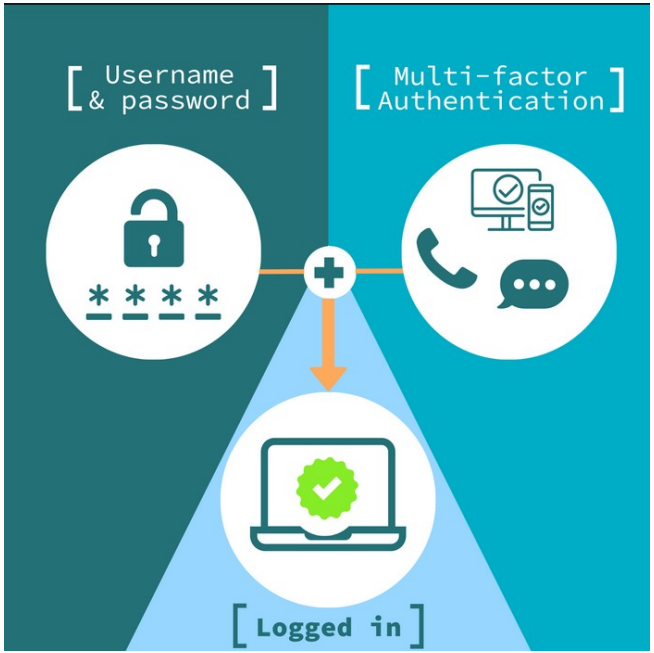
Multi-Factor Authentication and One Time Passwords

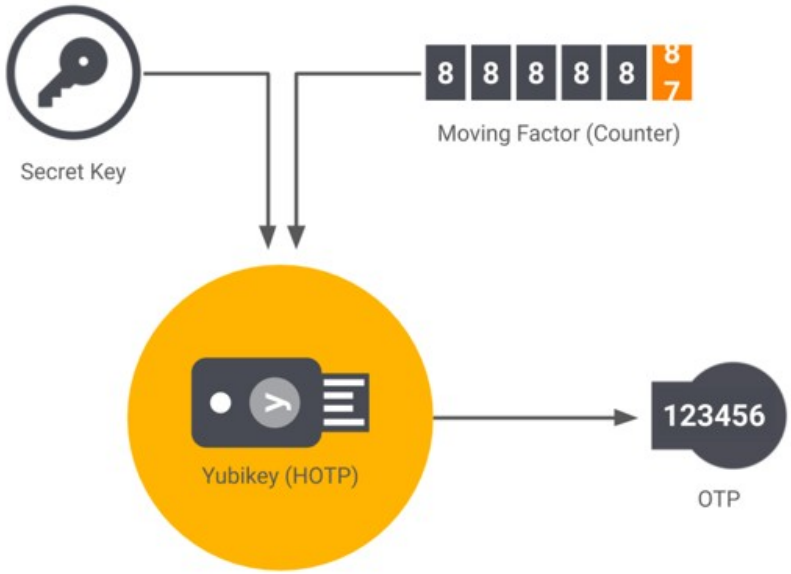
Adam Lamers no. 266559

What is Multi-factor authentication?

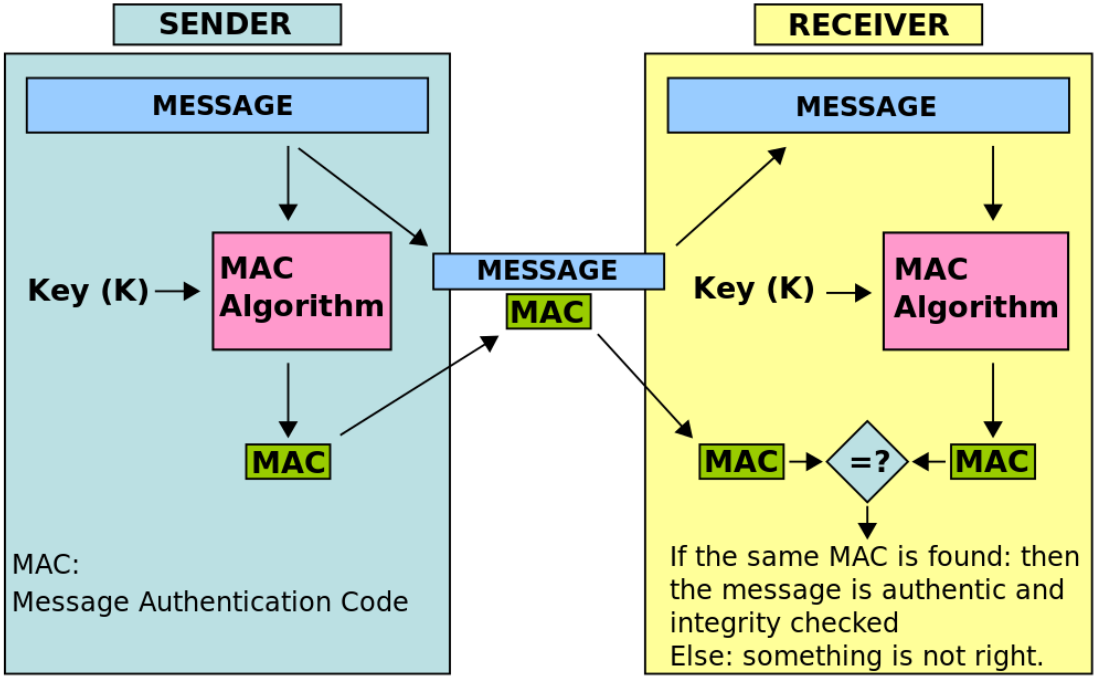


OTP - One Time Password

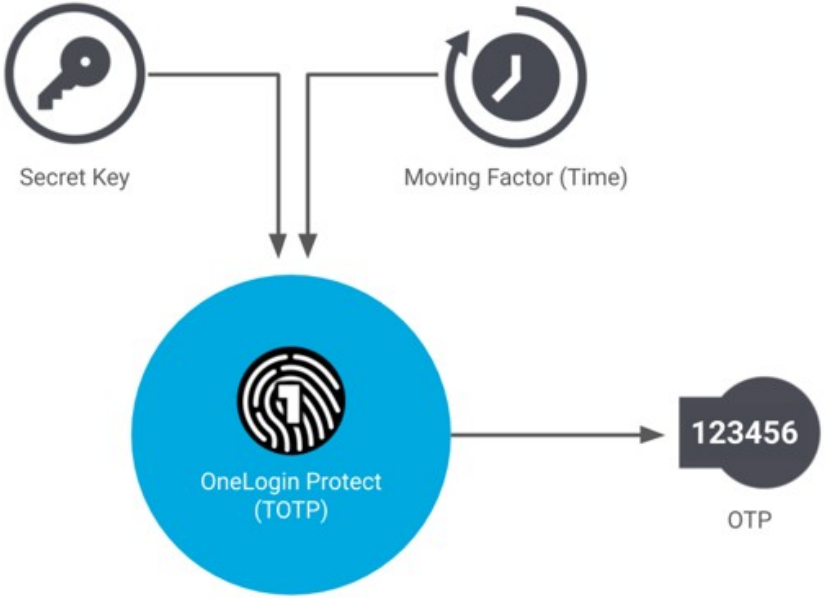
HOTP - HMAC-based one-time password



HMAC - Hashed-key MAC



TOTP - Time based One Time Password



TOTP Calculation

TOTP value(K) = HOTP value(K, C_T),

calculating counter value

$$C_T = \left\lfloor \frac{T - T_0}{T_X} \right\rfloor,$$

where

- C_T is the count of the number of durations T_X between T_0 and T,
- T is the current time in seconds since a particular epoch,
- T_0 is the epoch as specified in seconds since the Unix epoch (e.g. if using Unix time, then T_0 is 0),
- T_X is the length of one time duration (e.g. 30 seconds).


That's all Folks!

U2F - Universal two factor

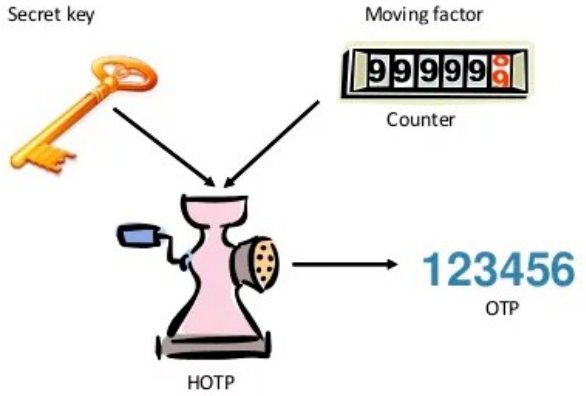
fido™ ALLIANCE

So, what about HOTP?

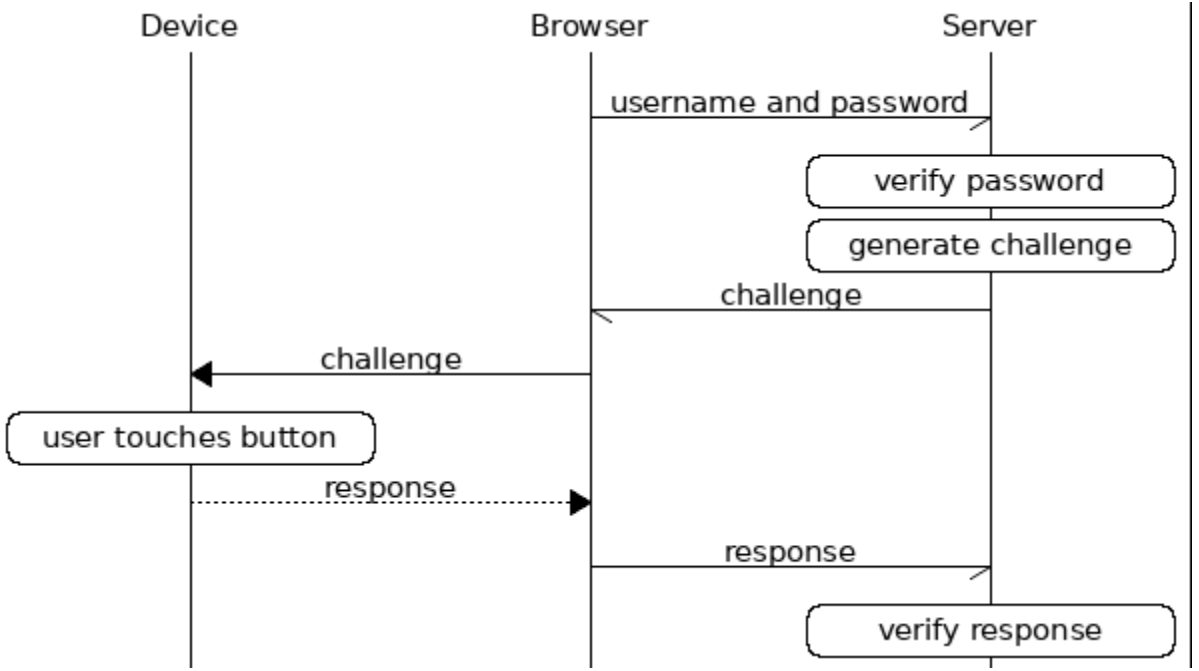
$$HOTP\ value = HOTP(K, C) \bmod 10^d.$$

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

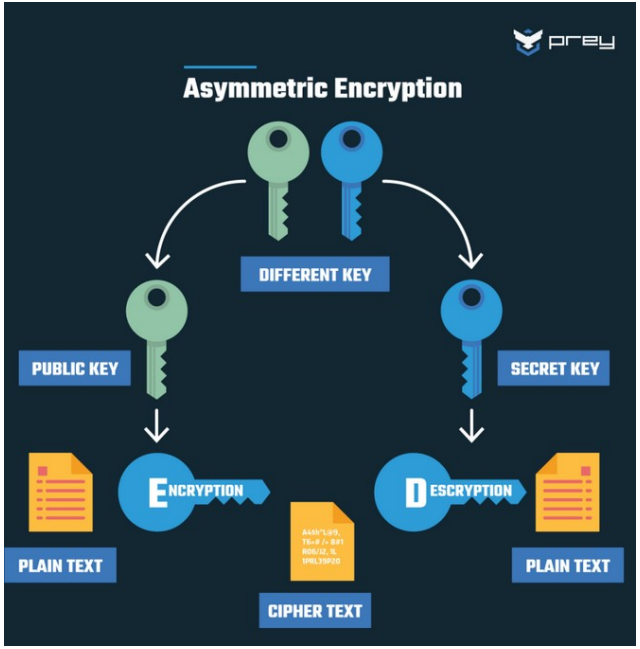
truncate(*MAC*) = extract31(*MAC*, *MAC*[(19 × 8 + 4):(19 × 8 + 7)]),

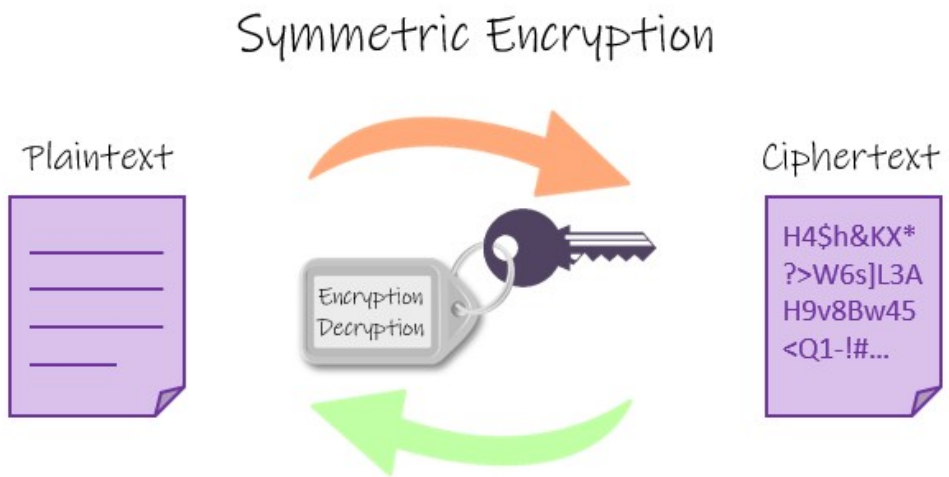


U2F Algorithm

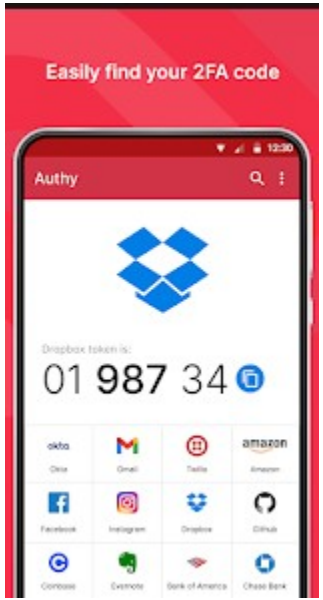


Diffrence between U2F and OAUTH based methods - symmetric and asymmetric encryption





What can be an authenticator?



How simple HMAC really is?

$$\mathrm{HMAC}(K, m) = \mathrm{H}\left(\left(K' \oplus opad\right) \parallel \mathrm{H}\left(\left(K' \oplus ipad\right) \parallel m\right)\right)$$

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

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.

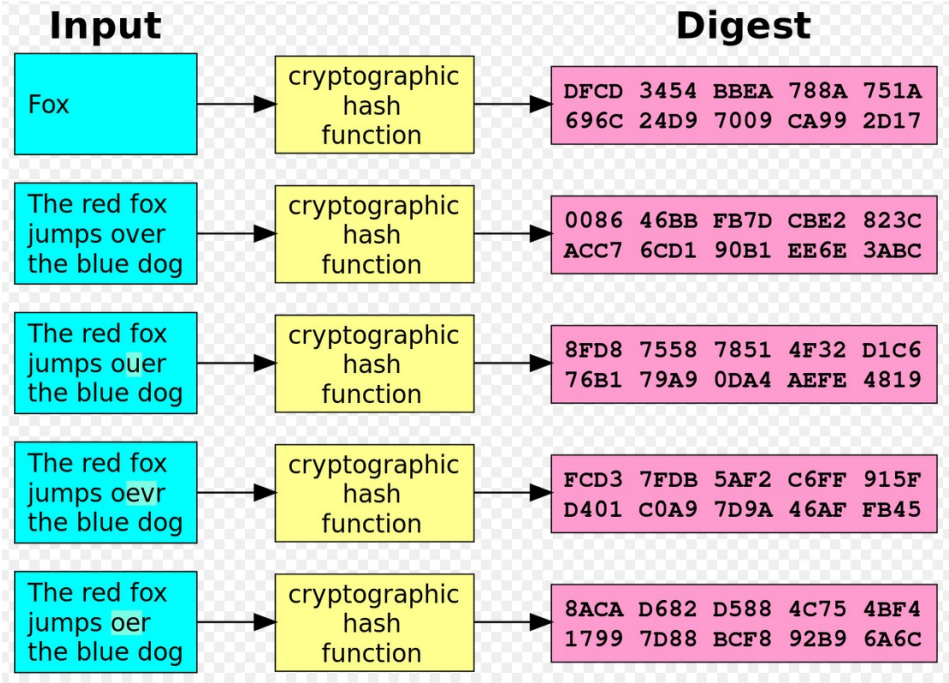
$\parallel$ denotes concatenation.

$\oplus$ 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



Standards for MFA (to be removed)