Suppose H is a Merkle-Damgård hash function built from a <u>secure</u> compression function

Several ways to build a keyed function:

1. Prepend key: $F(k, m) := H(k \| m)$
   ↳ Insecure due to structure of Merkle-Damgård: can mount an "extension attack:" given $H(k \| m)$, can compute $H(k \| m \| m')$ by extending Merkle-Damgård chain
2. Append key: $F(k,m) := H(m \| k)$
   ↳ Similar to hash-then-MAC construction and vulnerable to same offline attack: adversary finds a collision in the Merkle-Damgård prefix and uses that to construct a forgery
      ↳ Structure exploited in SHA-1 collision demonstration (can generate <u>arbitrary</u> collisions once prefix matches) → for SHA-1, they used PDF files
3. Envelope method: $F(k,m) := H(k \| m \| k)$
4. Two-key nest: $F((k_1, k_2), m) := H(k_2 \| H(k_1 \| m))$

} for reasonable pseudorandomness assumptions on h (e.g., both $F_1(k,m) := h(k,m)$ and $F_2(k,m) := h(m,k)$ is a PRF), both of these constructions are secure PRFs on a variable-size domain

hash-based MAC

HMAC is a PRF/MAC based on the two-key nest (though with correlated keys):

$$\mathrm{HMAC}(k, m) := H(k_1 \| H(k_2, m))$$

where $k_1 \leftarrow k \oplus \text{ipad}$ and $k_2 \leftarrow k \oplus \text{opad}$

and ipad and opad are fixed strings (specified in the HMAC standard)

ipad: 0x36 repeated; opad: 0x5C repeated

<u>Security</u>: Since k_1 and k_2 are correlated, need to make stronger assumption on security (e.g., h remains pseudorandom under a <u>related-key</u> attack)

<u>Instantiations</u>: Typically, denoted HMAC-H where H is the hash function

e.g., HMAC-SHA1

HMAC-SHA256 — one of the most widely-used MAC on the web (used in SSL/TLS, IPsec, SSH, and more)

<u>HMAC for key-derivation</u>: Recall that under reasonable assumptions, HMAC is a secure PRF

In many protocols, we need to derive multiple keys from a single master key (e.g., derived from a password)

↳ To derive multiple independent cryptographic keys, a PRF is a natural primitive:

$$k_{enc} \leftarrow \mathrm{HMAC}(k_{master}, \text{"enc"})$$
$$k_{mac} \leftarrow \mathrm{HMAC}(k_{master}, \text{"mac"})$$

} PRF security says derived keys are computationally indistinguishable from uniform

derived keys — master key — tag (just has to be unique)

This approach is used in TLS and IPsec to derive session keys durin session setup

↳ General paradigm is the "expand" step in hash-based key-derivation (HKDF — RFC 5869)

↳ Consists of two procedures:

- <u>Extract</u>: derive a master key from entropy source (e.g., a user password)
- <u>Expand</u>: derive sub-keys from the master key

Both steps rely on HMAC

How do we <u>combine</u> confidentiality and integrity?

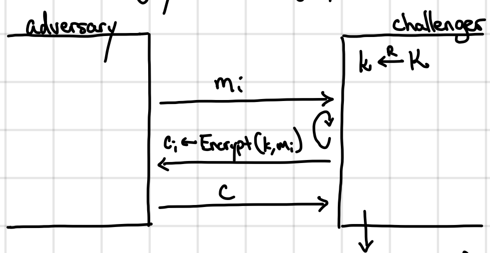
↳ Systems with both guarantees are called <u>authenticated encryption</u> schemes — gold standard for symmetric encryption

<u>Two natural options</u>:

1. Encrypt-then MAC (TLS 1.2+, IPsec) ← guaranteed to be secure if we instantiate using CPA-secure encryption and a secure MAC
2. MAC-then-encrypt (SSL 3.0/TLS 1.0, 802.11i) ← as we will see, <u>not</u> always secure

<u>Definition.</u> An encryption scheme $\Pi_{SE} = (\text{Encrypt}, \text{Decrypt})$ is an authenticated encryption scheme if it satisfies the following two properties:

- CPA security [confidentiality]
- ciphertext integrity [integrity]



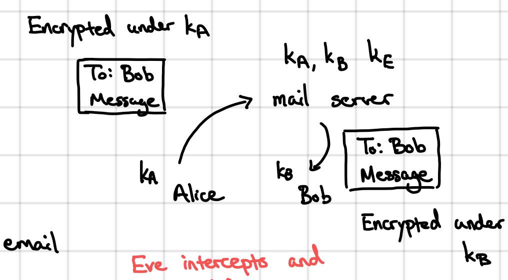
output 1 if $c \notin \{c_1, c_2, \dots\}$ and $\text{Decrypt}(k, c) \neq \bot$ ← special symbol $\bot$ to denote <u>invalid</u> ciphertext

Define $\text{CIAdv}[A, \Pi_{SE}]$ to be the probability that output of above experiment is 1. The scheme Π_{SE} satisfies ciphertext integrity if for all efficient adversaries A,

$$\text{CIAdv}[A, \Pi_{SE}] = \text{negl}(\lambda)$$

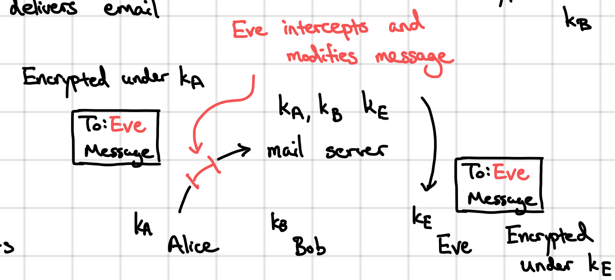
↑ security parameter determines key length

Ciphertext integrity says adversary cannot come up with a new ciphertext: only ciphertexts it can generate are those that are already valid. Why do we want this property?



Consider the following <u>active</u> attack scenario:

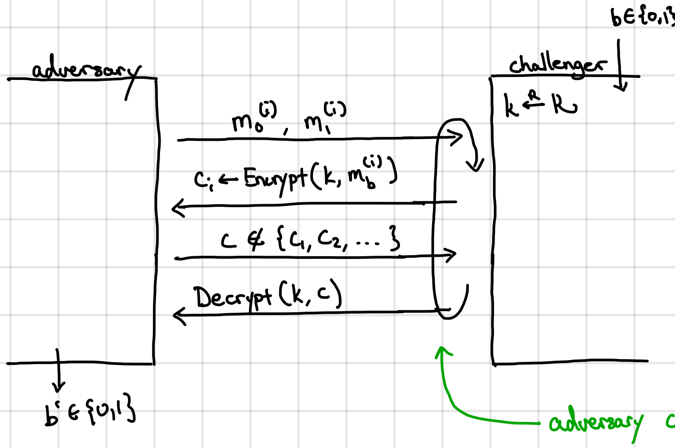
- Each user shares a key with a mail server
- To send mail, user encrypts contents and send to mail server
- Mail server decrypts the email, re-encrypts it under recipient's key and delivers email



If Eve is able to tamper with the encrypted message, then she is able to learn the encrypted contents (even if the scheme is CPA-secure)

↳ More broadly, an adversary can tamper and inject ciphertexts into a system and observe the user's behavior to learn information about the decrypted values — against active attackers, we need <u>stronger</u> notion of security

Definition. An encryption scheme $\Pi_{SE} = (\text{Encrypt}, \text{Decrypt})$ is secure against chosen-ciphertext attacks (CCA-secure) if for all efficient adversaries A, $\text{CCAAdv}[A, \Pi_{SE}] = \text{negl.}$ where we define $\text{CCAAdv}[A, \Pi_{SE}]$ as follows:



adversary can make arbitrary encryption and decryption queries, but cannot decrypt any ciphertexts it received from the challenger (otherwise, adversary can trivially break security)

↳ called an "admissibility" criterion

$$\text{CCAAdv}[A, \Pi_{SE}] = \left| \Pr[b' = 1 \mid b = 0] - \Pr[b' = 1 \mid b = 1] \right|$$

CCA-security captures above attack scenario where adversary can tamper with ciphertexts

↳ Rules out possibility of transforming encryption of $x \| z$ to encryption of $y \| z$

↳ Necessary for security against <u>active</u> adversaries [CPA-security is for security against <u>passive</u> adversaries]

↳ We will see an example of a real CCA attack in HW1

Theorem. If an encryption scheme Π_{SE} provide authenticated encryption, then it is CCA-secure.

Proof (Idea). Consider an adversary A in the CCA-security game. Since Π_{SE} provides ciphertext integrity, the challenger's response to the adversary's decryption query will be $\perp$ with all but negligible probability. This means we can implement the decryption oracle with the "output $\perp$" function. But then this is equivalent to the CPA-security game.

[Formalize using a "hybrid argument"]

simple counter-example: concatenate unused bits to end of ciphertext in a CCA-secure scheme (stripped away during decryption)

Note: Converse of the above is not true since CCA-security $\not\Rightarrow$ ciphertext integrity.

↳ However, CCA-security + plaintext integrity $\Rightarrow$ authenticated encryption

Take-away: Authenticated encryption captures meaningful confidentiality + integrity properties; provides <u>active</u> security

Encrypt-then-MAC: Let (Encrypt, Verify) be a CPA-secure encryption scheme and (Sign, Verify) be a secure MAC. We define Encrypt-then-MAC to be the following scheme:

$\text{Encrypt}'((k_E, k_M), m)$: $\quad c \leftarrow \text{Encrypt}(k_E, m)$

independent keys

$\qquad t \leftarrow \text{Sign}(k_M, c)$

$\qquad$ output (c, t)

$\text{Decrypt}'((k_E, k_M), (c, t))$: $\quad$ if $\text{Verify}(k_M, c, t) = 0$, output $\perp$

$\qquad$ else, output $\text{Decrypt}(k_E, c)$

Theorem. If (Encrypt, Decrypt) is CPA-secure and (Sign, Verify) is a secure MAC, then (Encrypt', Verify') is an authenticated encryption scheme

Proof. (Sketch). CPA-security follows by CPA-security of (Encrypt, Decrypt). Specifically, the MAC is computed on ciphertexts and not the messages. MAC key is independent of encryption key so cannot compromise CPA-security.

Ciphertext integrity follows directly from MAC security (i.e., any valid ciphertext must contain a new tag on some ciphertext that was not given to the adversary by the challenger)

Important notes:
- Encryption + MAC keys must be independent. Above proof required this (in the formal reduction, need to be able to simulate ciphertexts / MACs — only possible if reduction can chose its own key).
  - ↳ Can also give explicit constructions that are completely broken if same key is used (i.e., both properties fail to hold)
  - ↳ In general, never reuse cryptographic keys in different schemes; instead, sample fresh, independent keys!
- MAC needs to be computed over the entire ciphertext
  - Early version of ISO 19772 for AE did not MAC IV (CBC used for CPA-secure encryption)
  - RNCryptor in Apple iOS (for data encryption) also problematic (HMAC not applied to encryption IV)

  means first block (i.e., "header") is malleable

MAC-then-Encrypt: Let (Encrypt, Verify) be a CPA-secure encryption scheme and (Sign, Verify) be a secure MAC. We define MAC-then-Encrypt to be the following scheme:

Encrypt'$((k_E, k_M), m)$: $t \leftarrow \text{Sign}(k_M, m)$
$c \leftarrow \text{Encrypt}(k_E, (m,t))$
output c

Decrypt'$((k_E, k_M), (c,t))$: compute $(m,t) \leftarrow \text{Decrypt}(k_E, c)$
if $\text{Verify}(k_M, m, t) = 1$, output m, else, output $\perp$

Not generally secure! SSL 3.0 (precursor to TLS) used randomized CBC + secure MAC
↳ Simple CCA attack on scheme (by exploiting padding in CBC encryption)
[POODLE attack on SSL 3.0 can decrypt all encrypted traffic using a CCA attack]

Padding is a common source of problems with MAC-then-Encrypt systems [see HW1 for an example]

In the past, libraries provided separate encryption + MAC interfaces — common source of errors
↳ Good library design for crypto should minimize ways for users to make errors, not provide more flexibility

Today, there are standard block cipher modes of operation that provide authenticated encryption
- One of the most widely used is GCM (Galois counter mode) — standardized by NIST in 2007

GCM mode: follows encrypt-then-MAC paradigm
- CPA-secure encryption is nonce-based counter mode
- MAC is a Carter-Wegman MAC

Most commonly used in conjuction with AES (AES-GCM provides authenticated encryption)

Carter-Wegman MAC ("encrypted MAC"): very lightweight, randomized MAC:

- Let $H : \mathcal{K}_H \times \mathcal{M} \to \{0,1\}^n$ be a keyed hash function
- Let $F : \mathcal{K}_F \times \mathcal{R} \to \{0,1\}^n$ be a PRF

security relies on a mild assumption on the hash function and can be realized unconditionally
↳ security relies only on PRF security

The Carter-Wegman MAC is defined as follows:

$\text{Sign}((k_H, k_F), m)$: $r \xleftarrow{R} \mathcal{R}$
$t \leftarrow H(k_H, m) \oplus F(k_F, r)$
output (r, t)

$\text{Verify}((k_H, k_M), (r,t))$: output 1 if $F(k_F, r) \oplus t = H(k_H, m)$ and 0 otherwise

very simple construction!
but tags are longer (need both a nonce and a PRF output)

GCM encryption: encrypt message with AES in counter mode
compute Carter-Wegman MAC on resulting message using GHASH as the underlying hash function
and the block cipher as underlying PRF

Galois Hash

key derived from PRF evaluation at 0^n

↳ GHASH operates on blocks of 128-bits
operations can be expressed as operations over $GF(2^{128})$ — Galois field with 2^{128} elements
implemented in hardware — very fast!

Typically, use AES-GCM for authenticated encryption

$GF(2^{128})$ is defined by the polynomial $g(x) = x^{128} + x^7 + x^2 + x + 1$

↳ elements are polynomials over $\mathbb{F}_2$ with degree less than 128 [e.g. $x^{127} + x^{52} + x^2 + x + 1$]
(can be represented by 128-bit string: each bit is coefficient of polynomial)

↳ can add elements (xor) and multiply them (as polynomials) — implemented in hardware
(also used for evaluating the AES round function)

↳ $\text{GHASH}(k, \underbrace{m}_{(m[1], m[2], \ldots, m[\ell])}) := m[1]k^{\ell} + m[2]k^{\ell-1} + \cdots + m[\ell]k$ [values $m[1], \ldots, m[\ell]$ give coefficients of polynomial, evaluate at point k]

Oftentimes, only part of the payload needs to be hidden, but still needs to be authenticated

↳ e.g., sending packets over a network: desire confidentiality for packet body, but only integrity for packet headers (otherwise, cannot route!)

AEAD: authenticated encryption with associated data

↳ augment encryption scheme with additional plaintext input; resulting ciphertext ensures integrity for associated data, but not confidentiality
(will not define formally here but follows straightforwardly from AE definitions)

↳ can construct directly via "encrypt-then-MAC": namely, encrypt payload and MAC the ciphertext + associated data

↳ AES-GCM is an AEAD scheme