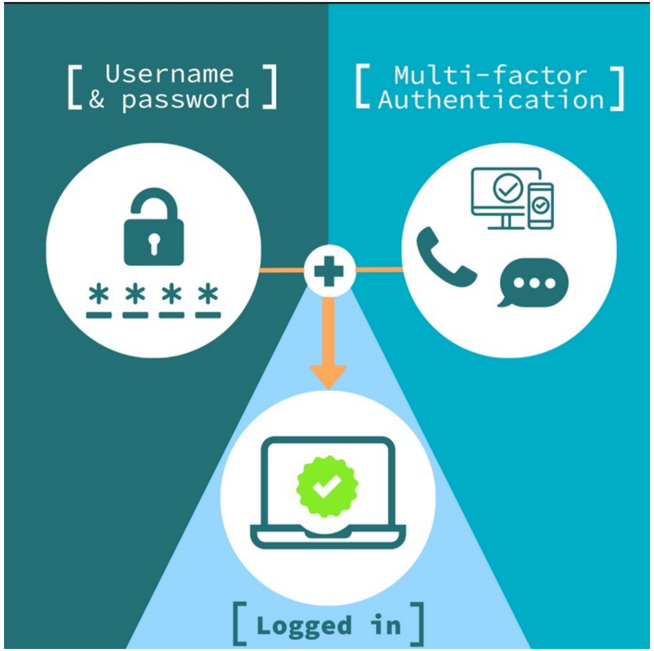
Multi-Factor Authentication and One Time Passwords

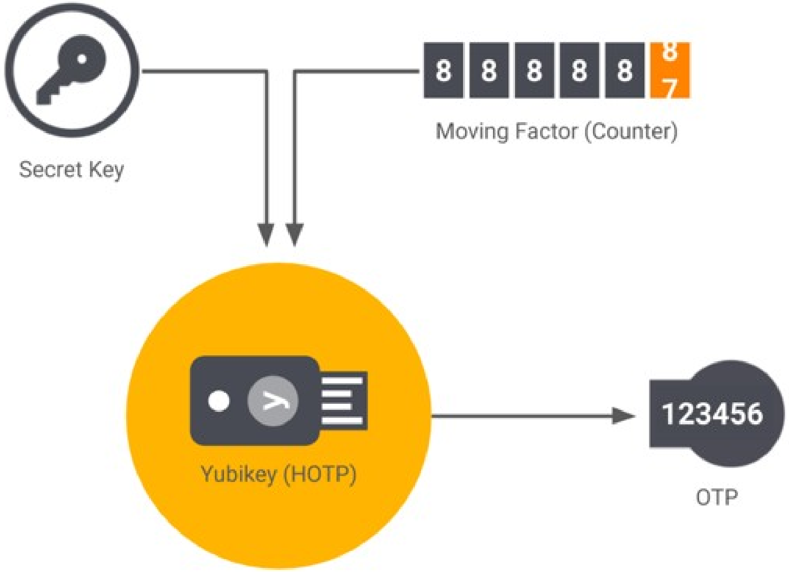
Adam Lamers no. 266559

What is Multi-factor authentication?

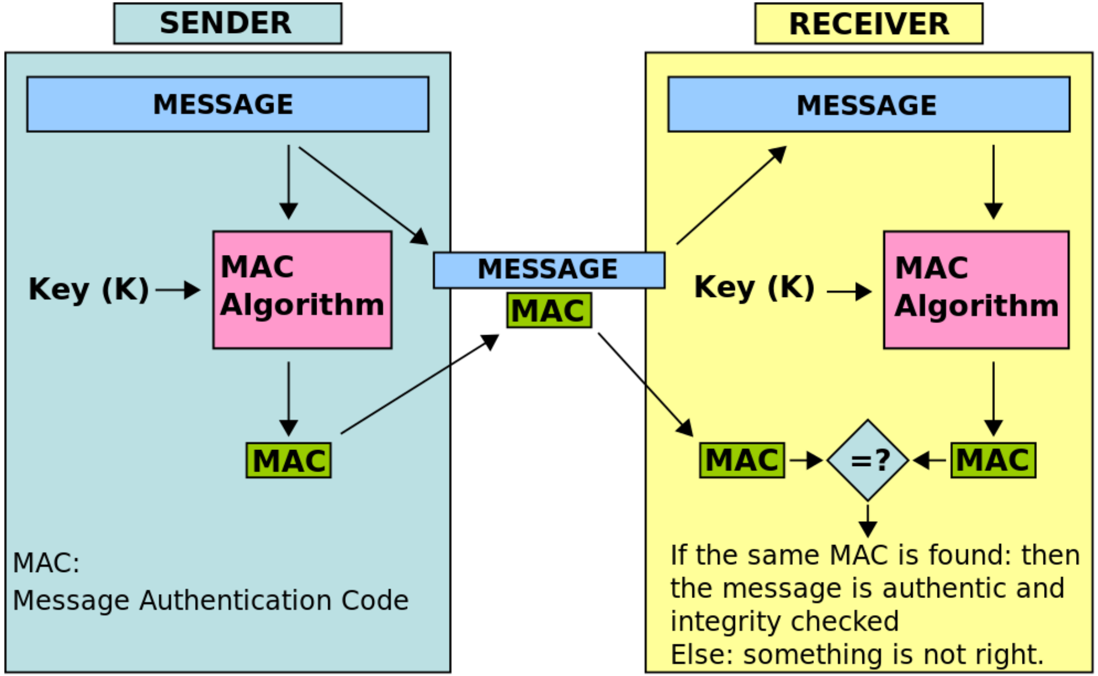


OTP - One Time Password

HOTP - HMAC-based one-time password



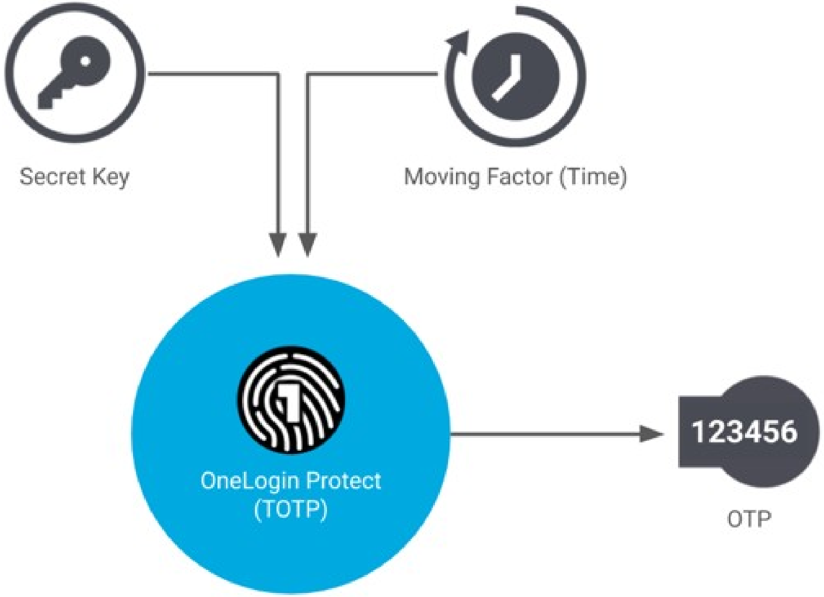
HMAC - Hashed-key MAC



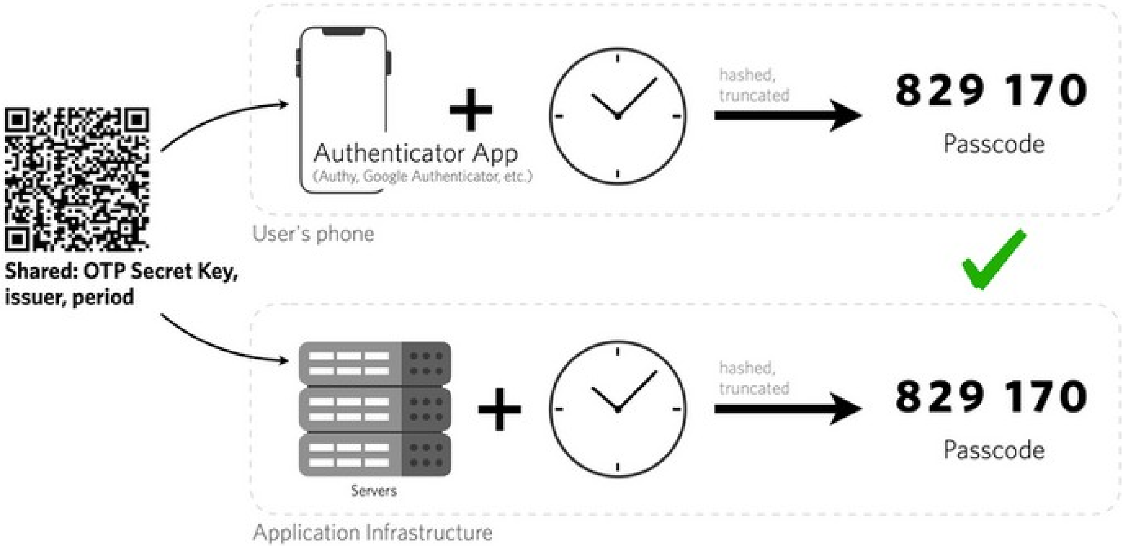
MAC:
Message Authentication Code

If the same MAC is found: then the message is authentic and integrity checked
Else: something is not right.

TOTP - Time based One Time Password



TOTP Calculation



That's all Folks!

U2F - Universal two factor

fido™

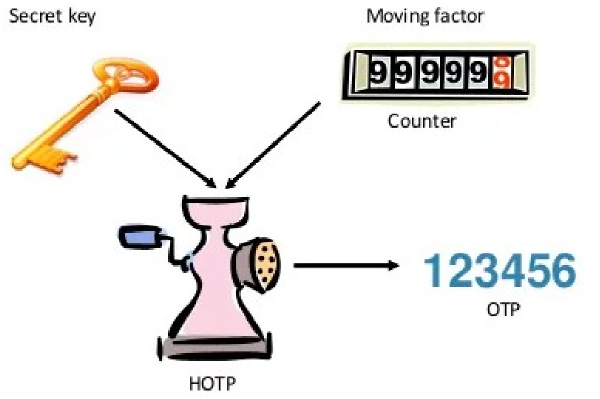
ALLIANCE

So, what about HOTP?

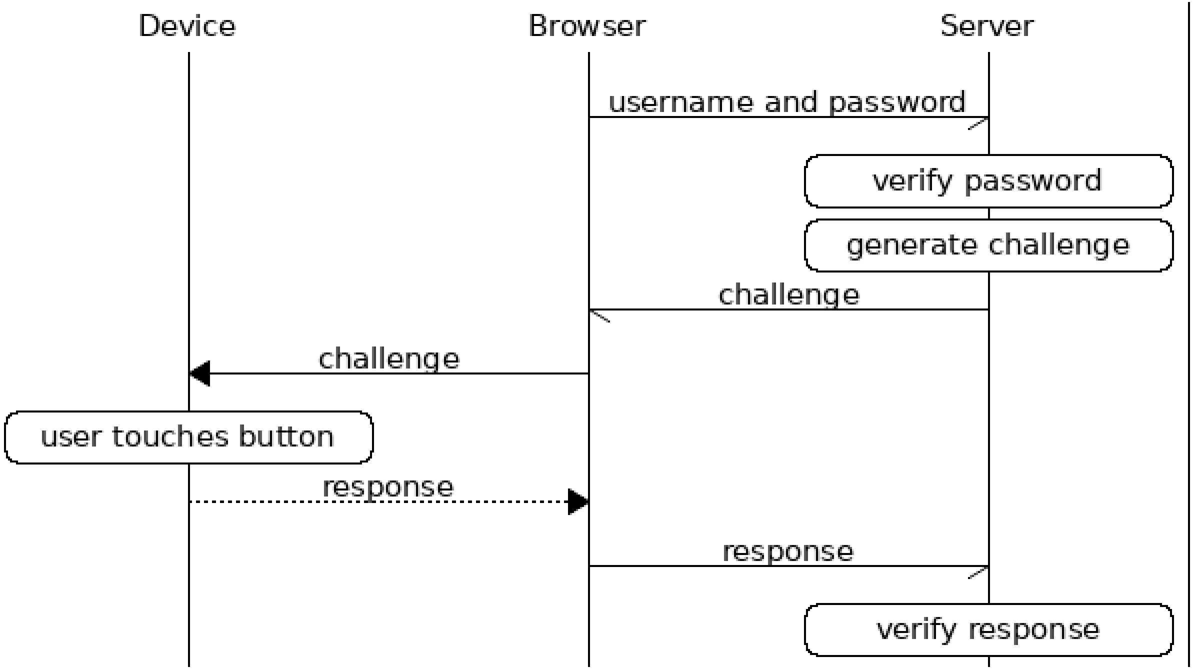
$$\mathit{HOTP\ value} = \mathit{HOTP}(K, C) \bmod 10^d.$$

```
HOTP(K,C) = Truncate(HMAC-SHA-1(K,C))
```

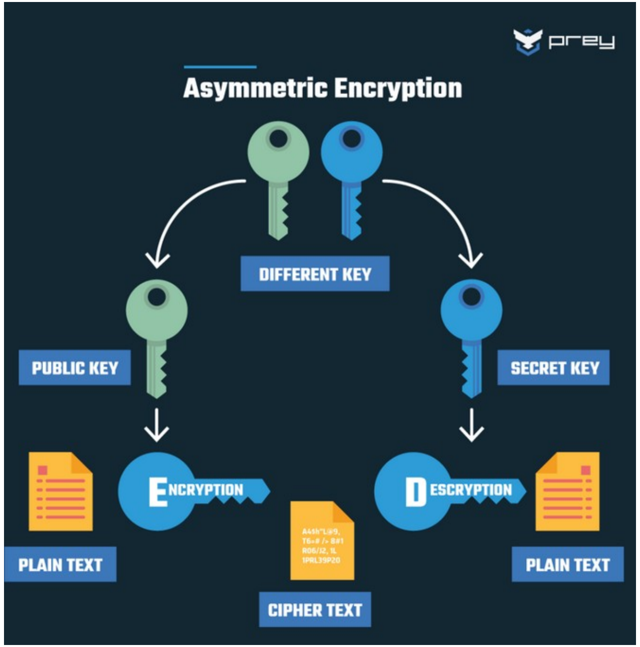
$$\text{truncate}(\mathit{MAC}) = \text{extract31}(\mathit{MAC}, \mathit{MAC}[(19 \times 8 + 4):(19 \times 8 + 7)]),$$

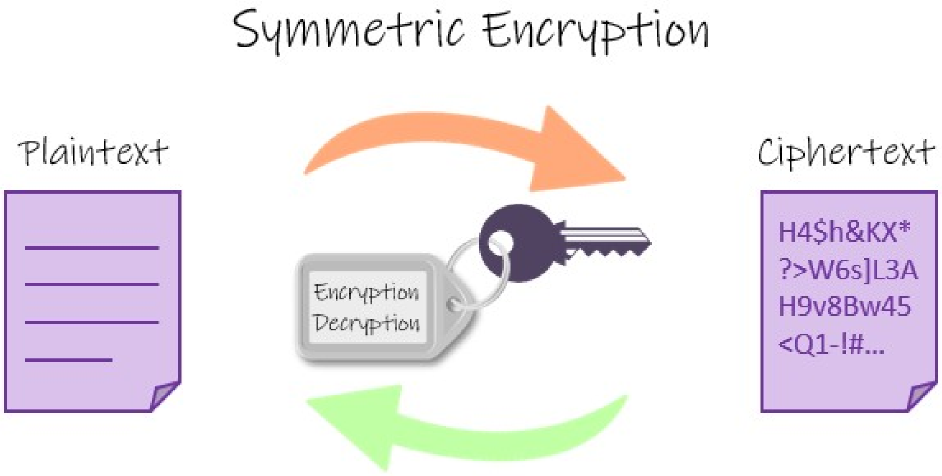


U2F Algorithm

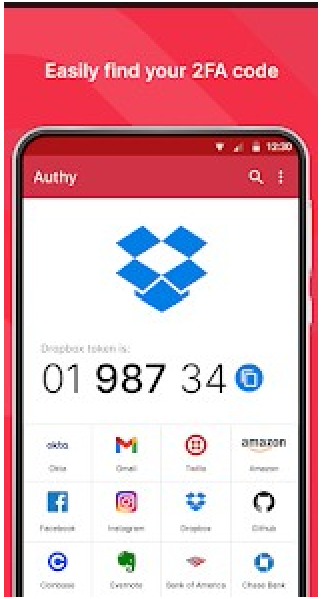


Diffrence between U2F and OAUTH based methods - symmetric and asymmetric encryption





What can be an authenticator?

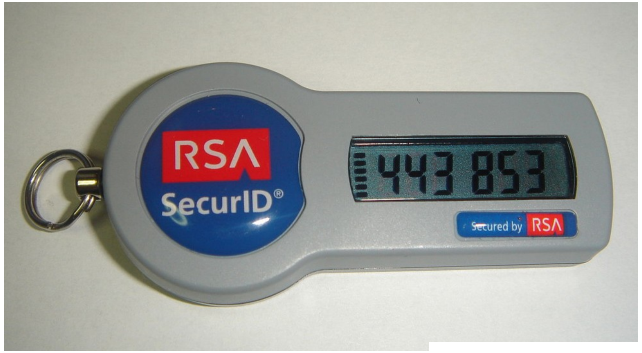


Easily find your 2FA code

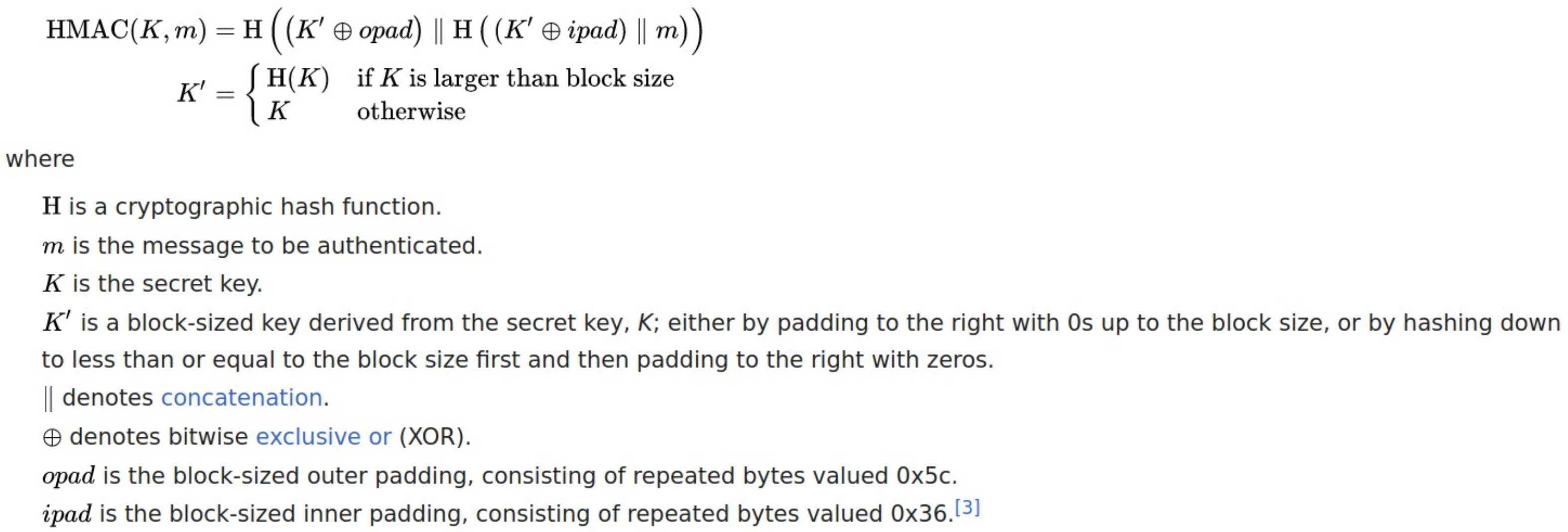
Authy

Dropbox token is:

01 987 34



How simple HMAC really is?



$$\operatorname{HMAC}(K, m) = \operatorname{H}\Big(\big(K' \oplus opad\big) \parallel \operatorname{H}\big(\big(K' \oplus ipad\big) \parallel m\big)\Big)$$

$$K' = \begin{cases} \operatorname{H}(K) & \text{if } K \text{ is larger than block size} \\ K & \text{otherwise} \end{cases}$$

where

H is a cryptographic hash function.

m is the message to be authenticated.

K is the secret key.

K' is a block-sized key derived from the secret key, *K*; either by padding to the right with 0s up to the block size, or by hashing down to less than or equal to the block size first and then padding to the right with zeros.

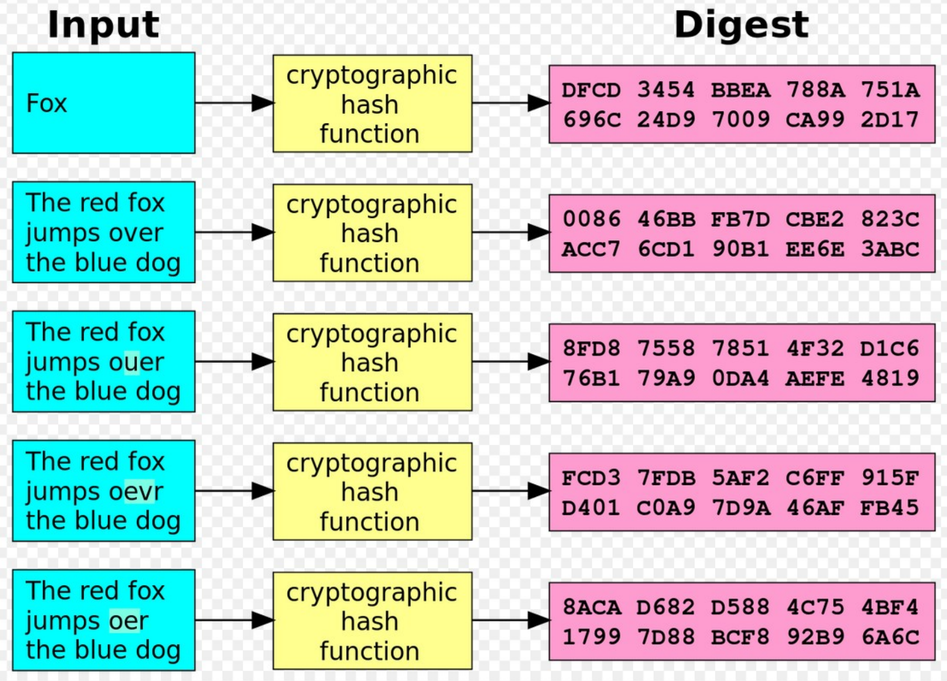
$\parallel$ denotes concatenation.

$\oplus$ denotes bitwise exclusive or (XOR).

$opad$ is the block-sized outer padding, consisting of repeated bytes valued 0x5c.

$ipad$ is the block-sized inner padding, consisting of repeated bytes valued 0x36.[3]

Hash function


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Standards for MFA (to be removed)