Password | Seq #

Challenge
(0 to 64 bytes,
presented by the API)

HMAC-SHA1

Shared Secret
(20 bytes,
programmed into
the YubiKey)

Response
(20 bytes, returned
by the API)

YubiKey 2.2 programmed in C-R HMAC-SHA1 mode

Figure 2: Working of Challenge-Response HMAC-SHA1 mode

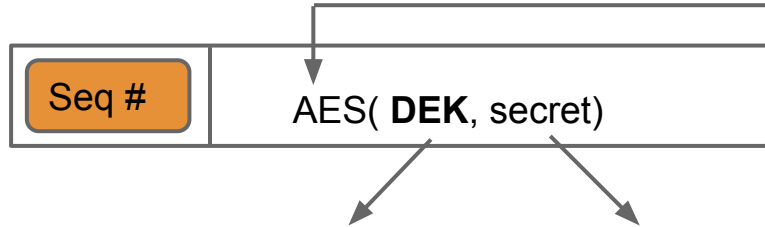Seq # | AES(**DEK**, secret)

Decrypt the actual drive

Re-encrypt the row entry:

HMAC-SHA1(Password Seq # + secret)