Authenticated Encryption

Rohit Musti

CUNY - Hunter College

February 23, 2022

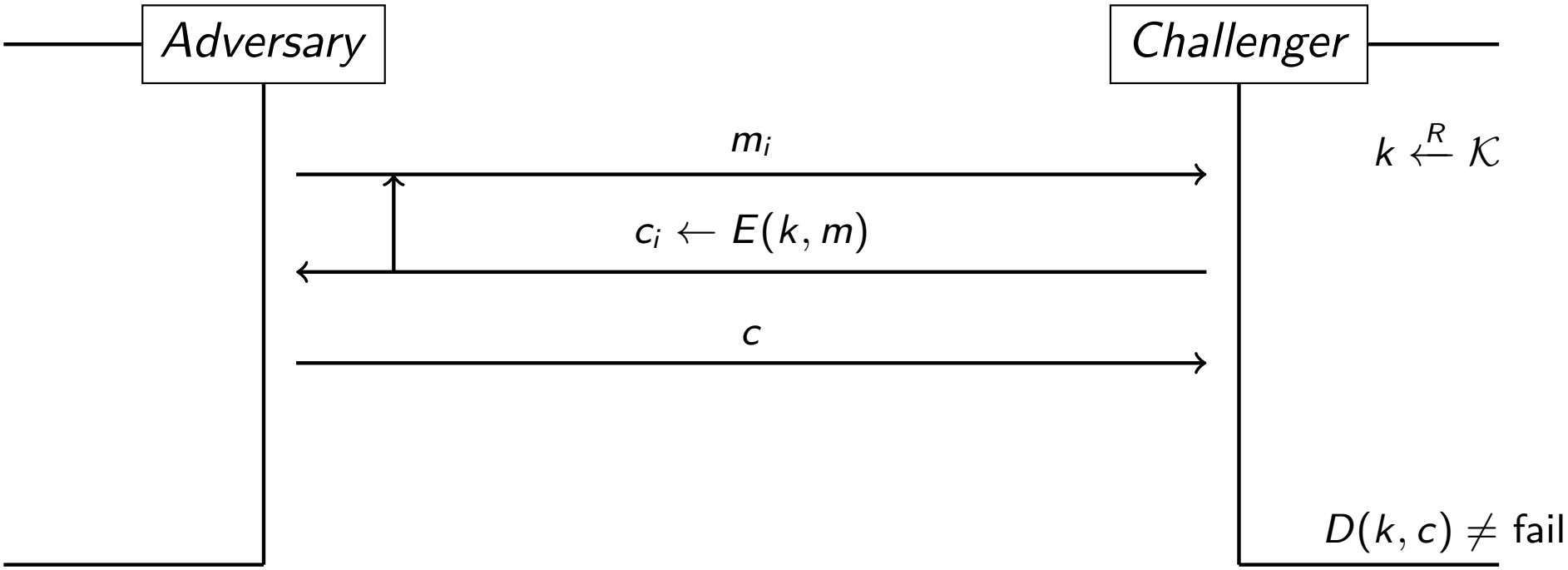
Authenticated Encryption Motivation

- Up until now we have considered systems that provide either message secrecy or integrity separately
- A system is said to provide authenticated encryption if it provides both message secrecy and integrity!
- At the end of this lecture, you will be empowered to analyze and construct authenticated encryption systems!

Basic Authenticated Encryption System

- We can use generic composition techniques to combine separate encryption and integrity schemes into an authenticated encryption scheme
- Let E, D be a cipher, k_c be the cipher key, S, V be a MAC, and k_m be the MAC key
- An integrated scheme builds directly ontop of cryptographic primitives without first constructing either a cipher of a MAC

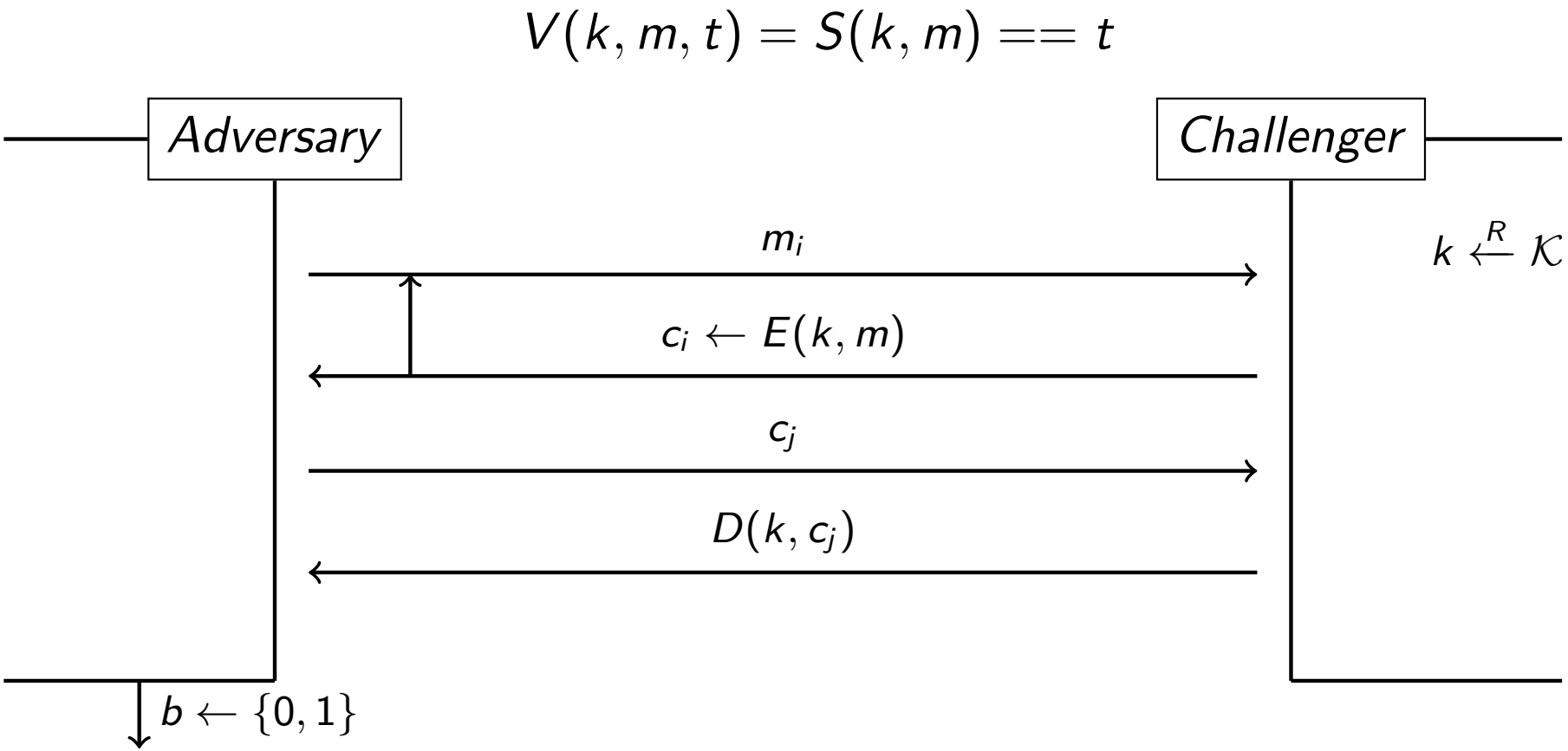
Cipher Text Integrity Game



Why is Cipher Text Integrity important?

- Suppose Alice emails Bob and every message starts with "To:bob@aol.com" and the mail servers knows to forward the plaintext message encrypted with Bob's key to Bob
- An attacker can intercept the message and modify the beginning to say "To: attacker@aol.com", the mail server will then forward the plaintext message encrypted with the Attacker's key to the Attacker
- If we an AE cipher (aka cipher text integrity secure cipher), then Mel cannot produce a valid modified cipher text

Chosen Ciphertext Attack (CCA) Game



MAC Then Encrypt

- generally not very secure
- SSL (precursor to TLS) used a randomized CBC and a secure MAC, attacks were able to decrypt all traffic
- This was due to padding errors