HMAC-based one-time password algoritme

`http://tools.ietf.org/html/rfc4226` HOTP: An HMAC-Based One-Time Password Algorithm
`http://tools.ietf.org/html/rfc6238` TOTP: Time-Based One-Time Password Algorithm

HOTP

HMAC based one-time password algoritme voor 2-factor authenticatie.

Definitie

- K is een *secret key*.
- C is een *counter*.
- HMAC(K,C) is een HMAC functie, in rfc4226 staat vermeld dat hier SHA1 moet worden gebruikt.
- Selecteer 4 bytes van de resulterende HMAC. We noemen deze functie $T()$. De 4-bytes moeten altijd op de zelde manier worden gekozen.
- HOTP(K,C) = T(HMAC(K,C)) & 0x7FFFFFFF. De reden dat we hier een AND-mask toepassen is om de MSB weg te werken enzo meer compatibel te zijn tussen verschillende processen.

Voorwaarden

Zoals vermeld moet er worden gebruikt gemaakt van een *secret key*. Deze key moet gekend zijn door de client als door de server, alsook de counter. De counter moet nooit worden gecommuniceerd met de server. De *secert key* wel.