-like operating systems such as, Linux, FreeBSD and MacOS. This document outlines the design of the program.

Flow

File encryption (AKMS-CBC) → KDF (QX) → HMAC (QX) → Key Exchange (QloQ) → Signing (QloQ)

Design

The design of DarkTomb is meant to be feature full without being too complex to follow. Each message has a random key generated through the operating system URANDOM PRNG and is encrypted for key exchange using QloQ. The file contents are then encrypted using the random key. The random key is run through the QX KDF function to produce a key suitable for the QX HMAC function. HMAC is run and the MAC is appended to the file. Lastly, the message is hashed and the hash used in QloQ public signing showing that the message comes from the originator.

Operation

QloQ public key pairs must be generated by each party in order to allow them to communicate securely. The .sk file must be kept secret at all times. The .pk file is meant to be exchanged between the two parties and may be kept public at all times.

Key Generation: tomb-keygen username

DarkTomb is executed using the following commands. Suppose Alice wants to send a message to Bob. Alice uses Bob's public key pair and her secret key pair to encrypt the message. Upon decryption, Bob uses Alice's public key pair and his secret key pair to decrypt the message.

Encryption: tomb akms-cbc -e msg msg.enc bob.pk alice.sk
Decryption: tomb akms-cbc -d msg.enc msg.dec alice.pk bob.sk