CSE 539: Applied Cryptography Lec 7: Message Authentication Codes

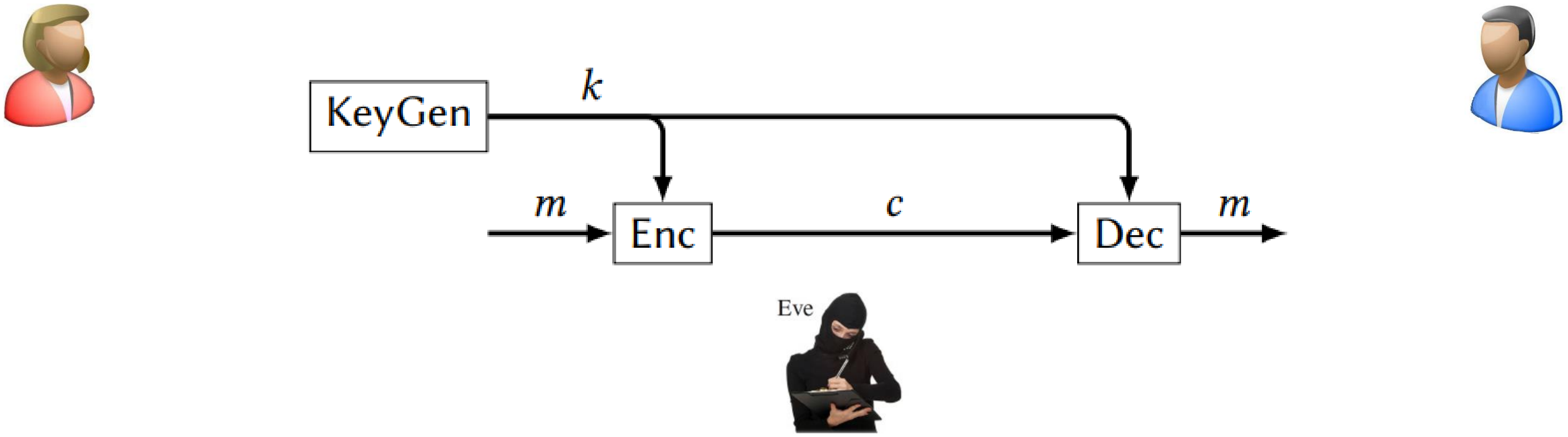
Ni Trieu (ASU)

Reading: https://joyofcryptography.com/pdf/chap10.pdf

Recap: PRG/PRF/PRP

- A PRG is a function $\mathbf{G}\colon \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{\lambda}} \to \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{\lambda}+\boldsymbol{\ell}}$
- A PRF is a function F: $\{\mathbf{0},\mathbf{1}\}^{\boldsymbol{\lambda}} \times \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{in}} \to \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{out}}$
- A PRP is a function F: $\{\mathbf{0},\mathbf{1}\}^{\boldsymbol{\lambda}} \times \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{blen}} \to \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{blen}}$

Recall: Encryption Basics & Terminology



KeyGen

k

m

Enc

c

Dec

m

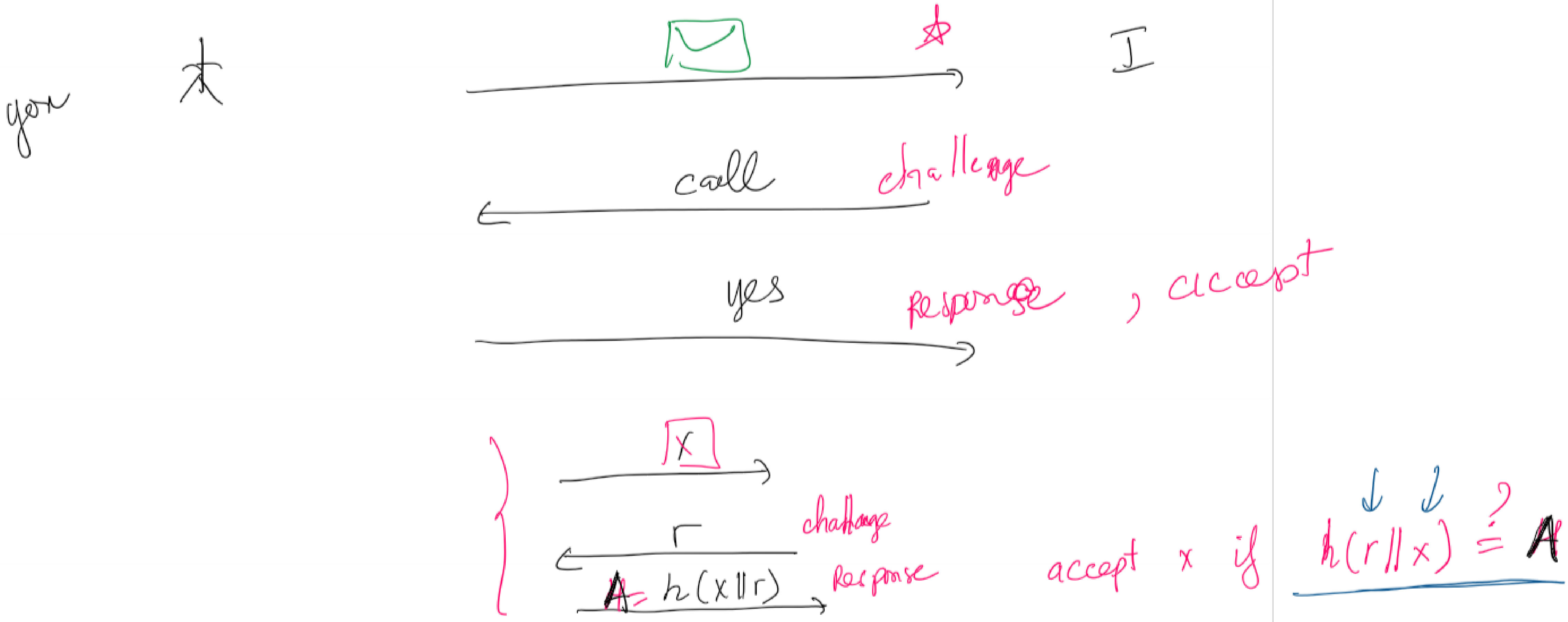
- How to ensure that c was generated by Alice? (CCA-secure?)

Authentication

- What we are asking for is not to hide the ciphertext but to authenticate it: to ensure that it was generated by someone who knows the secret key.

Authentication: Challenge & Response

Authentication: Challenge & Response

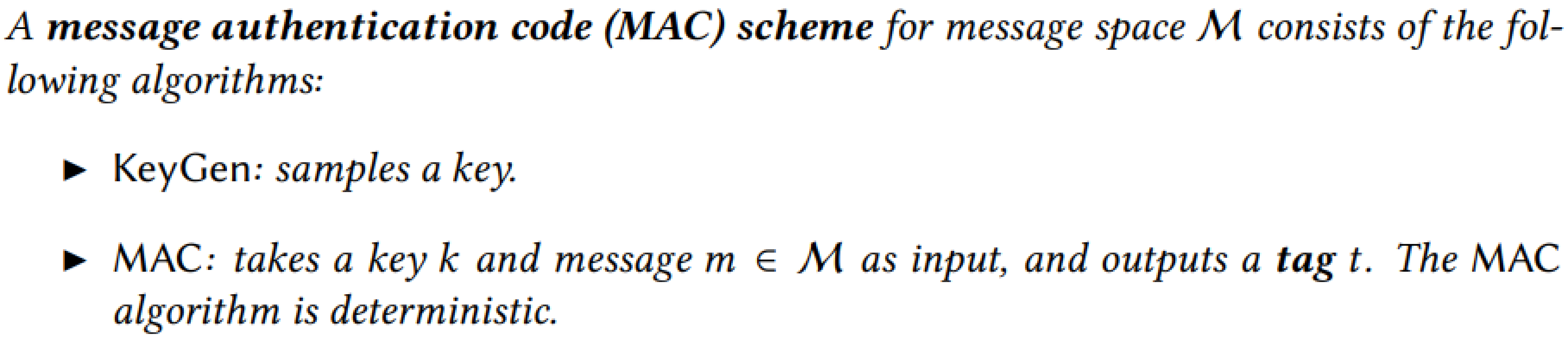


accept x if $\underline{h(r\|x) \overset{?}{=} A}$

A

Message Authentication Code (MAC)

- A MAC is like a signature that can be added to a piece of data, which certifies that someone who knows the secret key attests to this particular data

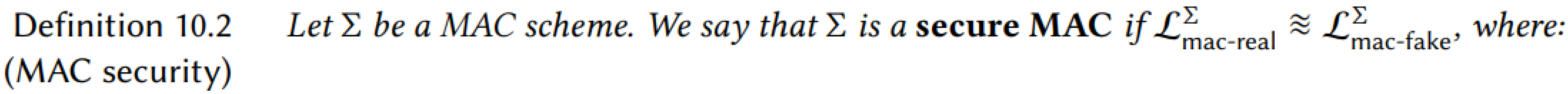


A ***message authentication code (MAC) scheme*** *for message space $\mathcal{M}$ consists of the following algorithms:*

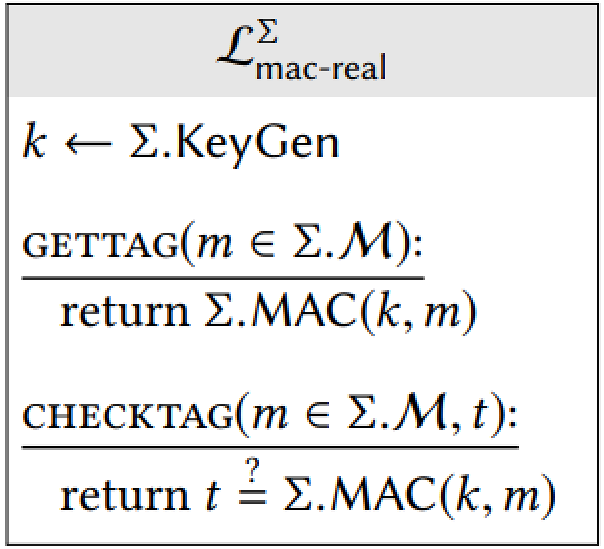
- KeyGen*: samples a key.*
- MAC*: takes a key k and message $m \in \mathcal{M}$ as input, and outputs a* ***tag*** *t. The* MAC *algorithm is deterministic.*

Message Authentication Code (MAC)

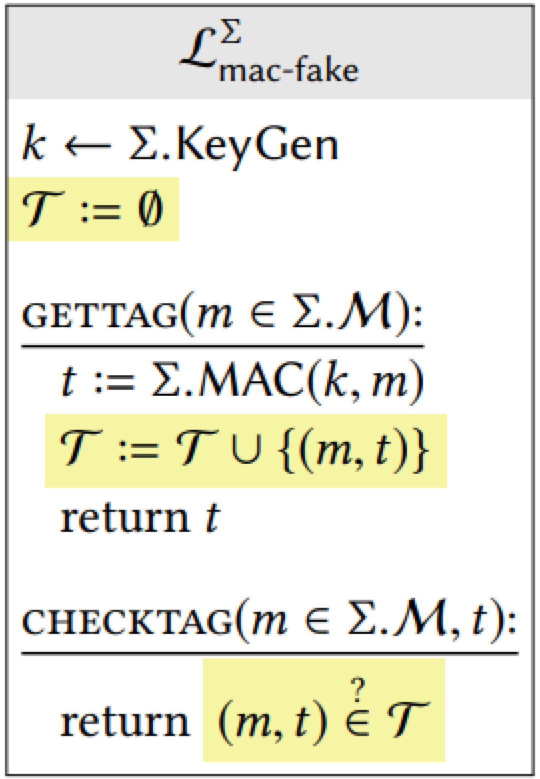
- A MAC scheme is a secure MAC if the adversary knows valid MACs corresponding to various messages, she cannot produce a valid MAC for a different message.



Definition 10.2 (MAC security) *Let Σ be a MAC scheme. We say that Σ is a* **secure MAC** *if $\mathcal{L}^{\Sigma}_{\text{mac-real}} \approx \mathcal{L}^{\Sigma}_{\text{mac-fake}}$, where:*



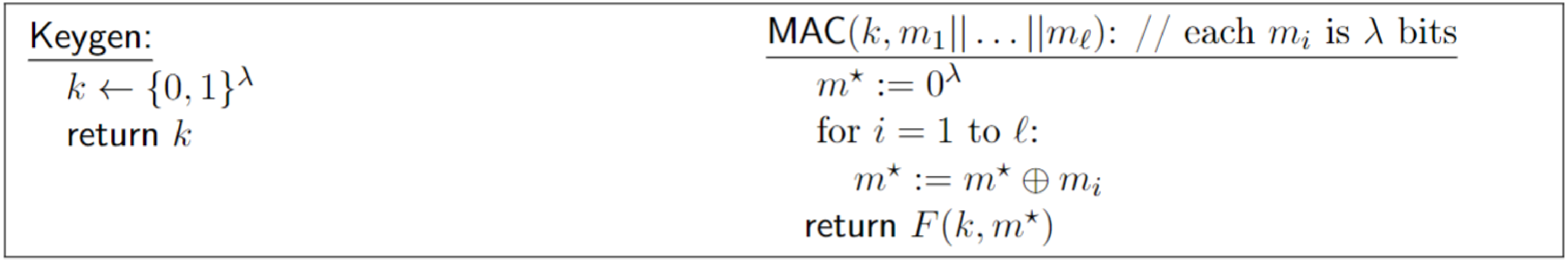
```
$\mathcal{L}^{\Sigma}_{\text{mac-real}}$

$k \leftarrow \Sigma.\text{KeyGen}$

$\underline{\text{GETTAG}(m \in \Sigma.\mathcal{M})\text{:}}$
    return $\Sigma.\text{MAC}(k, m)$

$\underline{\text{CHECKTAG}(m \in \Sigma.\mathcal{M}, t)\text{:}}$
    return $t \overset{?}{=} \Sigma.\text{MAC}(k, m)$
```



```
$\mathcal{L}^{\Sigma}_{\text{mac-fake}}$

$k \leftarrow \Sigma.\text{KeyGen}$
$\mathcal{T} := \emptyset$

$\underline{\text{GETTAG}(m \in \Sigma.\mathcal{M})\text{:}}$
    $t := \Sigma.\text{MAC}(k, m)$
    $\mathcal{T} := \mathcal{T} \cup \{(m, t)\}$
    return $t$

$\underline{\text{CHECKTAG}(m \in \Sigma.\mathcal{M}, t)\text{:}}$
    return $(m, t) \overset{?}{\in} \mathcal{T}$
```

Message Authentication Code (MAC)

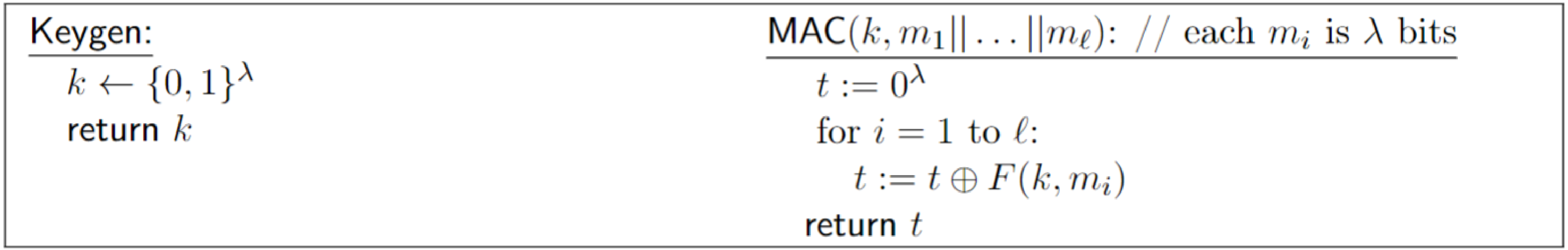
- Quiz Sample: Is the below MAC secure?



```
Keygen:
    $k \leftarrow \{0,1\}^\lambda$
    return $k$

MAC($k, m_1 || \ldots || m_\ell$):  // each $m_i$ is $\lambda$ bits
    $m^\star := 0^\lambda$
    for $i = 1$ to $\ell$:
        $m^\star := m^\star \oplus m_i$
    return $F(k, m^\star)$
```

Message Authentication Code (MAC)

- Quiz Sample: Is the below MAC secure?



```
Keygen:
    $k \leftarrow \{0,1\}^\lambda$
    return $k$

MAC($k, m_1 || \ldots || m_\ell$): // each $m_i$ is $\lambda$ bits
    $t := 0^\lambda$
    for $i = 1$ to $\ell$:
        $t := t \oplus F(k, m_i)$
    return $t$
```