HMAC (Hash Based Message Authentication code)

MD = Message Digest / Hash function used

M = The input Message

L = The number of blocks in the message M

b = The No. of bits in each block

K = The Shared Symmetric key to be used in HMAC

ipad = String 00110110 repeated b/8 times

opad = String 01011010 repeated b/8 times

1. Make the length of K equal to b

- Length of K < b

= K = b

K > b

b = 128

$\boxed{K = 200}$

128

2. XOR K with ipad to produce S1

$$S_1 = K \oplus ipad$$

3 Append M to S1

$$S_1 \,||\, M$$

4. $H = MD(S_1 \| M)$

5. XOR K with opad

$S_2 = K \oplus opad$

(6) Append H to S_2

$S_2 \| H$

(7) HMAC $= MD(S_2 \| H)$

Primitive roots

$G = \langle Z_n^*, \times \rangle$ when the order of an element is same as order of the group, that element is called primitive root of the group

$\phi(n)$

ord(a)

- The order of an element, a, is the smallest integer i such that $a^i \equiv e \pmod n$

$= a^i \pmod n = e$

Example

Find the primitive roots of $G = \langle Z_{10}^*, \times \rangle$

$\phi(10) = \{1, 3, 7, 9\} = 4$

1, 2 and 4

$1^1 \equiv 1 \bmod (10)$ $\quad ord(1) = 1$

$3^1 \equiv 3 \bmod (10)$, $3^2 \equiv 9 \pmod{10}$

$3^4 \equiv 1 \pmod{10}$ $\quad ord(3) = 4$

$7^1 \equiv 7 \pmod{10}$, $7^2 \equiv 9 \pmod{10}$, $7^4 \equiv 1 \pmod{10}$

$ord(7) = 4$

$9^1 \equiv 9 \pmod{10}$, $9^2 \equiv 1 \pmod{10}$, $9^4 \equiv 1 \bmod 10$

$ord(9) = 2$

3 and 7

$\phi(4) = 2$ $\quad 2^3$

2×5^1

$\boxed{\phi(\phi(n))}$

$G = \langle Z_8^*, \times \rangle$ The ~~gr~~

The group $G = \langle Z_n^*, \times \rangle$ has primitive roots iff $\boxed{2, 4, p^t, 2p^t}$