Cracking Duo?

•••

Cybersecurity UW - Oct 13th - C2 1240

Why Duo?

- A cybersecurity company specializing in multi-factor authentication.
- Founded in 2010.
- Acquired by Cisco in 2018.
- Known for its user-friendly two-factor authentication solutions.
    - Pioneered "Duo Push", an easy-to-use authentication method.

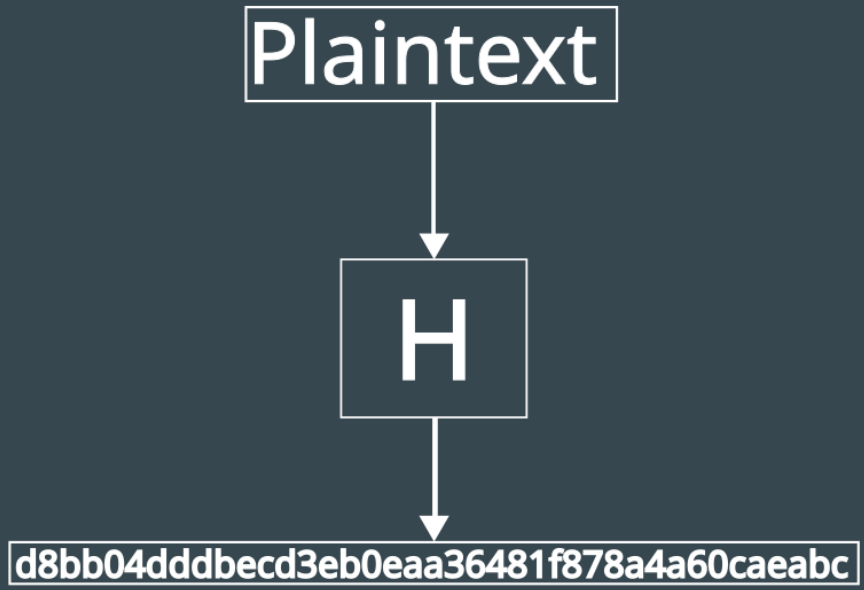
336

Compromised Accounts Last Month

OTP (One Time Password)

Hashing

A function $H: M \rightarrow B^n$

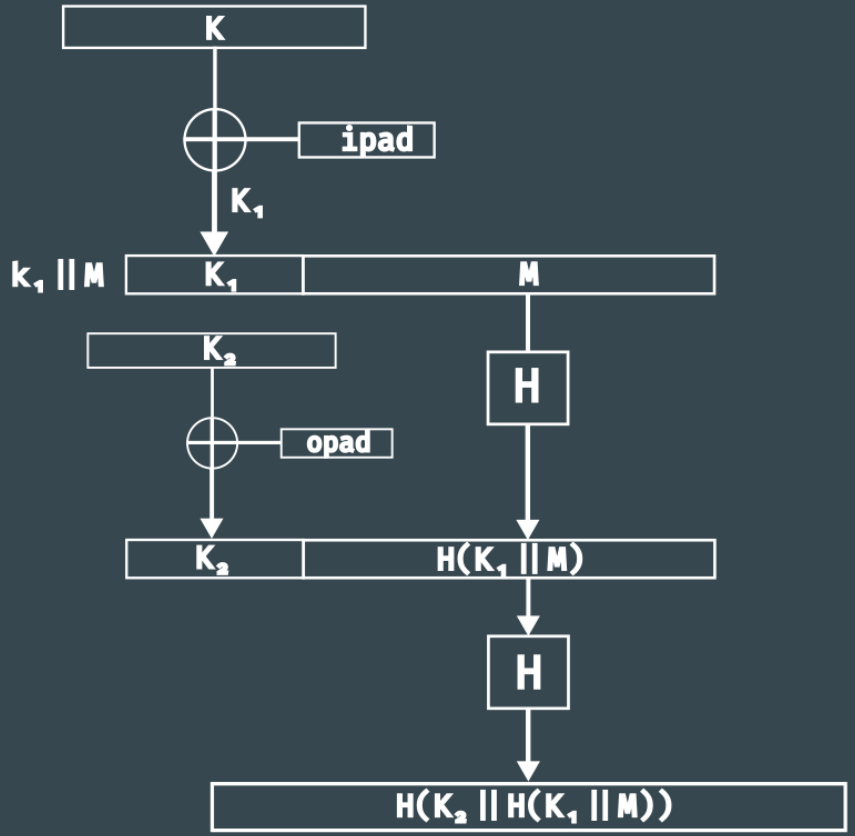


Hashing


Plaintext
H
d8bb04dddbecd3eb0eaa36481f878a4a60caeabc
Plaintext1
H
ee4418d433b8232e0ac15402c24bd13a9112ed95

HMAC

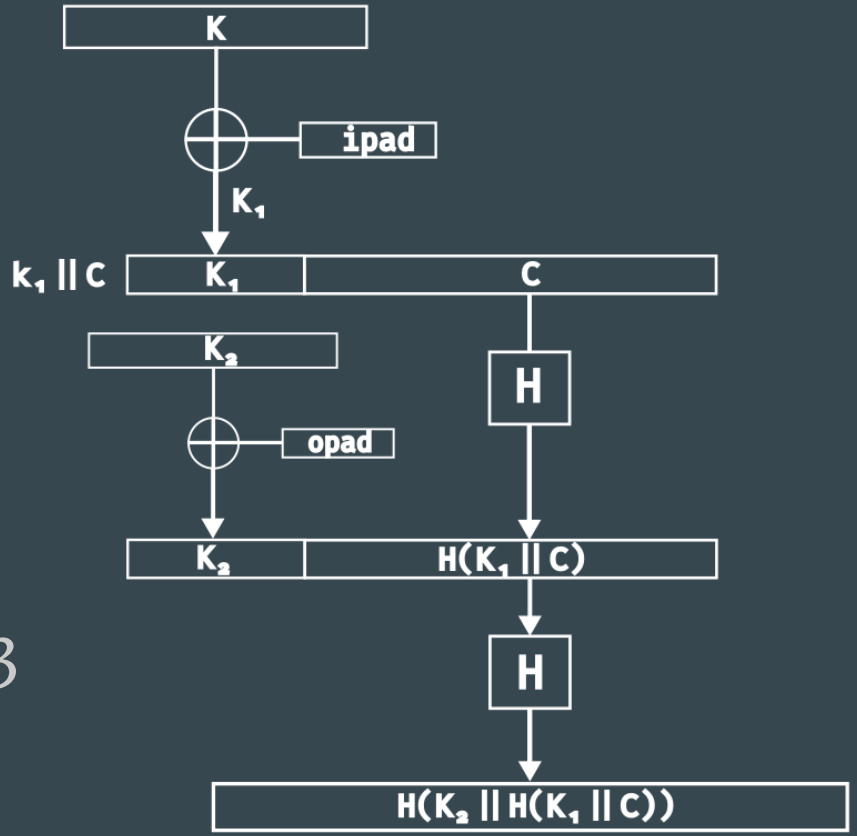
$H(K_2 \,||\, H(K_1||M)) = HMAC(K, M)$



HOTP

HMAC(K, C) truncated

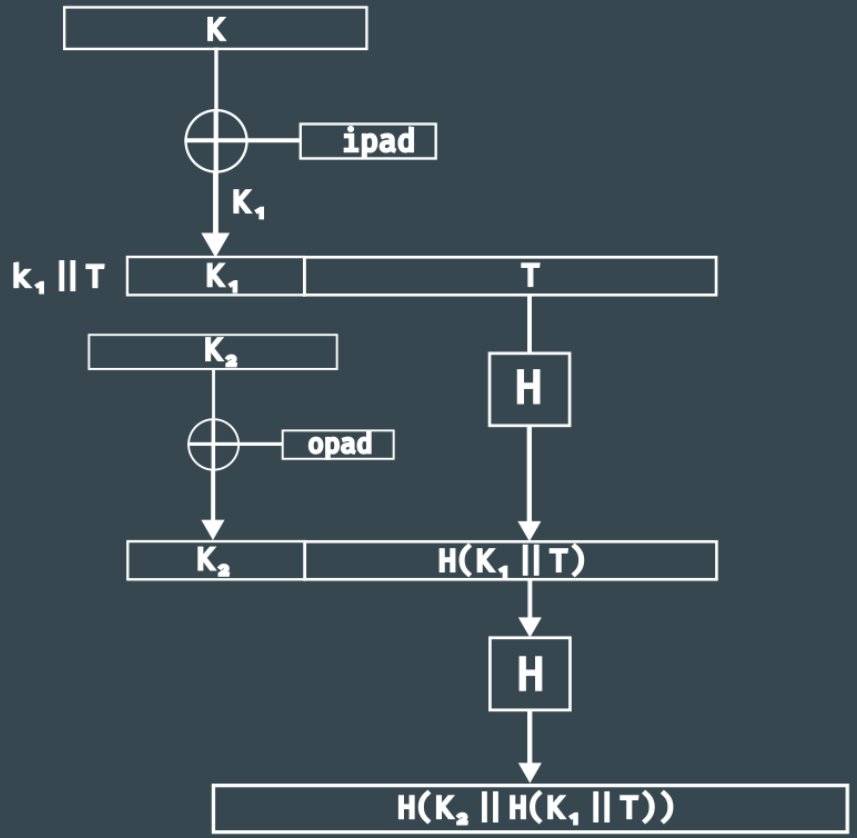
HOTP(“Foo Bar”, 10) = 107843



TOTP

HOTP(K, T) truncated

HOTP(“Foo Bar”, 10/13/23)



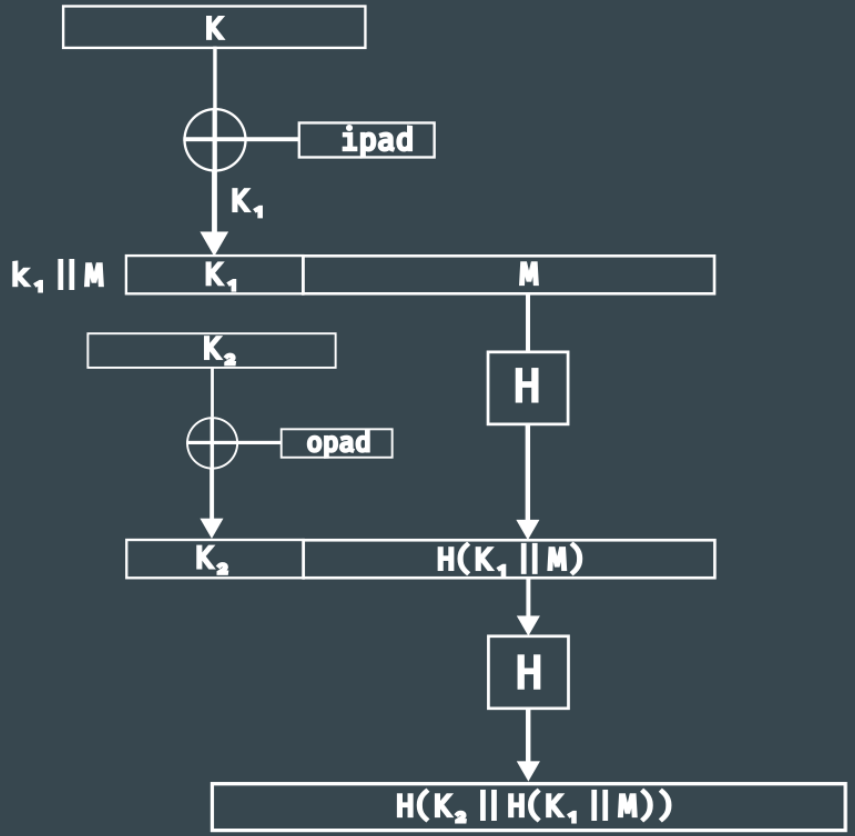
Two Factor with OTP

- Shared key on creation and counter
- OTP generated locally
- OTP is validated on the backend

“Cracking” OTP

HMAC

$H(K_2 \,||\, H(K_1||M)) = HOTP(K, M)$



Demo: Dumping Duo

evilcorp.digital