Remark Lecture Video 5 partly covered the proof of *PRF* $\Rightarrow$ *UNF-CMA-secure MAC*. The notes for this proof are contained in Lecture Notes 4. The current lecture notes cover part II of Lecture Video 5 which defines symmetric-key encryption schemes. We provide additional theorems and proofs in the current lecture notes which were not contained in the Lecture Video 5. Concretely, the current lecture notes contain

- the syntax of symmetric-key encryption schemes
- confidentiality of symmetric-key encryption schemes, captured by a security notion which we call *indistinguishability under chosen plaintext attacks (IND-CPA)*
- confidentiality and integrity of symmetric-key encryption schemes, captured by the security notion of *authenticated encryption* (AE).
- Theorems (informal):
  - A PRF in counter-mode (CTR-mode) yields IND-CPA-secure symmetric encryption.
  - A pseudorandom permutation (PRP) in CBC-mode yields IND-CPA-secure symmetric encryption.
  - AE-secure symmetric encryption schemes are also IND-CPA-secure.
  - If the encryption algorithm of a symmetric encryption scheme is deterministic, then it is not IND-CPA-secure.

1 Syntax of symmetric-key encryption schemes

A symmetric encryption scheme consists of two algorithms, an *encryption algorithm* and a *decryption algorithm.* The encryption algorithm of a symmetric-key encryption scheme takes a key k and a message m, and encrypts them into a ciphertext c. The encryption process is *randomized.* This is crucial for security, as we will see in Theorem 5.

Definition 1.1 (Syntax of symmetric encryption schemes)**.** A *symmetric encryption scheme* se consists of two probabilistic polynomial-time (PPT) algorithms

$$c \leftarrow\!\!\$\, \mathsf{se.enc}(k, m)$$
$$m \leftarrow \mathsf{se.dec}(k, c)$$

which have to satisfy the correctness criterion

$$\forall m \in \{0,1\}^* \ \Pr_{k \leftarrow\$\{0,1\}^n}[\mathsf{se.dec}(k, \mathsf{se.enc}(k, m)) = m] = 1$$

i.e. when a ciphertext is created using the encryption algorithm, the decryption algorithm always returns the original message.

2 IND-CPA-security for symmetric-key encryption schemes

Symmetric-encryption schemes should provide confidentiality. How do we define confidentiality? A first thought might be that *one-wayness* might be a good way to capture confidentiality. However, as we saw in the first lecture, one-wayness is a very weak security notion, and our symmetric encryption scheme might leak as much as half of the message if we use one-wayness as a security notion. Thus, one-wayness would be a terrible way to capture confidentiality.

Instead, what we will capture is the property that encryption should really not leak any information except for the length of the message—it has to leak the length of the message, since information-theoretically, longer messages have to be encrypted into longer ciphertexts. Now, if we cannot distinguish whether the message m was encrypted or the message $0^{|m|}$, then the ciphertext carries no information about m (except for the length of m).

We have already stated what we want, namely, that encryptions of m look like encryptions of $0^{|m|}$. But how do we choose m? We could define a game which chooses m uniformly at random from all bitstrings of some length. But this does not model real-life distributions very well. We could also parametrize our system with a distribution over messages, but this is a cumbersome definition.

To resolve this issue, we will apply a trick which we already used in the context of message authentication codes: We allow the *adversary* to choose the message! This simplifies our model and additionally gives us stronger properties (which we need if we recall the BEAST attack): Even if the adversary happens to be able to influence the content of the message, security of the system does not break down.

It might be a little counter-intuitive to model confidentiality by an adversary who already knows the message—but in fact, this only makes our property even stronger: Even though the adversary knows what m might be, it cannot distinguish between an encryption of m and an encryption of $0^{|m|}$.

Definition 2.1 (IND-CPA)**.** A symmetric encryption scheme $\mathtt{se}$ is IND-CPA-secure if the real game $\mathtt{Gind\text{-}cpa}^0$ and the ideal game $\mathtt{Gind\text{-}cpa}^1$ are computationally indistinguishable, that is, for all PPT adversaries $\mathcal{A}$, the advantage

$$\begin{aligned}&\mathbf{Adv}_{\mathcal{A}}^{\mathtt{Gind\text{-}cpa}^0,\mathtt{Gind\text{-}cpa}^1}(\lambda)\\ &:= \left|\Pr\left[1 = \mathcal{A} \to \mathtt{Gind\text{-}cpa}^0\right] - \Pr\left[1 = \mathcal{A} \to \mathtt{Gind\text{-}cpa}^1\right]\right|\end{aligned}$$

is negligible in λ.

```
$\texttt{Gind-cpa}^0_{\mathsf{se}}$

Parameters
$\lambda$:   sec. parameter
$\mathsf{se}$:  sym. enc. sch.

Package State
$k$:   key

$\mathsf{ENC}(x)$
if $k = \bot$ :
    $k \leftarrow\!\!\$ \{0,1\}^\lambda$
$c \leftarrow\!\!\$ \mathsf{se.enc}(k, x)$
return $c$
```

```
$\texttt{Gind-cpa}^1_{\mathsf{se}}$

Parameters
$\lambda$:   sec. parameter
$\mathsf{se}$:  sym. enc. sch.

Package State
$k$:   key

$\mathsf{ENC}(x)$
if $k = \bot$ :
    $k \leftarrow\!\!\$ \{0,1\}^\lambda$
$x' \leftarrow 0^{|x|}$
$c \leftarrow\!\!\$ \mathsf{se.enc}(k, x')$
return $c$
```

3 AE-Security

Authenticated encryption security, in addition to confidentiality, also captures integrity and authenticity. Namely, the adversary is also allowed to make *decryption* queries and can also be successful merely by *forging* a ciphertext. This is encoded by having the ideal decryption oracle return 0 for all fresh ciphertexts, i.e., for all ciphertexts which did not come from the encryption oracle.

Definition 3.1 (AE-security)**.** A symmetric encryption scheme is AE-secure if the real game $\texttt{Gae}^0_{\mathsf{se}}$ and the ideal game $\texttt{Gae}^1_{\mathsf{se}}$ are computationally indistinguishable, that is, for all PPT adversaries $\mathcal{A}$, the advantage

$$\mathbf{Adv}_{\mathcal{A}}^{\texttt{Gae}^0_{\mathsf{se}},\texttt{Gae}^1_{\mathsf{se}}}(\lambda) := \left|\Pr\left[1 = \mathcal{A} \rightarrow \texttt{Gae}^0_{\mathsf{se}}\right] - \Pr\left[1 = \mathcal{A} \rightarrow \texttt{Gae}^1_{\mathsf{se}}\right]\right|$$

is negligible in λ.

```
$\mathsf{Gae}^0_{\mathsf{se}}$

Parameters
$\lambda$:   sec. parameter
se:  sym. enc. sch.

Package State
$k$:   key

ENC($x$)
if $k = \bot$ :
    $k \leftarrow\$ \{0,1\}^\lambda$
$c \leftarrow\$ \mathsf{se.enc}(k, x)$
return $c$

DEC($c$)
if $k = \bot$ :
    $k \leftarrow\$ \{0,1\}^\lambda$
$x \leftarrow \mathsf{se.dec}(k, c)$
return $x$
```

```
$\mathsf{Gae}^1_{\mathsf{se}}$

Parameters
$\lambda$:   sec. parameter
se:  sym. enc. sch.

Package State
$k$:   key
$T$:   table

ENC($x$)
if $k = \bot$ :
    $k \leftarrow\$ \{0,1\}^\lambda$
$x' \leftarrow 0^{|x|}$
$c \leftarrow\$ \mathsf{se.enc}(k, x')$
$T[c] \leftarrow x$
return $c$

DEC($c$)
$x \leftarrow T[c]$
return $x$
```

4 Theorems

We describe how to build secure symmetric encryption schemes. We start with IND-CPA security and then turn to AE-security. Since PRFs and PRPs tend to operate on blocks, we will often need an *encoding* scheme which encodes messages into a multiple of the block length.

Definition 4.1 (Encoding scheme)**.** We call two functions $\mathsf{encode}_\lambda : \{0,1\}^* \to \{0,1\}^*$ and $\mathsf{decode}_\lambda : \{0,1\}^* \to \{0,1\}^*$ an *encoding scheme* if

- encode_λ and decode_λ are computable in time polynomial in λ and the length of the input.
- decode_λ is the inverse of encode_λ, i.e., for all $x \in \{0,1\}^*$, decode_λ can recover x from $\mathsf{encode}_\lambda(x)$, that is, we have $\mathsf{decode}_\lambda(\mathsf{encode}_\lambda(x)) = x$. In particular, encode_λ is *injective*, i.e., if $x \neq x'$, then $\mathsf{encode}_\lambda(x) \neq \mathsf{encode}_\lambda(x')$.
- the length encode_λ only depends on the length of the input, i.e., if $|x| = |x'|$, then $|\mathsf{encode}_\lambda(x)| = |\mathsf{encode}_\lambda(x')|$.
- for all $x \in \{0,1\}^*$, $|\mathsf{encode}_\lambda(x)|$ is divisible by λ.

Theorem 1 (PRP in CBC is IND-CPA)**.** Let $(\mathsf{encode}_\lambda, \mathsf{decode}_\lambda)$ be an encoding scheme and let f be a secure (λ, λ)-secure pseudorandom permutation. Then, the following encryption scheme $\mathsf{se}_{\text{CBC-f}}$ is IND-CPA-secure.

```
$\mathsf{se}_{\text{CBC-f}}.\mathsf{enc}(k, m)$
$\lambda \leftarrow |k|$
$m' \leftarrow \mathsf{encode}_\lambda(m)$
$nonce \leftarrow\$ \{0,1\}^\lambda$
$c_0 \leftarrow nonce$
$\ell \leftarrow \frac{|m'|}{\lambda}$
for $i = 1..\ell$
    $x_i \leftarrow m'_{(i-1)\lambda+1..i\lambda}$
    $c_i \leftarrow f(k, x_i \oplus c_{i-1})$
$c \leftarrow (c_0, .., c_\ell)$
return $c$
```

```
$\mathsf{se}_{\text{CBC-f}}.\mathsf{dec}(k, c)$
$\lambda \leftarrow |k|$
$\ell \leftarrow \frac{|c|}{\lambda} - 1$
Parse $c_0, .., c_\ell \leftarrow c$
for $i = 1..\ell$
    $x_i \leftarrow c_{i-1} \oplus f_{\text{inv}}(k, c_i)$
$m' \leftarrow x_1||..||x_\ell$
$m \leftarrow \mathsf{decode}_{|k|}(m')$
return $m$
```

Theorem 2 (PRF in CTR is IND-CPA)**.** Let $(\mathsf{encode}_\lambda, \mathsf{decode}_\lambda)$ be an encoding scheme and let f be a secure (λ, λ)-secure pseudorandom function. Then, the encryption scheme $\mathsf{se}_{\text{CTR-f}}$ is IND-CPA-secure.

```
$\mathsf{se}_{\text{CTR-f}}.\mathsf{enc}(k, m)$
$\lambda \leftarrow |k|$
$nonce \leftarrow\$ \{0,1\}^\lambda$
$m' \leftarrow \mathsf{encode}_\lambda(m)$
$\ell \leftarrow \frac{|m'|}{\lambda}$
for $i = 1..\ell$
    $pad_i \leftarrow f(k, nonce + i)$
$pad' \leftarrow pad_1||..||pad_\ell$
$pad \leftarrow pad_{1..|m|}$
$c \leftarrow m \oplus pad$
return $(nonce, c)$
```

```
$\mathsf{se}_{\text{CTR-f}}.\mathsf{dec}(k, (nonce, c))$
$\lambda \leftarrow |k|$
$\ell \leftarrow \frac{|c|}{\lambda}$
for $i = 1..\ell$
    $pad_i \leftarrow f(k, nonce + i)$
$pad' \leftarrow pad_1||..||pad_\ell$
$pad \leftarrow pad_{1..|c|}$
$m' \leftarrow c \oplus pad$
$m \leftarrow \mathsf{decode}_\lambda(m')$
return $m$
```

Theorem 3 (... is AE)**.** Will be added after Monday, October 10, 2022.

Generic transformations on symmetric encryption schemes

Theorem 4. If se is an IND-CPA secure encryption scheme, then se_1 is an IND-CPA secure encryption scheme.

```
$\mathsf{se}_1.\mathsf{enc}(k, m)$
$c' \leftarrow\$ \mathsf{se}.\mathsf{enc}(k, m)$
$c \leftarrow c'||1$
return $c$
```

```
$\mathsf{se}_1.\mathsf{dec}(k, c)$
$c' \leftarrow c[1..|c| - 1]$
$m \leftarrow \mathsf{se}.\mathsf{dec}(k, c')$
return $m$
```

Theorem 5. Let se be a symmetric encryption scheme such that $\mathsf{se}.\mathsf{enc}$ is deterministic. Then se is not IND-CPA-secure.