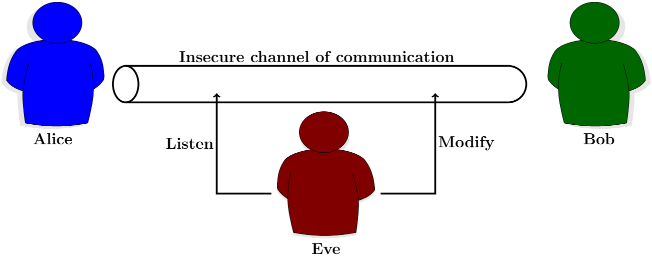
Hash Functions and Message Authentications

University of Birmingham

Outline of This Lecture

- Error Detection and non-cryptographic solutions
- Cryptographic Hash Functions
- Security of Hash Functions
- Message Authentication

Model



- Alice and Bob needs to communicate “correctly”.
- Example: Downloaded software may be corrupt.

Error Detection in Communication

- Communications are prone to error as the channel is untrusted

Error Detection in Communication

- Communications are prone to error as the channel is untrusted
- IDEA: Add a checksum after the string
- Parity Bits: 1-bit error detection
- Cyclic Redundancy Check: Algebraic Error Detection

Hash Functions

A Hash function is a function from $\{0,1\}^* \rightarrow \{0,1\}^n$, where n is a fixed integer.

Hash Functions

A Hash function is a function from $\{0,1\}^* \rightarrow \{0,1\}^n$, where n is a fixed integer.

- Practical hash functions have an upper bound μ on input message length with $\mu >> n$.

Hash Functions in Cryptography

- **Collision Attack.** If adversary could find *distinct* messages, m and m' such that $H(m) = H(m')$.
- **Preimage Attack.** Given a random $y \in \{0,1\}^n$, if the adversary could find a message m such that $H(m) = y$.

Hash Functions in Cryptography

- **Collision Attack.** If adversary could find *distinct* messages, m and m' such that $H(m) = H(m')$.
- **Preimage Attack.** Given a random $y \in \{0,1\}^n$, if the adversary could find a message m such that $H(m) = y$.

The idea of *Length Extension Attack* is also attributed to hash function.

Hardness of Collision Attack

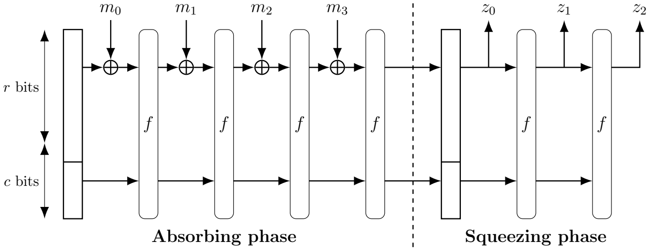
Hash Functions have collisions

For a secure hash function $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$, finding collision should take approximately $2^{n/2}$ computations.

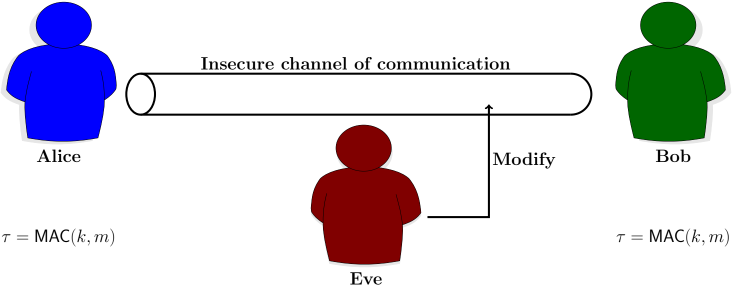
Usage of Cryptographic Hash Functions

- Hash functions are useful where only the message (without the checksum) is transferred via the channel, and the receiver can compute and compare the checksum

Design of Cryptographic Hash: SHA3



Message Authentication Codes



Insecure channel of communication

Alice

Modify

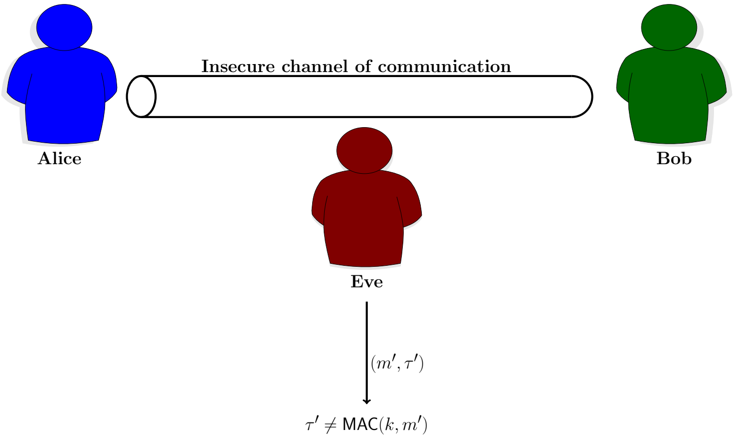
Bob

$\tau = \mathsf{MAC}(k, m)$

Eve

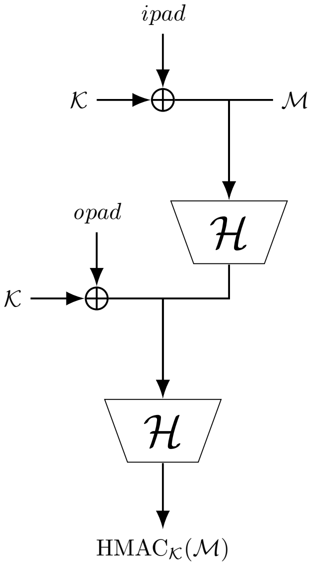
$\tau = \mathsf{MAC}(k, m)$

Message Authentication Codes: Security

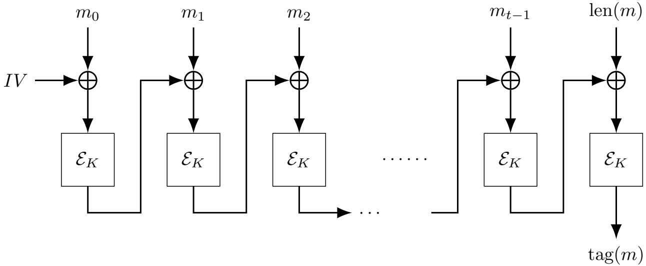


$\tau' \neq \mathsf{MAC}(k, m')$

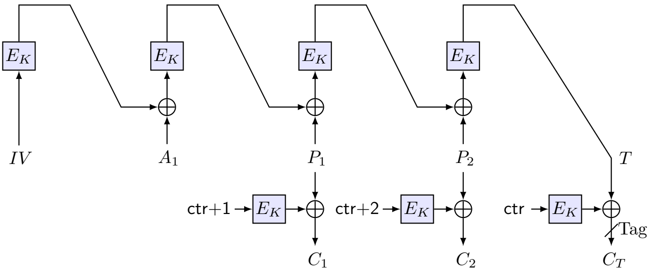
MAC design:HMAC



MAC design: CBC-MAC



Authenticated Encryption:CCM



A_1 is auxiliary data, initialized to 0^n.