HMAC

Sarthak Mahajan, 2018111005

March 7, 2022

1 HMAC Definition:

HMAC or Hashed Message Authentication codes are used instead of CBC-MAC as they are considered too slow. HMAC employs the use of collision resistant hash functions to generate message authentication codes, its faster as it uses much lesser XOR operations than CBC-MAC, and they both use blocks(Fixed length collision resistant hash function, PRF) based on DLP.

2 HMAC Construction:

- (Gen,h): A fixed length hash function
- (Gen,H): Hash function after applying MD transform to (Gen, h)
- Fixed constants: IV, opad and ipad
- opad: $0x36$ repeated as many times as needed
- ipad: $0x5C$ repeated as many times as needed

- HMAC tag for m=$\mathrm{H}^{\mathrm{s}}_{\mathrm{IV}}((k \oplus \text{ opad })||H^{\mathrm{s}}_{\mathrm{IV}}((k \oplus \text{ ipad })||m))$