CS171: Cryptography

Lecture 10

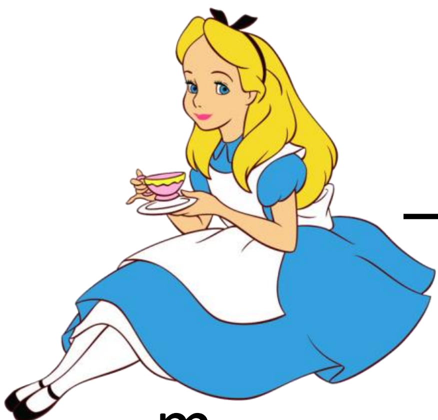
Sanjam Garg

Message Authentication Code (MAC)

message/tag pair

key

k



m,t

key

k

m

$t \leftarrow Mac_k(m)$

message/plaintext

$0/1 := Vrfy_k(m,t)$

verify

tag

MACs - Formally

- $(Gen, Mac, Vrfy)$
- $Gen(1^n)$: Outputs a key k.
- $Mac_k(m)$: Outputs a tag t.
- $Vrfy_k(m, t)$: Outputs 0/1.
- Correctness: $\forall\ n, k \leftarrow\ Gen(1^n), \forall m \in \{0,1\}^*$, we have that $Vrfy_k(m, Mac_k(m)) = 1$.
- Default Construction of $Vrfy$ (for deterministic Mac): $Vrfy_k(m, t)$ outputs 1 if and only $Mac_k(m) = t$.

Unforgeability/Security of MAC

$\text{MacForge}_{\text{A},\Pi}(1^n)$

1. Sample $k \leftarrow \text{Gen}(1^n)$.
2. Let (m^*, t^*) be the output of $A^{Mac_k(\cdot)}$. Let M be the list of queries A makes.
3. Output 1 if $Vrfy_k(m^*, t^*) = 1 \land m^* \notin M$ and 0 otherwise.

$\Pi = (Gen, Mac, Vrfy)$ is existentially unforgeable under adaptive chosen attack, or is *eu-cma-secure* if

$\forall$ PPT A it holds that:

$\Pr[\text{MacForge}_{\text{A},\Pi} = 1] \leq$ negl(n)

Saw last time

- Provably secure construction of Mac
  - Inefficient
- Efficient Construction – CBC Based
  - Not Proved

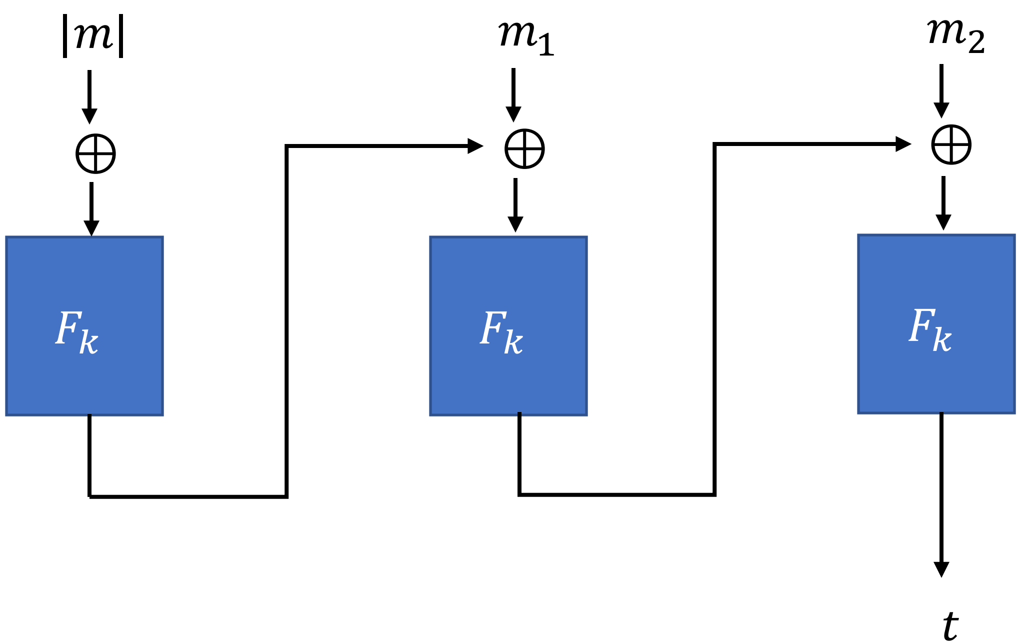
MAC (from fixed-length to arbitrary-length messages)

Construct Mac' (arbitrary-length) from Mac (fixed-length)

- $Mac'_k(m \in \{0,1\}^*)$:
  - Parse m as $m_1 \cdots m_d$ where each m_i is of length $n/4$
  - $r \leftarrow \{0,1\}^{n/4}$
  - Output r, $t_1 \ldots t_d$, where for each i we have
    - $t_i = Mac_k(r||\ell||i||m_i)$, where ℓ is the number of blocks

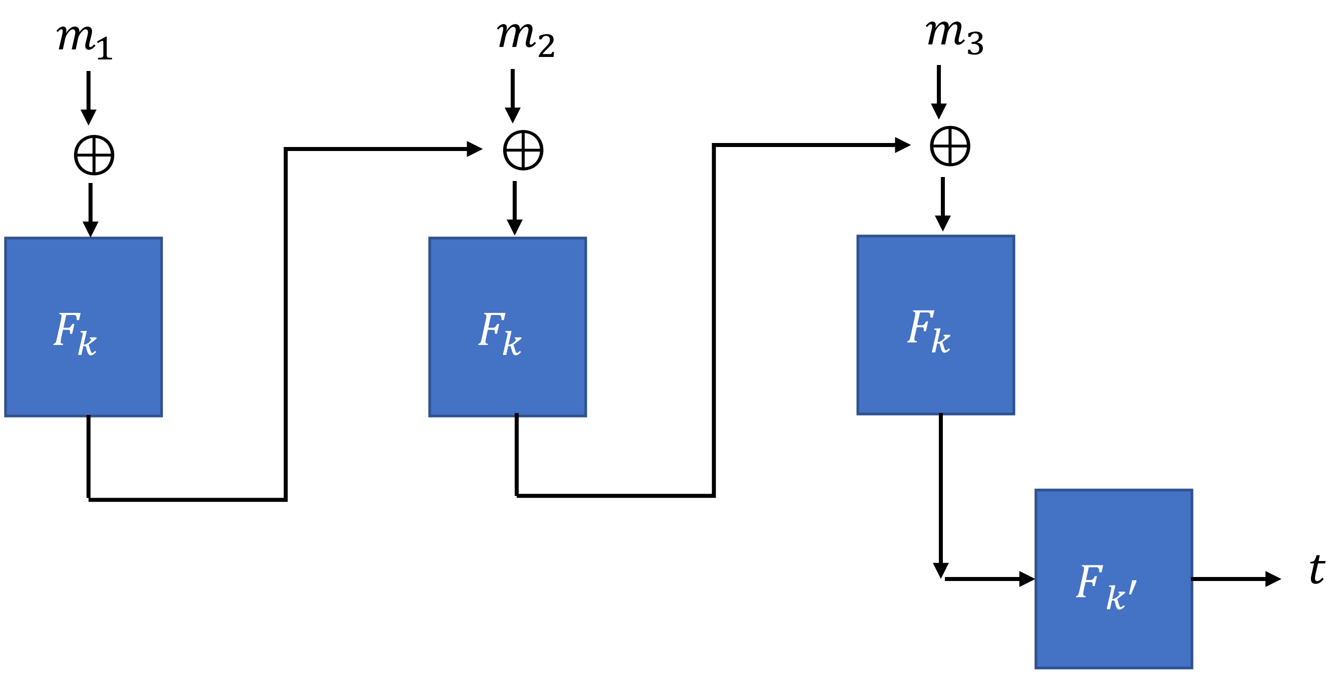
Use this to Mac messages of arbitrary length (multiples of n)

- Method 1: Mac on message m is the CBC-Mac on message $|m| \, || \, m$



Use this to sign messages of arbitrary length (multiples of n)

- Method 2: Mac of the CBC-Mac



Authenticated Encryption

Unforgeable Encryption

$\mathrm{EncForge}_{A,\Pi}(1^n)$

1. Sample $k \leftarrow \mathrm{Gen}(1^n)$.
2. Let c^* be the output of $A^{Enc_k(\cdot)}(1^n)$. Let Q be the list of messages A gets ciphertexts for from the oracle.
3. Output 1 if $Dec_k(c^*) \notin \{\perp\} \cup Q$ and 0 otherwise.

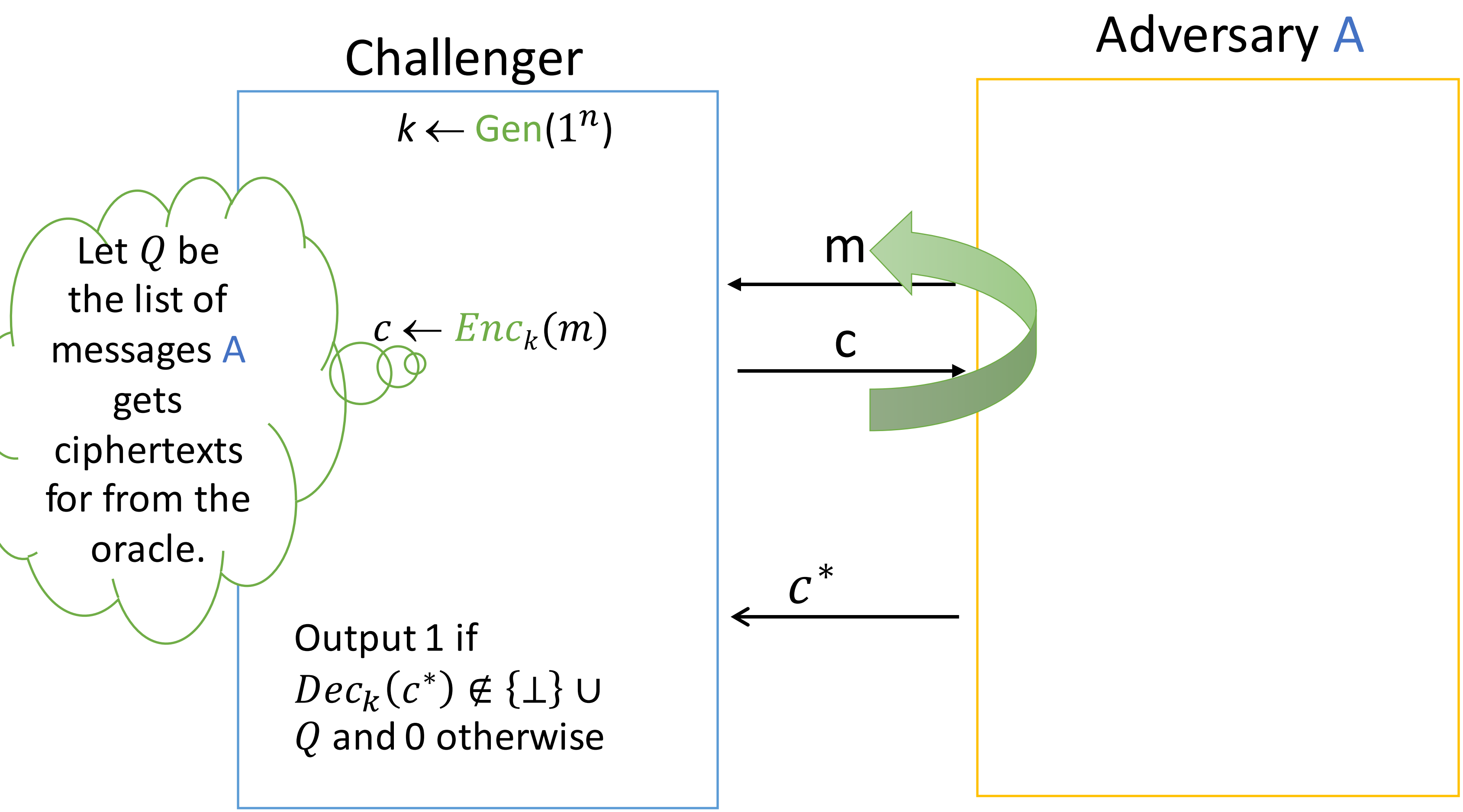
$\Pi = (Gen, Enc, Dec)$ is unforgeable if

$\forall$ PPT A it holds that:

$\Pr[\mathrm{EncForge}_{A,\Pi} = 1] \leq$ negl(n)

Unforgeable Encryption (Pictorially)

$\mathrm{EncForge}_{A,\Pi}(1^n)$



Is this scheme unforgeable?

No!

Let F be a PRF: $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$.

- $Gen(1^n)$: Choose uniform $k \in \{0,1\}^n$ and output it as the key
- $Enc_k(m)$: On input a message $m \in \{0,1\}^n$, sample $r \leftarrow U_n$ output the ciphertext c as
$$c \coloneqq \langle r, F_k(r) \oplus m \rangle$$
- $\mathrm{Dec}_k(c)$: On input a ciphertext $c = \langle r, s \rangle$ output the message
$$m \coloneqq F_k(r) \oplus s$$

Is this PRF-based CPA-secure encryption scheme unforgeable?

Authenticated Encryption

- A private-key encryption scheme is an authenticated encryption scheme if it is CCA-secure and unforgeable.

CCA-Security

$\mathrm{PrivK}^{\mathrm{CCA}}_{\mathrm{A},\Pi}(n)$

1. Sample $k \leftarrow \mathrm{Gen}(1^n)$, $A^{Enc_k(\cdot),Dec_k(\cdot)}$ outputs $m_0, m_1 \in \{0,1\}^*$, $|m_0| = |m_1|$.
2. $\mathrm{b} \leftarrow \{0,1\}$, $c^* \leftarrow Enc_k(m_b)$
3. c^* is given $A^{Enc_k(\cdot),Dec_k(\cdot)}$
4. $A^{Enc_k(\cdot),Dec_k(\cdot)}$ (query not allowed on c^*) output b'
5. Output 1 if $b = b'$ and 0 otherwise

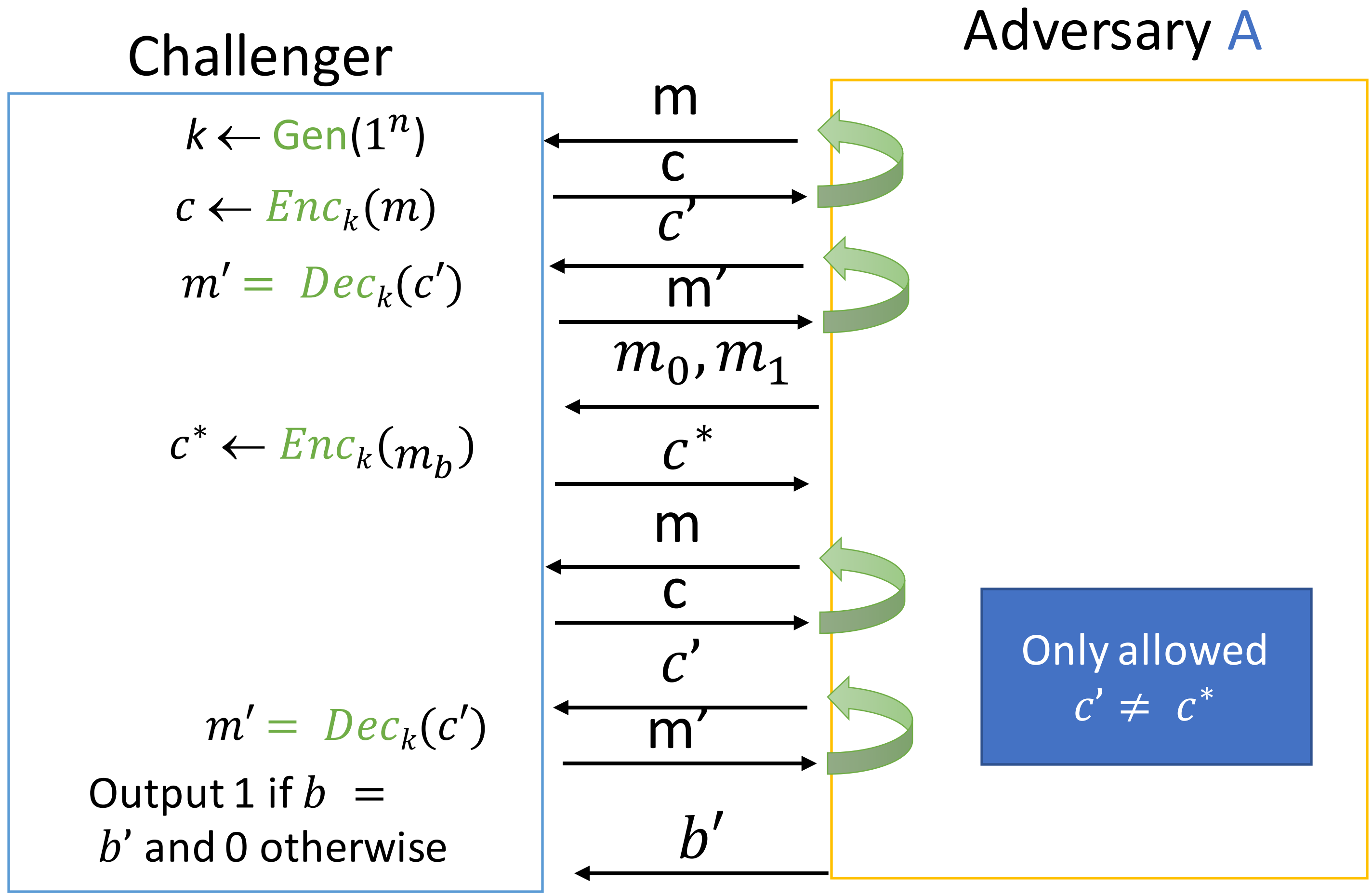
Encryption scheme $\Pi = (Gen, Enc, Dec)$ has indistinguishable encryptions under ciphertext attack, or is *CCA-secure* if

$\forall$ PPT A it holds that:

$$\Pr\left[\mathrm{PrivK}^{\mathrm{CCA}}_{\mathrm{A},\Pi} = 1\right] \leq \frac{1}{2} + \mathrm{negl}(n)$$

CCA-Security (Pictorially)

$$\mathrm{PrivK}^{\mathrm{CCA}}_{A,\Pi}(n)$$



Authenticated Encryption

- A private-key encryption scheme is an authenticated encryption scheme if it is CCA-secure and unforgeable.

Hard to come up with legitimate looking ciphertexts of new messages!

The power of decryption queries doesn't help!

Intuitively

- Can we have encryption scheme that is unforgeable but not CCA secure?
  - Perhaps, it is possible to modify a given ciphertext and get a new ciphertext encrypting the same message. This scheme would still be unforgeable but not CCA secure.
- Can we have encryption schemes that is CCA secure but not unforgeable?
  - Perhaps, it is possible to come up with a fresh ciphertext encrypting a new message. This scheme would still be CCA secure but not unforgeable.

Authenticated Encryption Construction

- Let (Enc, Dec) be CPA secure and (Mac, Vrfy) be unforgeable.
- Encrypt and Authenticate

$$c \leftarrow Enc_{k_E}(m) \quad t \leftarrow Mac_{k_M}(m)$$

- Authenticate then Encrypt

$$t \leftarrow Mac_{k_M}(m) \quad c \leftarrow Enc_{k_E}(m||t)$$

- Encrypt then Authenticate

$$c \leftarrow Enc_{k_E}(m) \quad t \leftarrow Mac_{k_M}(c)$$

Encrypt and Authenticate

- $c \leftarrow Enc_{k_E}(m) \quad t \leftarrow Mac_{k_M}(m)$
- The recipient decrypts c to get m and accepts only if t is a valid tag on the message m.

- This is insecure because Mac does not offer secrecy. Mac could leak the entire message. May not even be CPA secure.

Authenticate then Encrypt

- $t \leftarrow Mac_{k_M}(m) \quad c \leftarrow Enc_{k_E}(m||t)$
- The recipient decrypts c to get $m||t$ and accepts only if t is a valid tag on the message m.

- This is insecure as Enc is only CPA secure. Given c the attacker can get c' that encrypts the same message as c. This scheme will not be CCA-secure.

Is it CPA secure?

Is it unforgeable?

Also, the first CCA secure encryption we have seen!

Encrypt then Authenticate

- $c \leftarrow Enc_{k_E}(m) \quad t \leftarrow Mac_{k_M}(c)$
- The recipient accepts only if t is a valid tag on the ciphertext c and in this case decrypts c to get m.

- This is secure authenticated encryption scheme if Mac is strongly unforgeable.

Is it unforgeable?

Is it CCA-secure?

Can we use the same key?

- Set $k = k_E = k_M$. We have the encrypt and authenticate paradigm looks like $c \leftarrow Enc_k(m) \quad t \leftarrow Mac_k(c)$
- Is it secure?

- No! Let $Enc_k(m) = F_k(m||r)$, where $m \in \{0,1\}^{n/2}$ and r is uniform in $\{0,1\}^{n/2}$. And $Mac_k(m) = F_k^{-1}(m)$.
  - $Enc_k(m), \mathrm{Mac_k}\left(\mathrm{Enc_k}(\mathrm{m})\right) = \mathrm{F_k}(\mathrm{m}||\mathrm{r}), \mathrm{F_k^{-1}}(\mathrm{F_k}(\mathrm{m}||\mathrm{r}))$

Secure Communication

- Re-ordering attack
- Replay attack
- Reflection attack

- Can be solved using counters and a direction bit as part of the sent messages.

Thank You!