Authenticated Encryption

Purpose of AE

Provide both secrecy guarantees of secure ciphers and authenticity guarantees of MACs.

In general, to obtain both $\rightarrow$ use an appropriate combination of encryption and MACing.
Several possible combinations, not all of them secure?

Purpose of AE

Provide both secrecy guarantees of secure ciphers and authenticity guarantees of MACs.

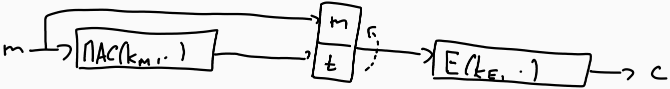
In general, to obtain both → use an appropriate combination of encryption and MACing.
Several possible combinations, not all of them secure?

- Encrypt-then-MAC

  ✓

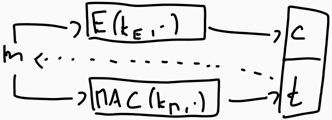
- MAC-then-encrypt

  ok



- Encrypt-and-MAC

  ✗



Instead of requiring the user to construct the correct combination manually, AE aims to provide a single primitive with both secrecy/authenticity guarantees.

Ciphers for AE

Definition 1: Cipher for AE

An AE-enabled cipher over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ is a tuple $\mathcal{E} = (E, D)$, where

- $E : \mathcal{K} \times \mathcal{M} \to \mathcal{D}(\mathcal{C})$ is a (possibly probabilistic) encryption algorithm
- $D : \mathcal{K} \times \mathcal{C} \to \mathcal{M} \cup \{\bot\}$ is a decryption algorithm s.t. for all $k \in \mathcal{K}, m \in \mathcal{M}$ it holds

$$D(k, E(k, m)) = m.$$

"reject"

AE Security

Definition 2: AE Security

Let $\mathcal{E}$ be an AE-enabled cipher. We say that $\mathcal{E}$ is (ε, δ)-AE secure if:

- $\mathcal{E}$ is ε-CPA secure; and
- $\mathcal{E}$ has an δ-ciphertext integrity (see next slide)

AE-secure ciphers provide security against both chosen plaintext and chosen ciphertext attacks (CCAs).

Ciphertext integrity attack game

Let $\mathcal{E} = (E, D)$ be an AE-enabled cipher over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$. The ciphertext integrity attack game between the challenger and the adversary $\mathcal{A}$ proceeds as follows:

- The challenger samples a key $k \in \mathcal{K}$ uniformly at random.
- $\mathcal{A}$ chooses a number of rounds N of the game. In each round $1 \leq i \leq N$:
  - $\mathcal{A}$ computes a message $m_i \in \mathcal{M}$ and sends it to the challenger;
  - the challenger computes $c_i = E(k, m_i)$ and sends c_i to the adversary.
- After the final round, $\mathcal{A}$ computes a ciphertext $c \in \mathcal{C}$ such that $c \notin \{c_1, c_2, \ldots, c_N\}$.

$\mathcal{A}$ wins the game if $D(k, c) \neq \bot$. We denote by $\mathbb{P}$ the probability measure corresponding to the game.

The CI-advantage of $\mathcal{A}$ against $\mathcal{E}$ is the quantity

$$ADV_{CI}(\mathcal{E}, \mathcal{A}) = \mathbb{P}(\mathcal{A} \text{ wins the AE attack game}).$$

We say that $\mathcal{E}$ has δ-ciphertext integrity if $ADV_{CI}(\mathcal{E}, \mathcal{A}) \leq \delta$ for all efficient adversaries $\mathcal{A}$.

AE Security

Definition 2: AE Security

Let $\mathcal{E}$ be an AE-enabled cipher. We say that $\mathcal{E}$ is (ε, δ)-AE secure if:

- $\mathcal{E}$ is ε-CPA secure; and
- $\mathcal{E}$ has an δ-ciphertext integrity (see next slide)

AE-secure ciphers provide security against both chosen plaintext and chosen ciphertext attacks (CCAs).

CCA attack game

Let (E, D) be a cipher over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$. The CCA attack game against (E, D) is played as follows:

Stage 1:

- The challenger samples a key $k \in \mathcal{K}$ and a bit $i \in \{0, 1\}$, both uniformly at random. Neither is revealed to the adversary.
- The adversary announces a number of rounds q for which the game will be played.

CCA attack game

Let (E, D) be a cipher over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$. The CCA attack game against (E, D) is played as follows:

Stage 2:

- In each round $1 \leq j \leq q$, the adversary chooses to perform either a plaintext query ciphertext query:
  - Plaintext query: the adversary computes two messages, m_0^j and m_1^j of the same length and sends them to the challenger, who responds with $c^j = E(k, m_i^j)$.
  - Ciphertext query: the adversary computes $c_i' \in \mathcal{C}$ s.t.

$$c_i' \notin \{c_j \mid \text{plaintext query was done in round } j < i\},$$

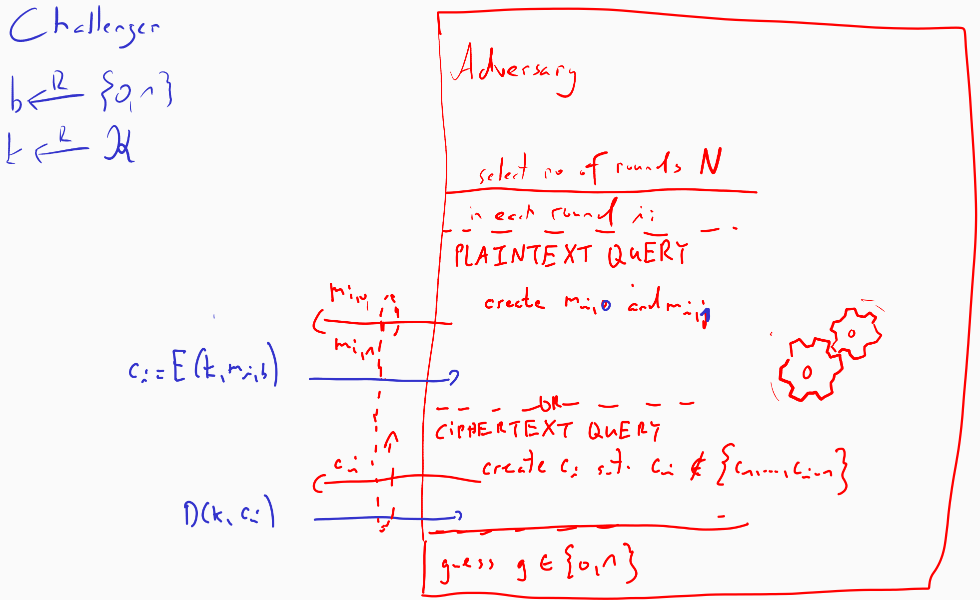
and sends c_i' to the challenger, who responds with $m_i' = D(k, c_i')$.

Stage 3:

- Finally, adversary outputs a guess $g \in \{0, 1\}$.

The adversary wins the game if $g = i$, otherwise it loses.

CCA attack game: picture



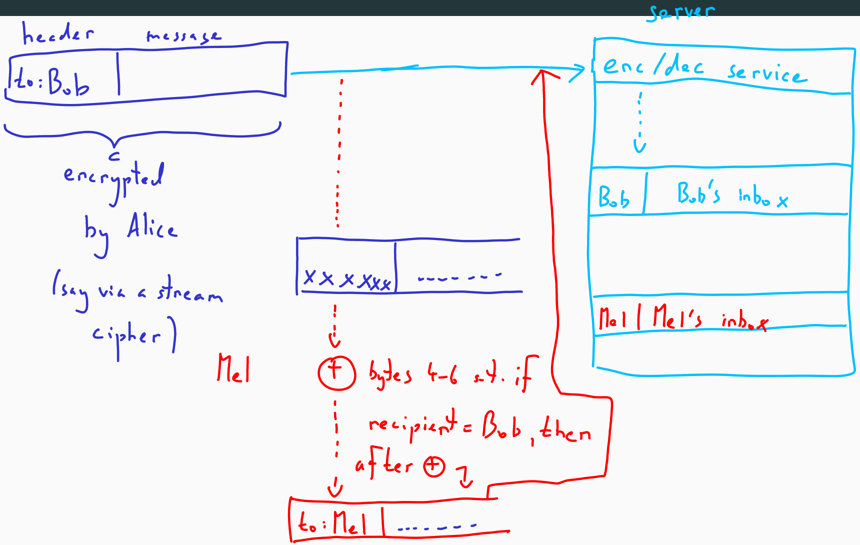
CCA security

We define the CCA advantage of $\mathcal{A}$ against $\mathcal{E}$ as the quantity

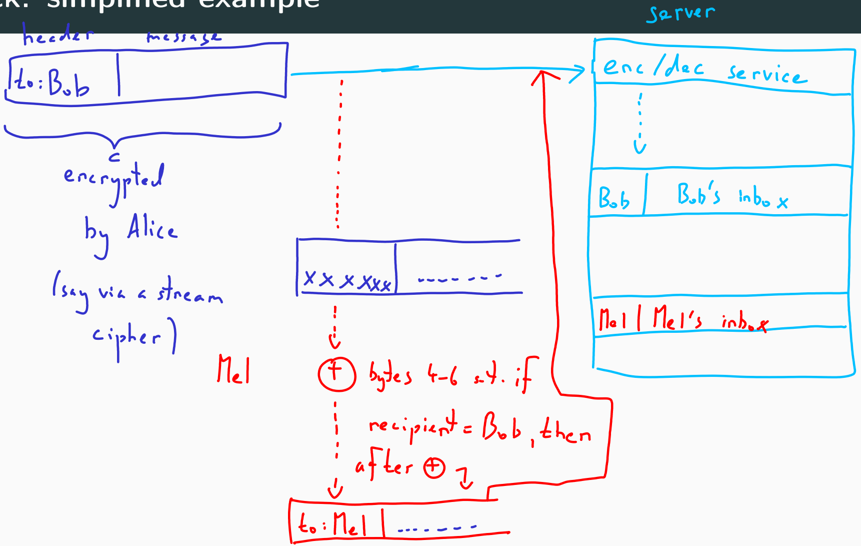
$$\mathcal{ADV}_{\mathcal{CCA}}(\mathcal{E}, \mathcal{A}) = |\mathbb{P}(\mathcal{A} \text{ wins the game against } \mathcal{E}) - \frac{1}{2}|.$$

We say that $\mathcal{E}$ is an ε-CCA secure cipher (where $\varepsilon > 0$) if for every efficient adversary it holds $ADV_{CCA}(\mathcal{E}, \mathcal{A}) \leq \varepsilon$.

CC attack: simplified example



CC attack: simplified example



For a practical example, see, e.g. the padding oracle CC attack POODLE (2014) completely breaking the security of SSL 3.0 (CBC-based MAC-then-encrypt).

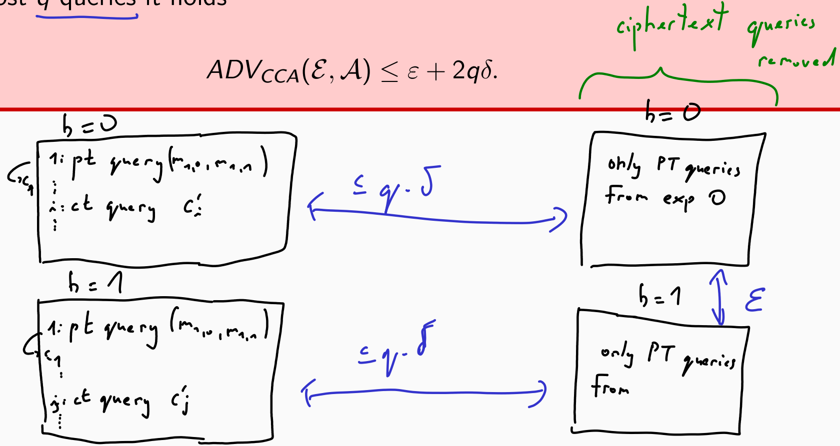
AE security provides CCA security

Theorem 1

Let $\mathcal{E} = (E, D)$ be an (ε, δ)-AE secure cipher. Then, for any efficient adversary $\mathcal{A}$ who makes at most q queries it holds

$$ADV_{CCA}(\mathcal{E}, \mathcal{A}) \leq \varepsilon + 2q\delta.$$

Proof sketch:



MAC-then-Encrypt

Definition 3: MAC-then-Encrypt (MtE) system

Let $MAC = (S, V)$ be a MAC over $(\mathcal{M}, \mathcal{H}, \mathcal{K}_M)$ and let $\mathcal{E} = (E, D)$ be a (classical) cipher over $(\mathcal{M} \times \mathcal{H}, \mathcal{C}, \mathcal{K}_E)$. An *MtE* system built from MAC and $\mathcal{E}$ is an AE-enabled cipher $\mathcal{E}_{MtE} = (E_{MtE}, D_{MtE})$ over $(\mathcal{M}, \mathcal{C}, \mathcal{K}_M \times \mathcal{K}_E)$ defined as follows:

- for every $m \in \mathcal{M}$, $(k_M, k_E) \in \mathcal{K}_M \times \mathcal{K}_E$ we put

$$E_{MtE}((k_M, k_E), m) = E(k_E, (m, S(k_M, m)))$$

- for every $c \in \mathcal{C}$, $(k_M, k_E) \in \mathcal{K}_M \times \mathcal{K}_E$, the decryption process $D_{MtE}((k_M, k_E), c)$:
  - first computes $(m, t) = D(k_E, c)$ (and outputs $\perp$ if $(m, t) \notin \mathcal{M} \times \mathcal{H}$)
  - checks that $V(k_M, m, t) = true$; if yes, the procedure outputs m, otherwise it outputs $\perp$.

MtE security

MtE systems generally do not provide AE security (see the POODLE attack against SSL 3.0). However, security guarantees can be recovered for certain underlying ciphers and additional assumptions.

Theorem 2

Let $\mathcal{E}$ be an ε-CPA secure cipher which is a randomized counter mode of some block cipher over the block space $\mathcal{X}$. Moreover, let *MAC* be an α-one-time secure MAC. Then, when restricting to adversaries that make at most q queries, the MtE system built from *MAC* and $\mathcal{E}$ is (ε, δ)-AE-secure for

$$\delta = \frac{q^2}{2|\mathcal{X}|} + (q+1) \cdot \alpha$$

For randomized CBC mode + secure MAC, similar theorem can be obtained assuming that $m \,||\, t$ is never padded (all messages consist of full blocks, tag one full block).

MtE advice

Nevertheless, due to the difficulty of implementing an MtE system correctly, its usage (in particular the design of new primitives based on this approach) is discouraged.

Encrypt-then-MAC

Definition 4: Encrypt-theh-MAC (EtM) system

Let $\mathcal{E} = (E, D)$ be a (classical) cipher over $(\mathcal{M}, \mathcal{C}, \mathcal{K}_E)$ and let $MAC = (S, V)$ be a MAC over $(\mathcal{C}, \mathcal{H}, \mathcal{K}_M)$. An *EtM* system built from $\mathcal{E}$ and MAC is an AE-enabled cipher $\mathcal{E}_{EtM} = (E_{EtM}, D_{EtM})$ over $(\mathcal{M}, \mathcal{C} \times \mathcal{H}, \mathcal{K}_E \times \mathcal{K}_M)$ defined as follows:

- for every $m \in \mathcal{M}$, $(k_E, k_M) \in \mathcal{K}_E \times \mathcal{K}_M$ we put

$$E_{EtM}((k_E, k_M), m) = (E(k_E, m), S(k_M, E(k_E, m)))$$

- for every $(c, t) \in \mathcal{C} \times \mathcal{H}$, $(k_E, k_M) \in \mathcal{K}_E \times \mathcal{K}_M$, the decryption process $D_{MtE}((k_E, k_M), (c, t))$:
  - first computes $m = D(k_E, c)$ and then checks whether $V(k_M, m, t) = true$; if yes, the procedure outputs m, otherwise it outputs $\perp$.

EtM security

Theorem 3

Let $\mathcal{E}$ be an ε-CPA secure cipher, and let *MAC* be a δ-secure MAC. Then, when restricting to adversaries the EtM system built from *MAC* and $\mathcal{E}$ is (ε, δ)-AE-secure.

Practical AE-enabled ciphers

random

$(r, E(k_1, r) \oplus S_{ot}(k_2, m))$

Typically dedicated modes of block ciphers:

- EAX: basically nonce-based CTR then CMAC.
- CCM: CBC-MAC then nonce-based CTR encryption (e.g. WiFi traffic)
- GCM: Galois counter mode, nonce-based CTR then a Carter-Wegman-style MAC based using the GHASH one-time MAC (like the polynomial MAC from previous lecture but working over an appropriate Galois field rather than over $\mathbb{Z}_p$)
  - fastest, in particular using the acceleration via the PCLMULQDQ instruction

OCB

Authenticated encryption with associated data

1. All the state-of-the-art AE modes do support authenticated encryption with associated data (AEAD).
   - message - encrypted and authenticated
   - associated data - only authenticated