Symmetric encryption schemes
A scheme $SE$ is specified by a key generation algorithm $K$, an encryption algorithm $E$, and a decryption algorithm $D$.

$$SE = (K, E, D)$$

It is required that for every $M \in \text{MsgSp}$ and every $K$ that can be output by $K$, $D(K, E(K, M)) = M$.

Block cipher modes of operation
- Modes of operation define how to use a block cipher to encrypt long messages.
- We will often assume that the message space consists of messages whose length is multiple of a block length.

- Often the key generation algorithm simply picks a random string from some key space $KeySp$ (e.g. $\{0,1\}^k$ for some integer $k$).
- In this case we will say that a scheme $SE$ is defined by $KeySp$ and two algorithms: $SE = (KeySp, E, D)$.
- The encryption algorithm can be either
  - randomized (take as input a random string)
  - or stateful (take as input some state (e.g. counter) that it can update)
Electronic Code Book (ECB) mode

Let $E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a block cipher. ECB$=\langle \{0,1\}^k, E, \mathcal{D} \rangle$:

**Encryption algorithm $E$**

\[
\begin{array}{c|c|c}
\text{M}[1] & \text{M}[2] & \text{M}[m] \\
\downarrow & \downarrow & \downarrow \\
E_K & E_K & E_K \\
\downarrow & \downarrow & \downarrow \\
\end{array}
\]

**Decryption algorithm $D$**

\[
\begin{array}{c|c|c}
\text{C}[1] & \text{C}[2] & \text{C}[m] \\
\downarrow & \downarrow & \downarrow \\
E^{-1}_K & E^{-1}_K & E^{-1}_K \\
\downarrow & \downarrow & \downarrow \\
\text{M}[1] & \text{M}[2] & \text{M}[m] \\
\end{array}
\]

Cipher-block chaining (CBC) mode with random IV

Let $E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a block cipher. CBC$=\langle \{0,1\}^k, E, \mathcal{D} \rangle$:

**Encryption algorithm $E$**

\[
\begin{array}{c|c|c}
\text{IV} & \text{M}[1] & \text{M}[m] \\
\downarrow & \downarrow & \downarrow \\
E_K & E_K & E_K \\
\downarrow & \downarrow & \downarrow \\
\text{C}[1] & \text{C}[2] & \text{C}[m] \\
\end{array}
\]

**Decryption algorithm $D$**

\[
\begin{array}{c|c|c}
\text{IV} & \text{C}[1] & \text{C}[m] \\
\downarrow & \downarrow & \downarrow \\
E^{-1}_K & E^{-1}_K & E^{-1}_K \\
\downarrow & \downarrow & \downarrow \\
\text{M}[1] & \text{M}[2] & \text{M}[m] \\
\end{array}
\]
Stateful Cipher-block chaining (CBC) mode with counter IV

Let $E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a block cipher. CBC = $(\{0,1\}^k, E, D)$:

Encryption algorithm $E$

$\text{ctr} \leftarrow 0^n$

The counter $\text{ctr}$ is incremented for each new message

<table>
<thead>
<tr>
<th>$\text{ctr}$</th>
<th>$\text{M}[1]$</th>
<th>$\text{M}[2]$</th>
<th>...</th>
<th>$\text{M}[m]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{E}_k$</td>
<td>$\text{C}[1]$</td>
<td>$\text{C}[2]$</td>
<td>...</td>
<td>$\text{C}[m]$</td>
</tr>
</tbody>
</table>

Decryption algorithm $D$

<table>
<thead>
<tr>
<th>$\text{ctr}$</th>
<th>$\text{C}[1]$</th>
<th>$\text{C}[2]$</th>
<th>...</th>
<th>$\text{C}[m]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{E}^{-1}_k$</td>
<td>$\text{M}[1]$</td>
<td>$\text{M}[2]$</td>
<td>...</td>
<td>$\text{M}[m]$</td>
</tr>
</tbody>
</table>

Randomized counter mode (CTR$^*$)

Let $E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a block cipher. CTR$^* = (\{0,1\}^k, E, D)$:

Encryption algorithm $E$

$\text{R} \leftarrow \{0,1\}^n$

<table>
<thead>
<tr>
<th>$\text{R}$</th>
<th>$\text{R}+1$</th>
<th>$\text{R}+2$</th>
<th>...</th>
<th>$\text{R}+m$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{E}_k$</td>
<td>$\text{M}[1]$</td>
<td>$\text{M}[2]$</td>
<td>...</td>
<td>$\text{M}[m]$</td>
</tr>
</tbody>
</table>

Decryption algorithm $D$

<table>
<thead>
<tr>
<th>$\text{R}$</th>
<th>$\text{R}+1$</th>
<th>$\text{R}+2$</th>
<th>...</th>
<th>$\text{R}+m$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{E}^{-1}_k$</td>
<td>$\text{C}[1]$</td>
<td>$\text{C}[2]$</td>
<td>...</td>
<td>$\text{C}[m]$</td>
</tr>
</tbody>
</table>

Stateful counter mode (CTRC)

Let $E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a block cipher. CTRC = $(\{0,1\}^k, E, D)$:

Encryption algorithm $E$

$\text{ctr}$ is initially $0^n$

<table>
<thead>
<tr>
<th>$\text{ctr}$</th>
<th>$\text{ctr}+1$</th>
<th>$\text{ctr}+2$</th>
<th>...</th>
<th>$\text{ctr}+m$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{E}_k$</td>
<td>$\text{M}[1]$</td>
<td>$\text{M}[2]$</td>
<td>...</td>
<td>$\text{M}[m]$</td>
</tr>
</tbody>
</table>

Decryption algorithm $D$

<table>
<thead>
<tr>
<th>$\text{ctr}$</th>
<th>$\text{ctr}+1$</th>
<th>$\text{ctr}+2$</th>
<th>...</th>
<th>$\text{ctr}+m$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{E}^{-1}_k$</td>
<td>$\text{C}[1]$</td>
<td>$\text{C}[2]$</td>
<td>...</td>
<td>$\text{C}[m]$</td>
</tr>
</tbody>
</table>
What is a secure encryption scheme?

- Recall, perfectly secure schemes are impractical
- We assume that adversaries are computationally bounded
- A scheme is secure when it is not insecure.
- Insecure = adversaries can do bad things.
- Bad things: an adversary who sees ciphertexts
  - can compute the secret key
  - can compute some plaintexts
  - can compute the first bit of a plaintext
  - can compute the sum of the bits of a plaintext
  - can see when equal messages are encrypted
  - can compute ..........

So what is a secure encryption scheme?

- Informally, an encryption scheme is secure if no adversary with “reasonable” resources who sees several ciphertexts can compute any* partial information about the plaintexts, besides some a-priori information.
  * Any information, except the length of the plaintexts. We assume the length of the plaintexts is public.

- Note, that the above implies that the bad things we mentioned do not happen. And the other “bad” things.
- While the above “definition” captures the right intuition, it’s too informal to be useful.

Security of encryption (still informally)

- An encryption scheme is semantically secure if no adversary with reasonable resources who is given a ciphertext can get any information about the underlying message better than anyone who is not given the ciphertext.
- An encryption scheme is indistinguishable under chosen-plaintext attacks if no adversary with reasonable resources who is given a ciphertext of the one of two messages of its choice, can figure out which message was encrypted.
- These two definitions can be formalized and proven equivalent.

Indistinguishability under chosen-plaintext attacks

Fix an encryption scheme SE=(KeySp,E,D)
Pick a key K at random from KeySp
For an adversary A and a bit b consider two experiments Exp-ind-cpa-b (SE,A), for b=0 or b=1
The difference between probabilities of outputting 0 in two experiments is called ind-cpa-advantage of A in attacking SE.

A symmetric encryption scheme SE is indistinguishable under chosen-plaintext attacks (IND-CPA secure) if prf-advantage of any adversary with “reasonable” resources is “close” to 0.
Why IND-CPA ensures that no partial information is leaked?

- Fix SE=(KeySp,E,D) with MsgSp={0,1}m. Assume for example that there exists an efficient adversary B that after seeing a few plaintext-ciphertext pairs and a challenge ciphertext can always compute the challenge plaintext.
- Then we can easily show that SE is not IND-CPA secure. We present an adversary A:

  Adversary A, given access to E_K(L(·; b)):
  - Pick any two distinct messages M_0, M_1 from {0,1}^m
  - Query them to the oracle, get back a ciphertext C_0
  - Run the adversary B
    - If B requests to see an encryption of a message M,
      - Query (M,M) to the oracle, get back C, give C back to B
      - Give C as the challenge to B
    - Until B outputs plaintext M
  - If M'=M_0 then return 0, else return 1 EndIf

A is correct whenever B is correct. I.e. in Exp-ind-cpa-0 A returns 0 if B was correct (always by assumption), in Exp-ind-cpa-1 A outputs 0 only if B is incorrect (never). Thus ind-cpa advantage of A is 1-0=1. A is efficient. Thus SE is not IND-CPA.

ECB is not IND-CPA

We construct an adversary A. A weakness is that equal plaintext blocks always yield equal ciphertext blocks. The adversary just asks to see a ciphertext of two messages where only one has equal blocks.

Adversary A^E_k(L(·; b))
- M_1 ← 0^n; M_0 ← 0^n || 1^n
- C[1]/C[2] ← E_k(L(M_0, M_1, b))
- If C[1] = C[2] then return 1 else return 0

A is always correct, thus it always outputs 0 in experiment Exp-ind-cpa-0, and never in Exp-ind-cpa-1. Thus ECB is not IND-CPA.

Analysis of the ECB mode.

Let E:{0,1}^k x {0,1}^n -> {0,1}^n be a block cipher. ECB={0,1}^k,E,D:

Encryption algorithm E

```
```

```
E_K  E_K  ......................
```

Conjecture, ECB hides the plaintexts.
But is it enough? Is ECB a good encryption scheme?
Is ECB IND-CPA secure?

Note

- We broke the ECB scheme without breaking the underlying block cipher (it can be secure PRF).
- The weaknesses were in the scheme, not the tools.
• **Claim.** Any deterministic, stateless scheme is not IND-CPA
• **Why?**

---

### Security of the CTRC

Let E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n be a function family. CTRC=(\{0,1\}^k,E,D):

**Encryption algorithm E**

- ctr is initially 0^n
- A current counter
- ctr is maintained as a state

The scheme is used to encrypt at most 2^n blocks (so that the counter does not wrap around)

* How good is the scheme?
* The flaws seem hard to find.
* Q. But may be they exist and we just don’t see them?
* A. The mode is as good as it can be and one can **prove** it.

---

### (In)security of CBCC

Let E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n be a block cipher. CBCC=(\{0,1\}^k,E,D):

**Stateful Encryption algorithm E**

```
ctr \rightarrow 0^n
```

incremented for each new message

```
ctr + 1
```

```
ctr + 2
```

```
ctr + m
```

- **Theorem.** CBCC is not IND-CPA. There exists an efficient adversary A with ind-CPA advantage 1.
- **Proof idea.**
  - Adversary \( \mathcal{A}^{E_k(\cdot, \cdot)} \)
  - \( M_{0_1} \rightarrow 0^n \); \( M_{1_1} \rightarrow 0^n \)
  - \( M_{0_2} \rightarrow 0^n \); \( M_{1_2} \rightarrow 0^{n+1} \)
  - \( (IV_1, C_1) \leftarrow E_k(\cdot, \cdot) ) \)
  - \( (IV_2, C_2) \leftarrow E_k(\cdot, \cdot) ) \)
  - If \( C_1 = C_2 \) then return 1 else return 0

---

### Security of CTRC, CTR\$, CBC\$

- **Theorem 1.** If E is a PRF, then CTRC is IND-CPA. I.e. For any adversary A there exists an adversary B such that
  - ind-CPA-advantage of A \( \leq 2 \) prf-advantage of B,
  - and B has comparable resources.
- **Theorem 2.** If E is a PRF, then CTR\$ is IND-CPA. (a similar concrete-security statement can be made).
- **Theorem 3.** If E is a PRF, then CBC\$ is IND-CPA. (a similar concrete-security statement can be made).
Did we get all we wanted?

- Is IND-CPA security definition strong enough (does it take into account all the bad things that can happen?)
- An adversary wants to win: to get some partial information about the plaintext from a challenge ciphertext
- What if the adversary can make the receiver to decrypt other ciphertexts of the adversary’s choice, learn the plaintexts and this helps it to win?
- Our definition didn’t consider such “chosen-ciphertext” attacks

Indistinguishability under chosen-ciphertext attacks

Fix an encryption scheme \( SE = (KeySp, E, D) \)

Pick a key \( K \) at random from \( KeySp \)

For an adversary \( A \) and a bit \( b \) consider two experiments \( \text{Exp-ind-cca-b (SE,A)} \), for \( b = 0 \) or \( b = 1 \)

The difference between probabilities of outputting 0 in two experiments is called \( \text{ind-cca-advantage} \) of \( A \) in attacking \( SE \).

A symmetric encryption scheme \( SE \) is indistinguishable under chosen-ciphertext attacks (IND-CCA secure) if prf-advantage of any adversary with “reasonable” resources is “close” to 0.