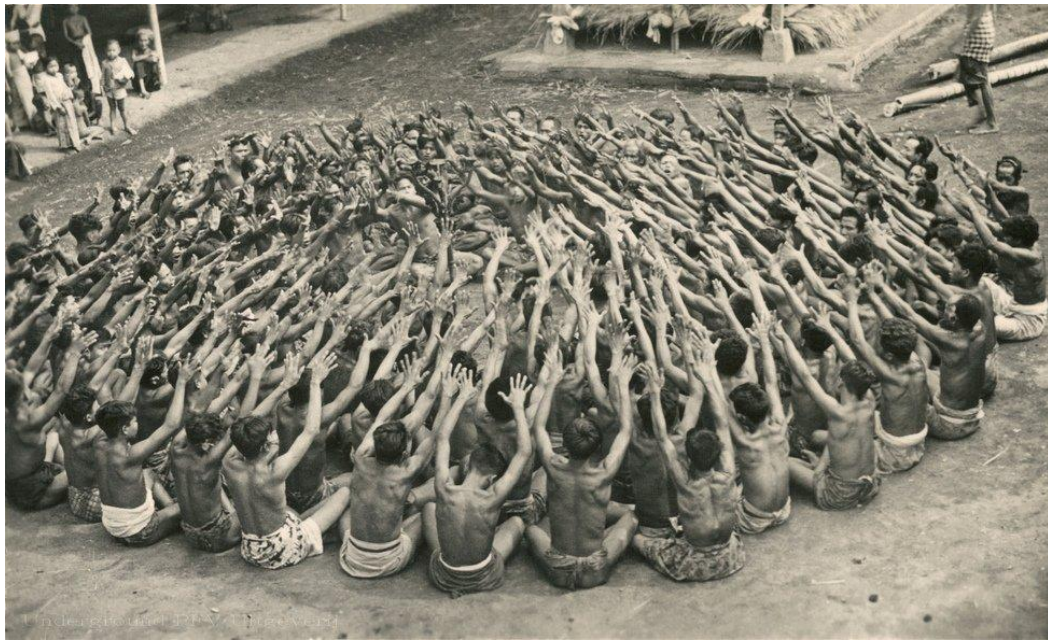


Kecak Dance

CS 553

CRYPTOGRAPHY

Lecture 21

Keyed Hashing

MAC

Instructor

Dr. Dhiman Saha

Image Source: Google

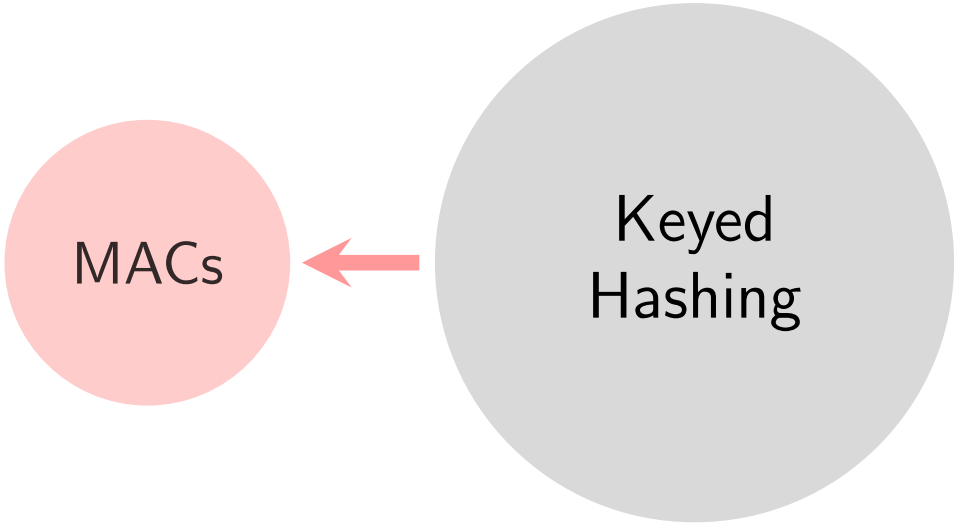
Keyed Hash Functions

Hashing with secret keys

Keyed
Hashing

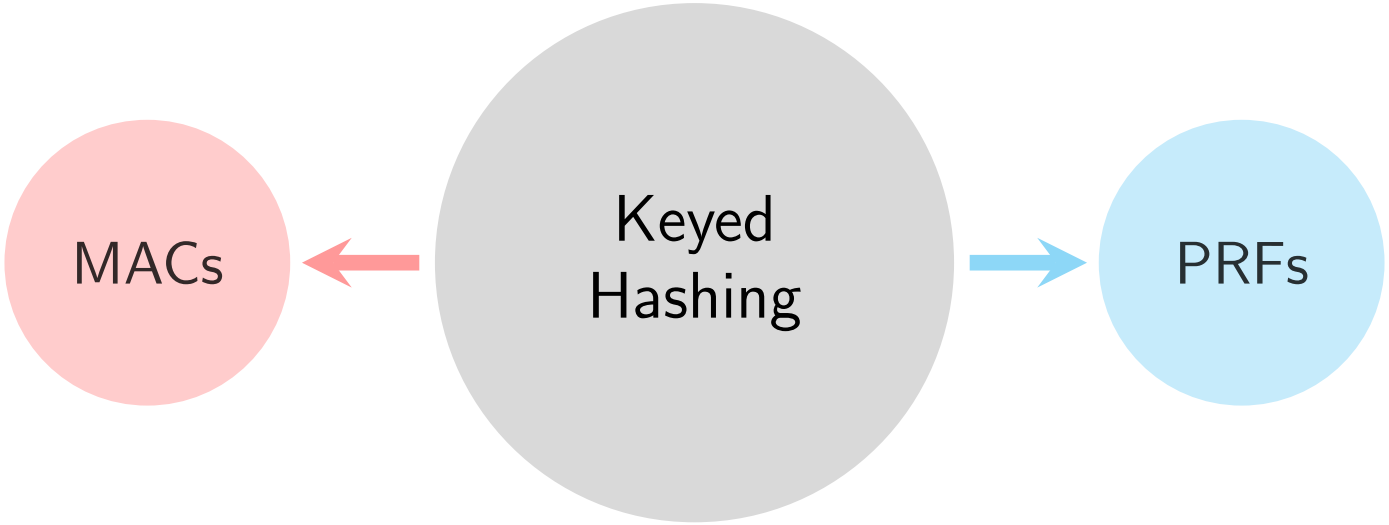
Keyed Hash Functions

Hashing with secret keys

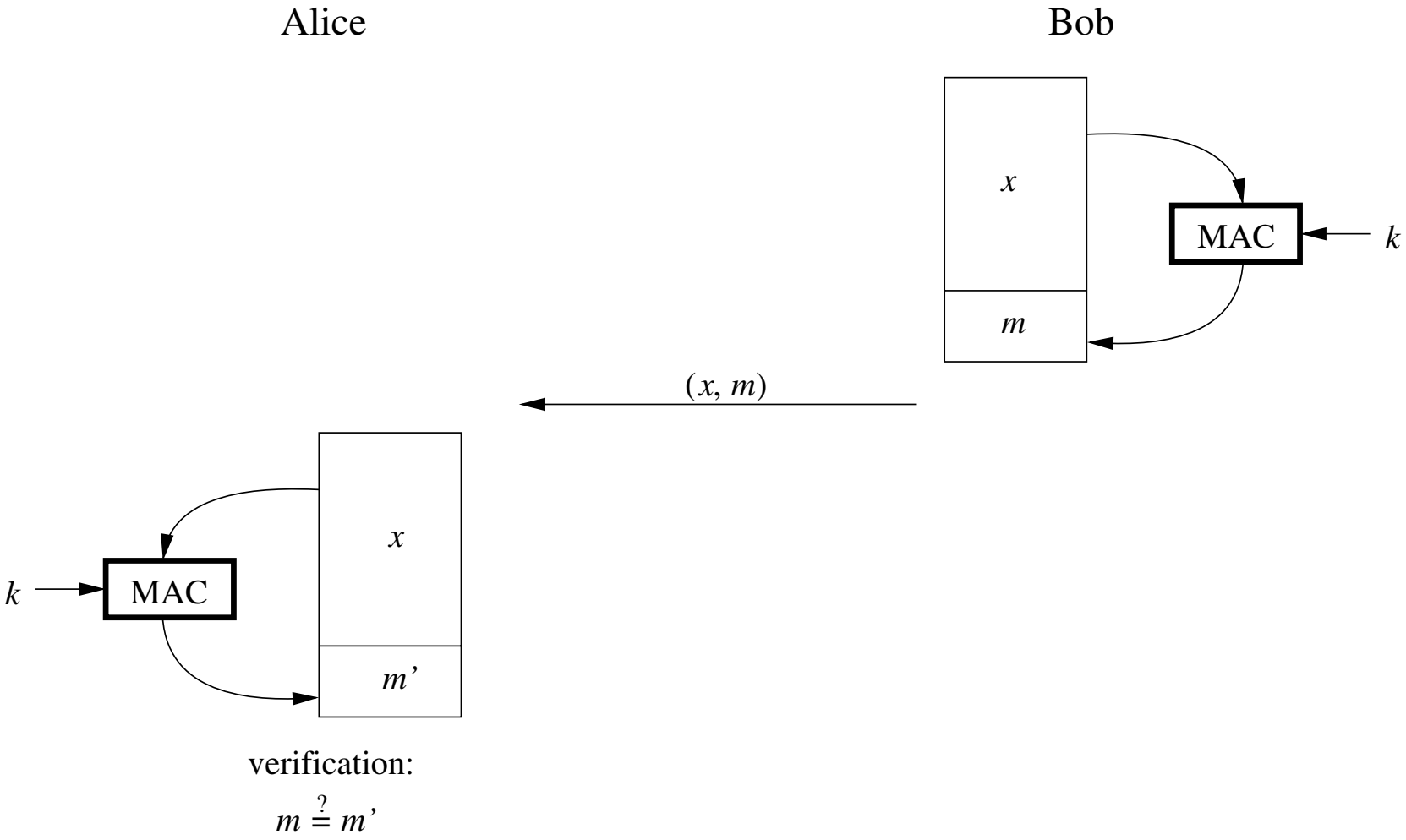


Keyed Hash Functions

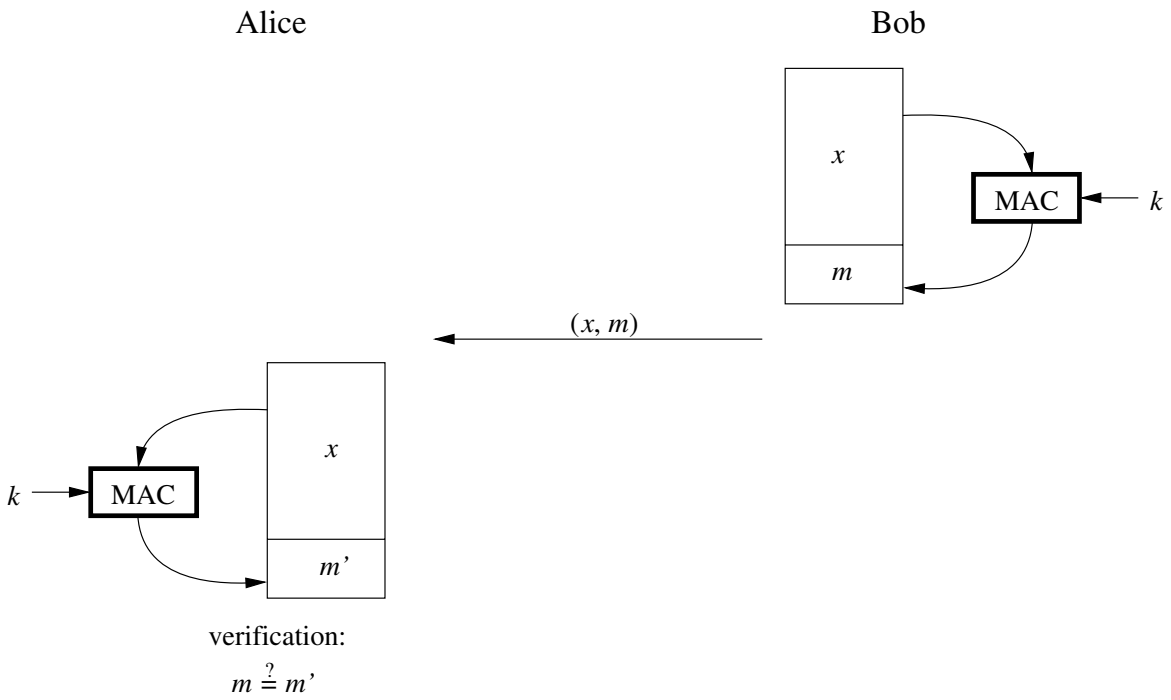
Hashing with secret keys



Message Authentication Codes



$m = MAC_k(x)$ $\leftarrow$ Authentication Tag



Integrity

Alice knows that the message wasn't corrupted in transit

Authenticity

Alice knows that Bob sent that message

When used and when not

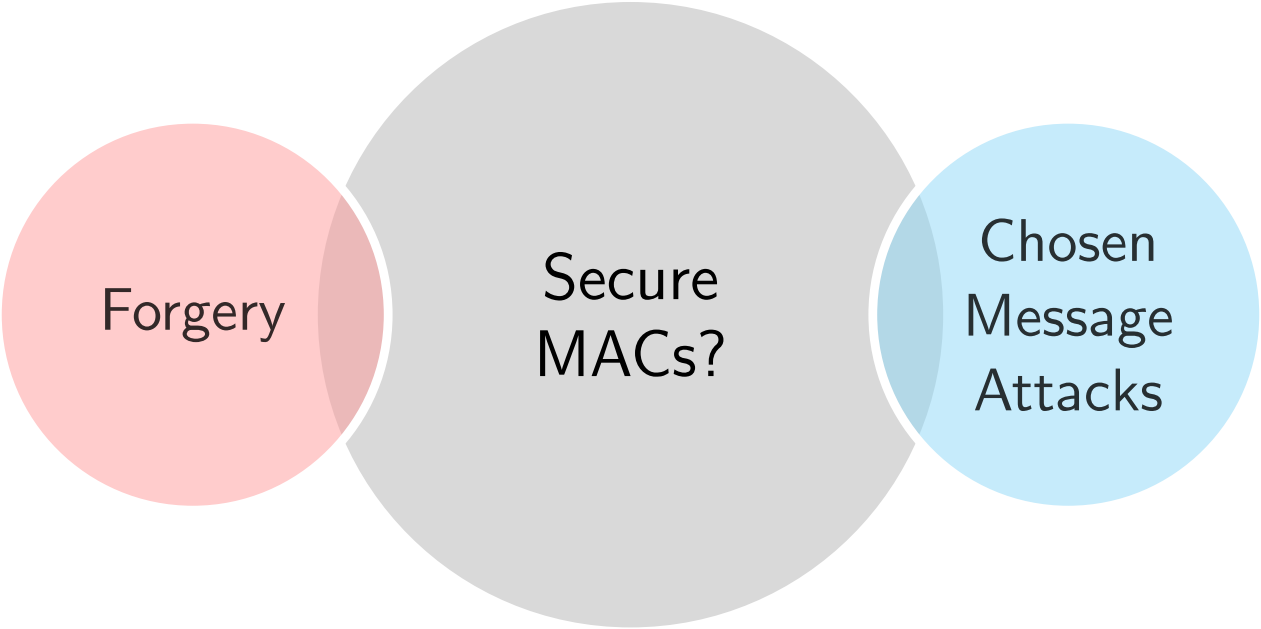
Generate a MAC for each network packet transmitted

- Internet Protocol Security (IPSec)
- Secure Shell (SSH)
- Transport Layer Security (TLS)

Ciphertext expansion adds overhead

- MAC not generated in 3G and 4G mobile telephony standards
- Whats the implication?

Security of MACs



Forgery

- Generating new message/tag pair

Attack Model

- Known Message Attack
- Chosen Message Attack

Replay Attacks

- What's a replay attack?

Why?

- MACs vulnerable to replay attacks
- What's the strategy to handle this?

Pseudorandom Functions (PRFs)

A PRF is a function that uses a secret key to return $PRF(K, M)$ such that the output looks random.

Used as part of other cryptographic primitive

- To make block ciphers
- Key derivation schemes
- Identification schemes
  - Generate a response from a random challenge.

Security Notion

Indistinguishability from a <u>random</u> function.

How?

MACs have weaker security requirements

Any secure PRF is also a secure MAC

If a PRF's outputs can't be distinguished from random strings, the implication is that their values can't be guessed which implies **unforgeability** and hence a secure MAC.

- Is the converse true?

Example (PRF $\rightarrow$ PRF2 from secure PRF $\rightarrow$ PRF1)

$$PRF2(K, M) = PRF1(K, M)||0$$

Keyed Hashes $\leftarrow$ Unkeyed Hashes

The Secret-Prefix Construction

$$\text{Hash}(K \mid\mid M)$$

Vulnerabilities

- Length Extension Attacks
- Different Key Lengths (HomeWork)

The Secret-Suffix Construction

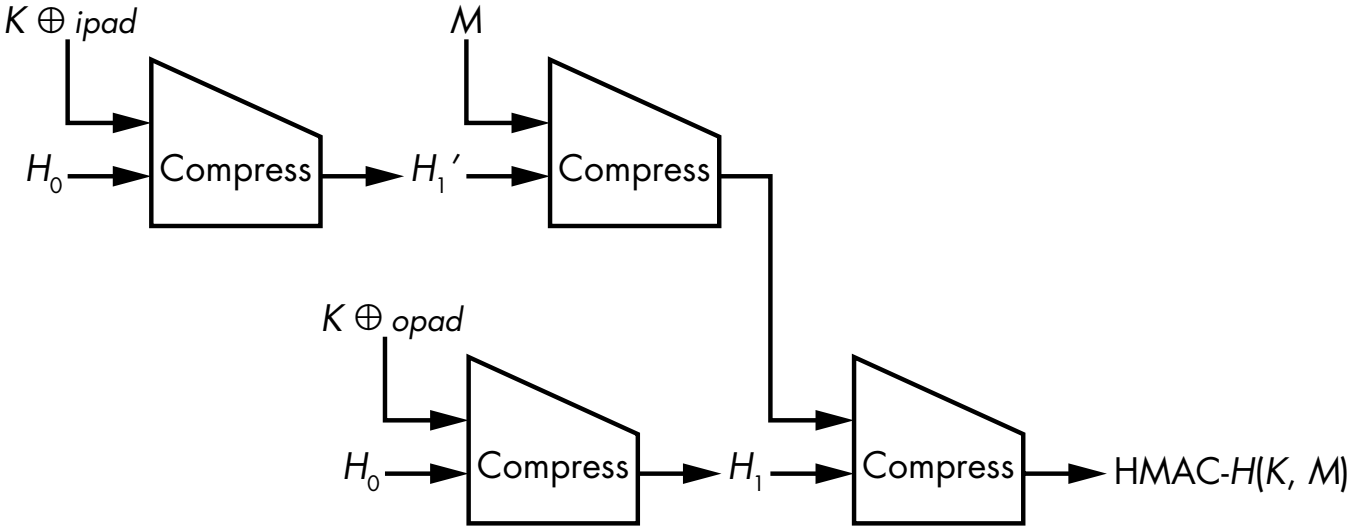
$$\text{Hash}(M \mid\mid K)$$

Vulnerabilities

- ~~Length Extension Attacks~~
- Colliding Messages $\implies$ forgery

The HMAC Construction

$$Hash((K \oplus opad) \,||\, Hash((K \oplus ipad) \,||\, M))$$

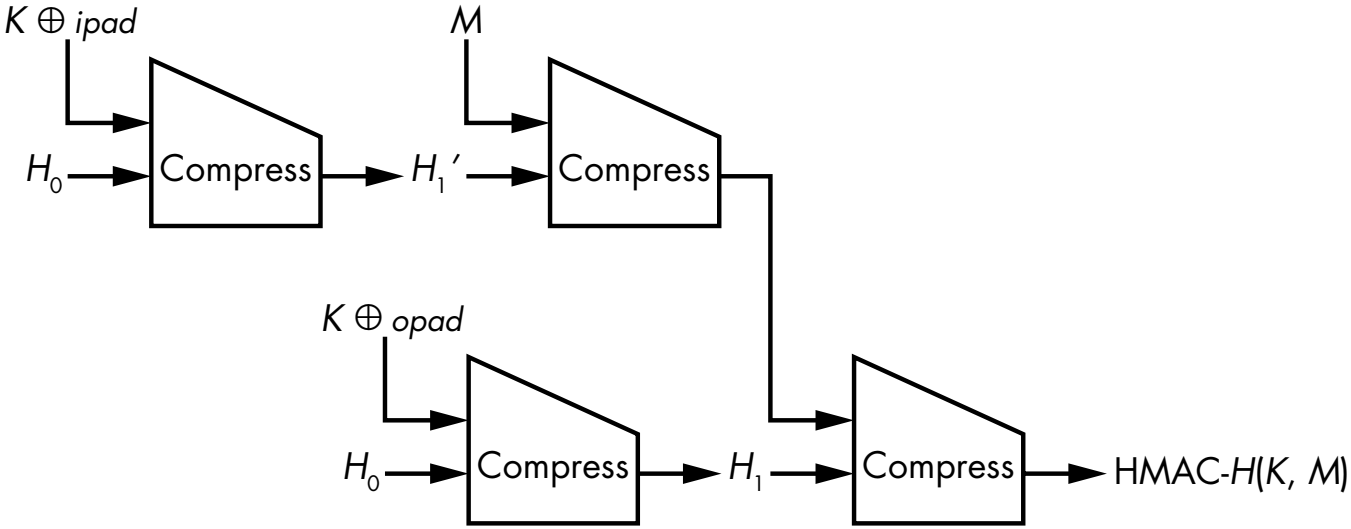


Envelope Mode

$$Hash(K||M||K)$$

The HMAC Construction

$$Hash((K \oplus opad) \,||\, Hash((K \oplus ipad) \,||\, M))$$



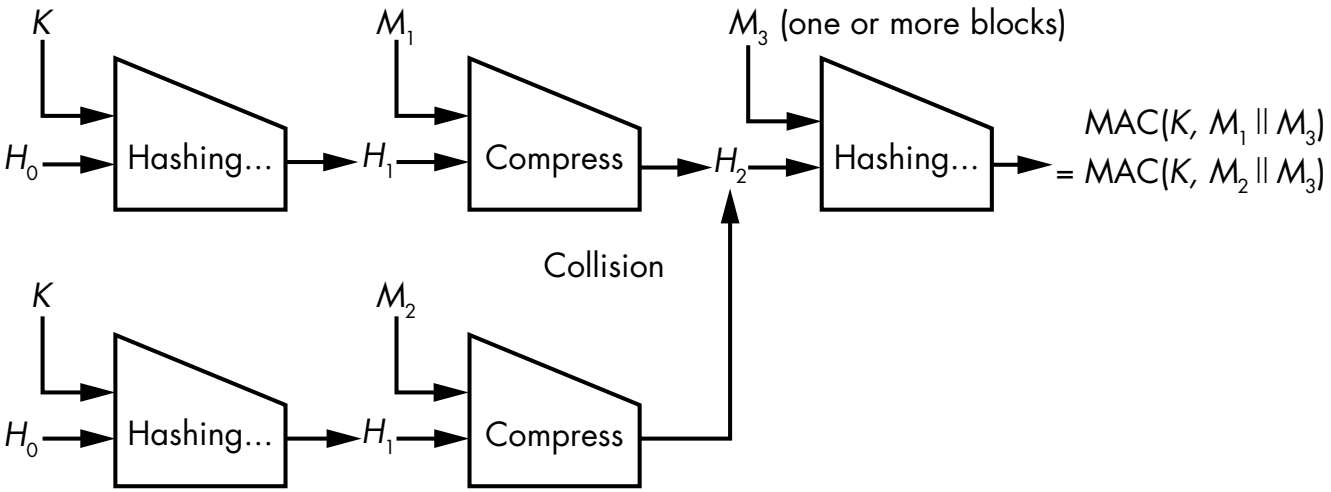
Envelope Mode

$$Hash(K||M||K)$$

Generic Attack Against Hash-Based MACs

Cost? $2^{\frac{n}{2}}$ MAC Tags

Use a hash collision to get a collision of MACs



The principle of the generic forgery attack on hash-based MACs

How? HomeWork

This attack will work even if the hash function is **not** vulnerable to length extension, and it will work for **HMAC**, too.

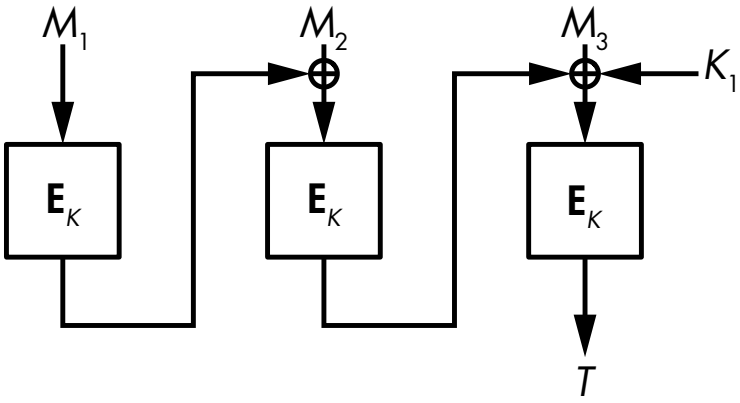
CMAC

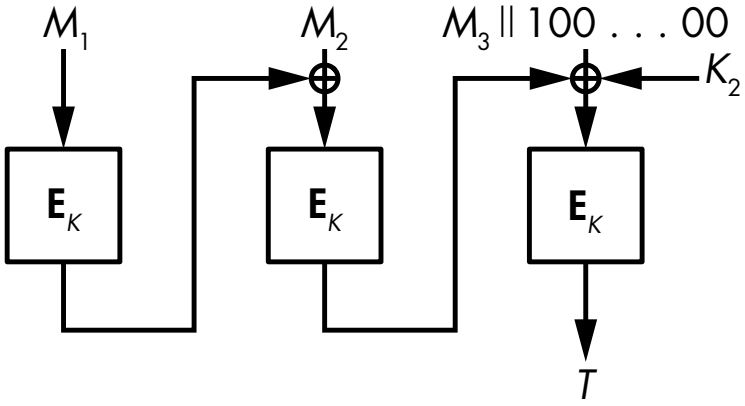
Cipher-based MAC

- CMAC → successor of CBC-MAC
- Recall CBC mode of operation
- What is the problem with CBC-MAC?

- Forgery with CBC-MAC

Based on M being a sequence of integral blocks or not





Note

Unlike the CBC encryption mode, CMAC does not take an IV as a parameter and is deterministic. Can you justify this?

HomeWork

- Side Channel Attacks on MACs