Keyed Hash

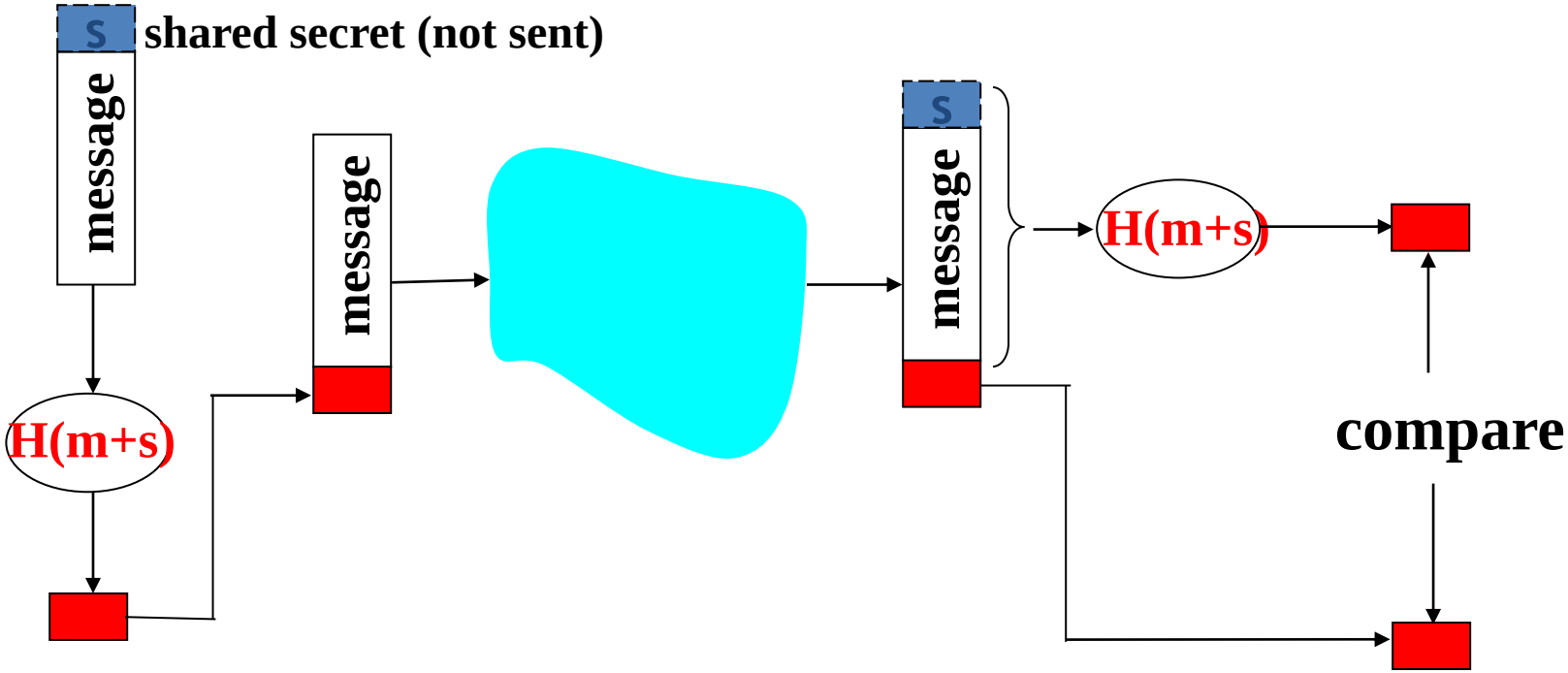
Hyoungshick Kim

Department of Software

College of Software

Sungkyunkwan University

Keyed hash



- ***Authenticates sender***
- ***Verifies message integrity***
- No encryption !
- Example: HMAC (Key-Hashing for Message Authentiction)

HMAC

- HMAC stands for Hash-based Message Authentication Code
- It used to verify data integrity and authenticity of a message
- It uses current cryptographic hash functions with a secret key (SHA or MD5)
  - The name of the function changes depending on what hash function you use
  - MD5 would result to HMAC-MD5
  - SHA# would result to HMAC-SHA#

Security of HMAC

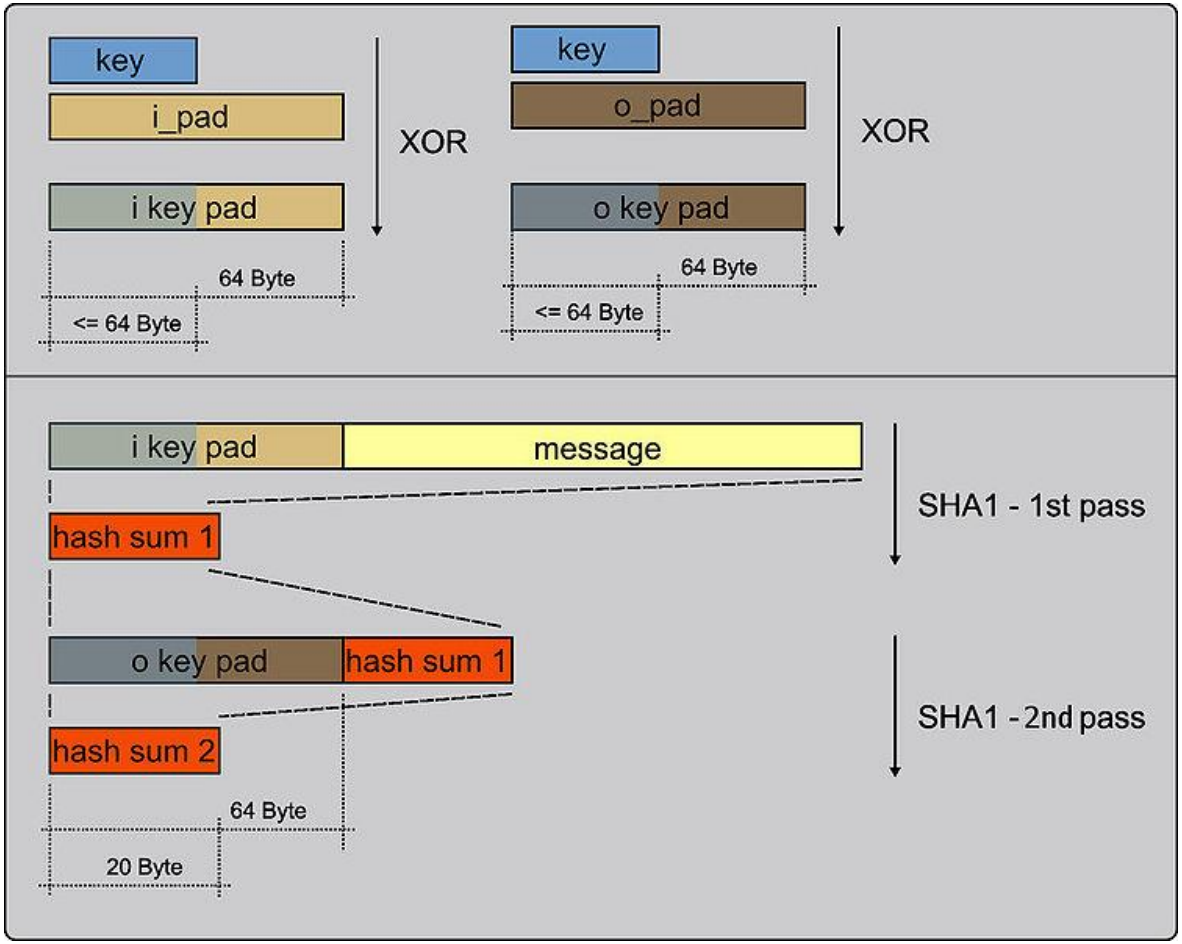
- The strength of HMAC relies on the strength of the hash algorithm used and the quality of the key
- The outputted size is the same as the hash function
  - 128-bit or 160-bit with SHA-1 or MD5

HMAC calculation

- HMAC(k,m) = H((k XOR o_key_pad) ||
  H((k XOR i_key_pad) || m))

  - o_key_pad = outer padding (one block long 0x36)
  - i_key_pad = inner padding (one block long 0x5c)

A visual look (using SHA-1)



Pseudocode

```
Function hmac (k, m)
   if (length(k) > blocksize) then
         k = hash(k)
   endif
   if (length(k) < blocksize) then
         k = k || (0x00 * (blocksize – length(k)))
   endif
   o_key_pad = (0x5c * blocksize) XOR k
   i_key_pad = (0x36 * blocksize) XOR k
   return hash(o_key_pad || hash(i_key_pad || m))
End Function
```

HMAC - Fun facts

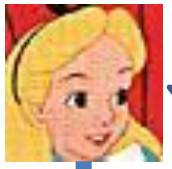
- Using MD5 as the hashing function in HMAC does not seem to compromise the function in regards to the MD5 weaknesses.
  - Even if a hash function *h* is weak, this is believed to make exploitable collisions harder to find [RFC2014].
- Although SHA is much stronger, MD5 is best for performance if it is needed.
- The most common attack against HMAC is brute force to get the secret key.

Applications of cryptographic hash functions

1. Hashing a message before digital signature
2. Storing passwords. (Why?)
3. If we want to compute a MAC without using a cipher (e.g. to avoid export controls), we can use HMAC (hash-based message authentication code)
4. Another application is tick payments – make a chain $h_1 = H(X)$, $h_2 = H(h_1)$, … $h_k = H(h_{k-1})$ for k tokens; sign h_k; reveal h_{k-1}, h_{k-2}, … to pay for stuff
5. A third is to make commitments that are to be revealed later; Just publish the hash value of the confidential document. (e.g., block chain)

Coin-tossing protocol

Alice A



Can you guess which side I chose?

Bob B

Choose
$x \leftarrow \{0, 1\}$;
$m \leftarrow H(x)$

m

Choose
$g \leftarrow \{0, 1\}$

g

x

Compute
$m \leftarrow H(x)$;
if x=g, B Wins!

Is it OK?

B can precompute m!

Random oracle assumption

- A random oracle is an oracle (a theoretical black box) that responds to every unique query with a (truly) random response chosen uniformly from its output domain.
- Random oracle is typically used when the cryptographic hash functions in the method cannot be proven to possess the mathematical properties required by the proof.

Q. Do random oracles exist?

1. Yes
2. Maybe, but we don't know of one yet
3. No, it is impossible to construct one

Uniform distribution → deterministic, so we can't add randomness

Questions?


Sungkyunkwan
Campus
Social
Institute
Graduate
constructed
English
Professors
Building
campus
Global
Sciences
University
Seoul
Natural
Suwon
university
School
Korean
edit
established
Humanities
lecturers