C 0000010 mmmv cryptokey ID scheme t1

C 1..100

Each key has a private ID that is never attached to a ciphertext and many, possibly thousands, IDs that can be attached to a ciphertext. After encryption one of the keys that can be attached to a ciphertext is chosen randomly and attached to the ciphertext. A database engine is used at the decryption side to efficiently find the key instance according to the key ID at the ciphertext.

The motive is to make crypto-analysis harder without storing that many different symmetric cryptography keys that might be relatively large. The number of IDs at a key may vary and may be in some cases the number of different IDs might be just 5 or 3.

Implementation Related Ideas

May be the database engine might be SQLite, which handles mutexes/locks.

Main page
Recent changes
Random page
Help
Tools
What links here
Related changes
Special pages
Printable version
Permanent link
Page information