



Authenticated Encryption

Definitions

Goals


An **authenticated encryption** system (E,D) is a cipher where

As usual: $E: K \times M \times N \rightarrow C$

but $D: K \times C \times N \rightarrow M \cup \{\perp\}$

Security: the system must provide

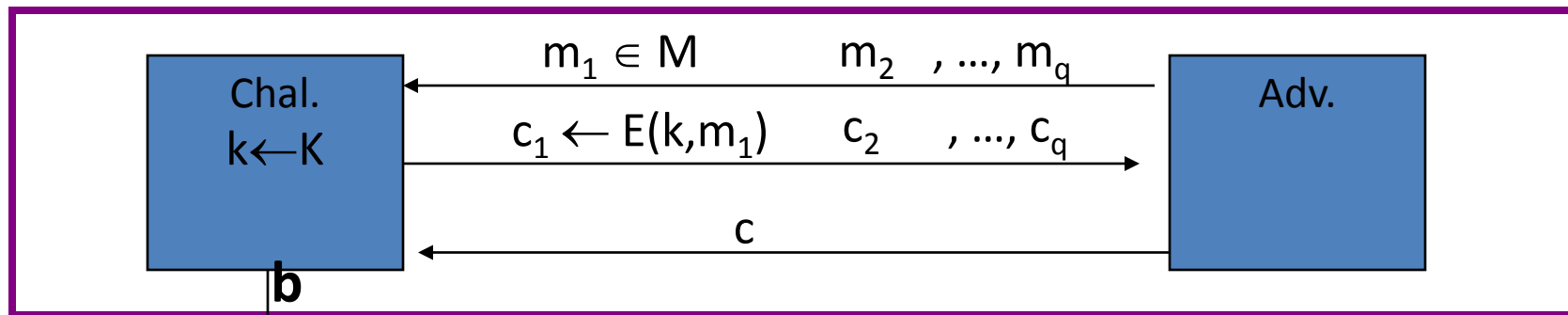
- sem. security under a CPA attack, and
- **ciphertext integrity**:
attacker cannot create new ciphertexts that decrypt properly



ciphertext
is rejected

Ciphertext integrity

Let (E,D) be a cipher with message space M .



$$\begin{cases} b=1 & \text{if } D(k,c) \neq \perp \text{ and } c \notin \{c_1, \dots, c_q\} \\ b=0 & \text{otherwise} \end{cases}$$

Def: (E,D) has **ciphertext integrity** if for all “efficient” A :

$$\text{Adv}_{\text{CI}}[A,E] = \Pr[\text{Chal. outputs 1}] \text{ is “negligible.”}$$

Authenticated encryption

Def: cipher (E,D) provides authenticated encryption (AE) if it is

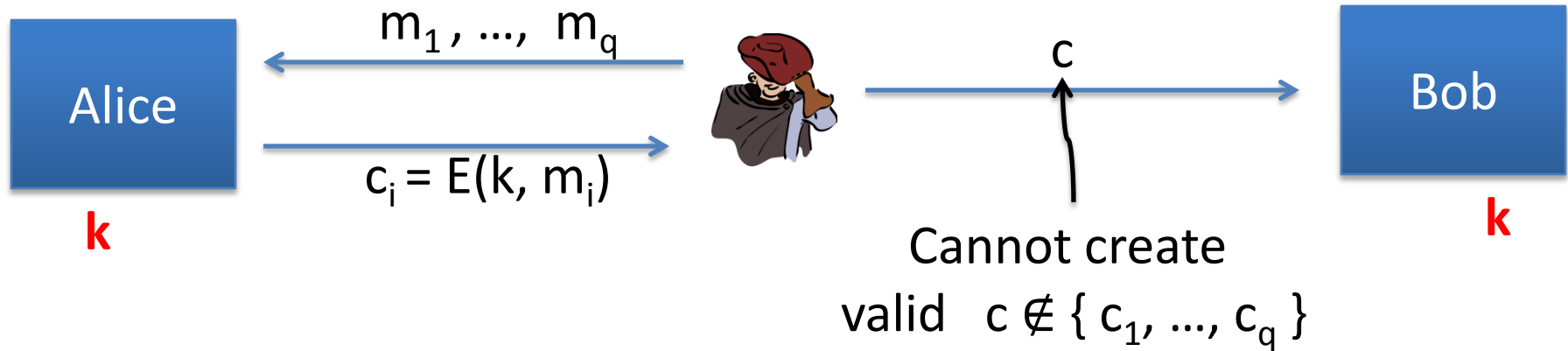
- (1) semantically secure under CPA, and
- (2) has ciphertext integrity

Bad example: CBC with rand. IV does not provide AE

- $D(k,\cdot)$ never outputs \perp , hence adv. easily wins CI game

Implication 1: authenticity

Attacker cannot fool Bob into thinking a message was sent from Alice



\Rightarrow if $D(k, c) \neq \perp$ Bob knows message is from someone who knows k
(but message could be a replay)

Implication 2

Authenticated encryption \Rightarrow

Security against **chosen ciphertext attacks**
(next segment)

End of Segment