DECRYPTION

Check for Encrypted file → Open the encrypted file → Read cipher text from the encrypted file → Read the nonce by reading the last 12 digit of the encrypted file

12 bytes nonce was added to the encrypted file at the end while with encyption

Same Password | Byte Length | SHA-1 | iterators → Password Based derivation Function

Password Based derivation Function → Derived Key

Derived Key → aes cipher

Advanced Encryption Standard

Solid Encryption ability

aes cipher → Cipher Block

more encryption with data integrity checks

Cipher Block → galois counter mode

GCM generates a tag. Which is appended to the cipher text. data upon decryption

GCM and AES to encrypt the plain text data. It operates in a counter mode and generates a stream of encryption blocks.

galois counter mode → aesGCM.OPEN

Password cipher text to this function without the nonce → aesGCM.OPEN → Get the plain Text

Get the plain Text → Create file for waiting the decrypted data → Write decrypted data to it