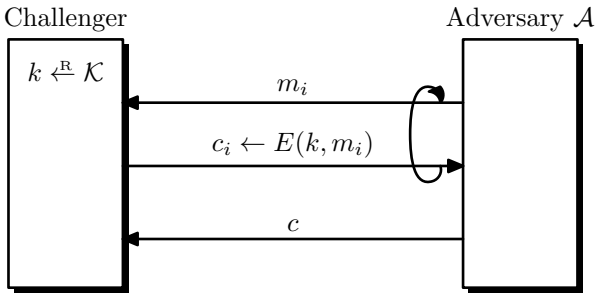

Figure 9.2: Ciphertext integrity game (Attack Game 9.1)

- $\mathcal{A}$ queries the challenger several times. For $i = 1, 2, \ldots$, the ith query consists of a message $m_i \in \mathcal{M}$. The challenger computes $c_i \xleftarrow{R} E(k, m_i)$, and gives c_i to $\mathcal{A}$.
- Eventually $\mathcal{A}$ outputs a candidate ciphertext $c \in \mathcal{C}$ that is not among the ciphertexts it was given, i.e.,

$$c \notin \{c_1, c_2, \ldots\}.$$

We say that $\mathcal{A}$ wins the game if c is a valid ciphertext under k, that is, $D(k, c) \neq \mathsf{reject}$. We define $\mathcal{A}$'s advantage with respect to $\mathcal{E}$, denoted $\mathrm{CI}\mathsf{adv}[\mathcal{A}, \mathcal{E}]$, as the probability that $\mathcal{A}$ wins the game. Finally, we say that $\mathcal{A}$ is a **Q-query adversary** if $\mathcal{A}$ issues at most Q encryption queries. □

Definition 9.1. *We say that a $\mathcal{E} = (E, D)$ provides **ciphertext integrity**, or* CI *for short, if for every efficient adversary $\mathcal{A}$, the value* $\mathrm{CI}\mathsf{adv}[\mathcal{A}, \mathcal{E}]$ *is negligible.*

CPA security and ciphertext integrity are the properties needed for authenticated encryption. This is captured in the following definition.

Definition 9.2. *We say that a cipher $\mathcal{E} = (E, D)$ provides **authenticated encryption**, or is simply **AE-secure**, if $\mathcal{E}$ is (1) semantically secure under a chosen plaintext attack, and (2) provides ciphertext integrity.*

Why is Definition 9.2 the right definition? In particular, why are we requiring *ciphertext* integrity, rather than some notion of *plaintext* integrity (which might seem more natural)? In Section 9.2, we will describe a very insidious class of attacks called *chosen ciphertext attacks*, and we will see that our definition of AE-security is sufficient (and, indeed, necessary) to prevent such attacks. In Section 9.3, we give a more high-level justification for the definition.

9.1.1 One-time authenticated encryption

In practice, one often uses a symmetric key to encrypt a single message. The key is never used again. For example, when sending encrypted email one often picks an ephemeral key and encrypts the email body under this ephemeral key. The ephemeral key is then encrypted and transmitted in the email header. A new ephemeral key is generated for every email.

In these settings one can use a one-time encryption scheme such as a stream cipher. The cipher must be semantically secure, but need not be CPA-secure. Similarly, it suffices that the