Lecture 6 – Symmetric-Key Encryption

COSC-260 Codes and Ciphers
Adam O’Neill

Adapted from http://cseweb.ucsd.edu/~mihir/cse107/
Setting the Stage

• We have studied our first lower-level primitive, blockciphers.
Setting the Stage

• We have studied our first lower-level primitive, blockciphers.
• Today we will study how to use it to build our first higher-level primitive, symmetric-key encryption.
Syntax

A symmetric-key encryption scheme $\mathcal{SE} = (K, E, D)$ is a triple of algorithms defined as follows.

* The key-generation algorithm $K$ outputs a key $K$.

* The encryption algorithm $E$ on input $K$ and a message $M \in \text{MsgSp}$ outputs a ciphertext $C$.

* The decryption algorithm on input $K$ and $C$ outputs a message $m$ or $\perp$.
Correctness

For all $K$, output by $E$ and all $m \in \text{MsgSp}$,

$$\Pr[D(K, E(K, m)) = m] = 1$$

where the probability is over the coins of $E$. 

$$c = E(K, m)$$

$D(K, c)$
Blockcipher Modes of Operation

\[ E : \{0, 1\}^k \times \{0, 1\}^n \to \{0, 1\}^n \text{ a block cipher} \]

**Notation:** \(x[i]\) is the i-th n-bit block of a string \(x\), so that \(x = x[1] \ldots x[m]\)

if \(|x| = nm\).

**Always:**

\[
\begin{align*}
\text{Alg } K \\
K &\overset{\$}{\leftarrow} \{0, 1\}^k \\
\text{return } K
\end{align*}
\]

Now we want encryption and decryption algs where the message-space consists of messages whose length is a multiple of \(n\).

Different such algs correspond to different modes of operations.
Electronic Codebook Mode

$\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ where:

**Algorithm $\mathcal{E}_K(M)$**

for $i = 1, \ldots, m$
do
$C[i] \leftarrow E_K(M[i])$

return $C$

**Algorithm $\mathcal{D}_K(C)$**

for $i = 1, \ldots, m$
do
$M[i] \leftarrow E_K^{-1}(C[i])$

return $M$

Correct decryption relies on $E$ being a block cipher, so that $E_K$ is invertible.
Weakness of ECB

\[ \text{Documents} \]

Looks which blocks are the same.
Introducing Randomized Encryption

• Encryption algorithm flips coins.
Introducing Randomized Encryption

• Encryption algorithm flips coins.
• Many possible ciphertexts for each message (using the same key).
Introducing Randomized Encryption

- Encryption algorithm flips coins.
- Many possible ciphertexts for each message (using the same key).
- Decryption still recovers the (unique) message.
CBC-$\$:
Cipher-block Chaining Mode with Random IV

$\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ where:

**Alg $\mathcal{E}_K(M)$**

\[
C[0] \leftarrow \{0, 1\}^n \\
\text{for } i = 1, \ldots, m \text{ do} \\
\quad C[i] \leftarrow E_K(M[i] \oplus C[i - 1]) \\
\text{return } C
\]

**Alg $\mathcal{D}_K(C)$**

\[
\text{for } i = 1, \ldots, m \text{ do} \\
\quad M[i] \leftarrow E_K^{-1}(C[i]) \oplus C[i - 1] \\
\text{return } M
\]

Correct decryption relies on $E$ being a block cipher.

Mihir Bellare
UCSD
CTR-$\$ Mode

**Counter mode with random IV.**

If $X \in \{0, 1\}^n$ and $i \in \mathbb{N}$ then $X + i$ denotes the $n$-bit string formed by converting $X$ to an integer, adding $i$ modulo $2^n$, and converting the result back to an $n$-bit string.

**Alg $E_K(M)$**

$C[0] \leftarrow \{0, 1\}^n$

for $i = 1, \ldots, m$ do

$P[i] \leftarrow E_K(C[0] + i)$

$C[i] \leftarrow P[i] \oplus M[i]$

return $C$

**Alg $D_K(C)$**

for $i = 1, \ldots, m$ do

$P[i] \leftarrow E_K(C[0] + i)$

$M[i] \leftarrow P[i] \oplus C[i]$

return $M$
Voting with CBC-§

Suppose we encrypt $M_1, M_2 \in \{Y, N\}$ with CBC$.

$E_K M_1 \xrightarrow{\dagger} C_1[0] \xrightarrow{\dagger} C_1[1]$

$E_K M_2 \xrightarrow{\dagger} C_2[0] \xrightarrow{\dagger} C_2[1]$

Adversary $A$ sees $C_1[0] = C_1[0] C_1[1]$ and $C_2[0] = C_2[0] C_2[1]$.

Suppose $A$ knows that $M_1 = Y$.

Can $A$ determine whether $M_2 = Y$ or $M_2 = N$?
Assessing Security

• How to determine which modes of operations are “good” ones?
Assessing Security

• How to determine which modes of operations are “good” ones?
• E.g., CBC-$ seems better than ECB. But is it secure? Or are there still attacks?
Assessing Security

• How to determine which modes of operations are “good” ones?
• E.g., CBC-\$ seems better than ECB. But is it secure? Or are there still attacks?
• Important since CBC-\$ is widely used.
Towards a Master Property

• As before, one approach is to list requirements for a “good” encryption scheme.
Towards a Master Property

• As before, one approach is to list requirements for a “good” encryption scheme.
  • Key recovery is hard.
Towards a Master Property

• As before, one approach is to list requirements for a “good” encryption scheme.
  • Key recovery is hard.
  • Message recovery is hard
Towards a Master Property

• As before, one approach is to list requirements for a “good” encryption scheme.
  • Key recovery is hard.
  • Message recovery is hard
  • ...


Towards a Master Property

• As before, one approach is to list requirements for a “good” encryption scheme.
  • Key recovery is hard.
  • Message recovery is hard
  • ...
• Better idea: Specify a master property that implies all the properties in such an (infinite) list.
Rule: Every query \((M_0, M_1)\) made by \(A\) must satisfy \(|M_0| = |M_1|\).

**IND-CPA**

Indistinguishability under chosen-plaintext attack

Let \(SE = (K, E, D)\) be an encryption scheme.

**Game \(\text{Left}_{SE}\)**

**procedure Initialize**
\(K \leftarrow \mathcal{K}\)

**procedure LR\((M_0, M_1)\)**

Return \(C \leftarrow E_K(M_0)\)

**Game \(\text{Right}_{SE}\)**

**procedure Initialize**
\(K \leftarrow \mathcal{K}\)

**procedure LR\((M_0, M_1)\)**

Return \(C \leftarrow E_K(M_1)\)

Associated to \(SE\), \(A\) are the probabilities

\[
\Pr\left[\text{Left}^A_{SE} \Rightarrow 1\right] \quad | \quad \Pr\left[\text{Right}^A_{SE} \Rightarrow 1\right]
\]

that \(A\) outputs 1 in each world. The (ind-cpa) advantage of \(A\) is

\[
\text{Adv}^{\text{ind-cpa}}_{SE}(A) = \Pr\left[\text{Right}^A_{SE} \Rightarrow 1\right] - \Pr\left[\text{Left}^A_{SE} \Rightarrow 1\right]
\]

**IND-CPA advantage of \(A\) against \(SE\).**
Advantage Interpretation

\[
\text{Adv}^\text{ind-cca}_{\mathcal{S}\mathcal{E}}(A) \approx 1 \text{ means } A \text{ is doing well and } \mathcal{S}\mathcal{E} \text{ is not ind-cca-secure.}
\]

\[
\text{Adv}^\text{ind-cca}_{\mathcal{S}\mathcal{E}}(A) \approx 0 \text{ (or } \leq 0) \text{ means } A \text{ is doing poorly and } \mathcal{S}\mathcal{E} \text{ resists the attack } A \text{ is mounting.}
\]

Adversary resources are its running time \( t \) and the number \( q \) of its oracle queries, the latter representing the number of messages encrypted.

**Security:** \( \mathcal{S}\mathcal{E} \) is IND-CPA-secure if \( \text{Adv}^\text{ind-cca}_{\mathcal{S}\mathcal{E}}(A) \) is “small” for ALL \( A \) that use “practical” amounts of resources.

**Insecurity:** \( \mathcal{S}\mathcal{E} \) is not IND-CPA-secure if we can specify an explicit \( A \) that uses “few” resources yet achieves “high” ind-cca-advantage.
Theorem. ECB is not IND-CPA secure.

Proof:

Adversary $A$

$C[1][2] \leftarrow LR(C_{0^n 0^n}, 1^n 0^n)$

If $C[1] = C[2]$ then ret 0

else ret 1.

$Adv_{ECB}^{ind-cpa}(A) = P[R_{\text{RIGHT}}^{A}_{ECB} = 1] - P[L_{\text{LEFT}}^{A}_{ECB} = 1]$

$\geq P[R_{\text{RIGHT}}^{A}_{ECB} = 1] = 1$ by def. of block cipher

$P[L_{\text{LEFT}}^{A}_{ECB} = 0] = 0$ by def. of block cipher.
Security Analysis of CTR-$^\$

Let $E : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a blockcipher and $SE = (K, E, D)$ the corresponding CTR$^\$ symmetric encryption scheme. Suppose 1-block messages $M_0, M_1$ are encrypted:

Let us say we are **lucky** if $C_0[0] = C_1[0]$. If so:

$$C_0[1] = C_1[1] \text{ if and only if } M_0 = M_1$$

So if we are lucky we can detect message equality and violate IND-CPA.
The Adversary

Adversary A

For i=1 to q do:

$c_i [T_0][i] \leftarrow \text{LR}(O^n, <i>)$

If for some i, j: $C_i[T_0] = C_j[T_0]$

If $C_i[T_1] = C_j[T_1]$ then return 0

Else return 1

Return 0.

Adv ind-cpa$_{ctr-8}$ (A) = $C(2^n, q) - 0 \geq \frac{3q(q-1)}{2^n}$. 
Advantage Analysis
Conclusion: CTR$ can be broken (in the IND-CPA sense) in about $2^{n/2}$ queries, where $n$ is the block length of the underlying block cipher, regardless of the cryptanalytic strength of the block cipher.
So far: A $q$-query adversary can break CTR$ with advantage $\approx \frac{q^2}{2^{n+1}}$

Question: Is there any better attack?
So far: A $q$-query adversary can break CTR with advantage $\approx \frac{q^2}{2^{n+1}}$

Question: Is there any better attack?

Answer: NO!

We can prove that the best $q$-query attack short of breaking the block cipher has advantage at most

$$\frac{\sigma^2}{2^n}$$

where $\sigma$ is the total number of blocks encrypted.

Example: If $q$ 1-block messages are encrypted then $\sigma = q$ so the adversary advantage is not more than $q^2/2^n$.

For $E = AES$ this means up to $2^{64}$ blocks may be securely encrypted, which is good.
Theorem Statement

**Theorem:** [BDJR98] Let $E : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a block cipher and $SE = (K, E, D)$ the corresponding CTR$\$ symmetric encryption scheme. Let $A$ be an ind-cpa adversary against $SE$ that has running time $t$ and makes at most $q$ LR queries, these totalling at most $\sigma$ blocks. Then there is a prf-adversary $B$ against $E$ such that

$$\text{Adv}_{\text{SE}}^{\text{ind-cpa}}(A) \leq 2 \cdot \text{Adv}_E^{\text{prf}}(B) + \frac{\sigma^2}{2^n}$$

Furthermore, $B$ makes at most $\sigma$ oracle queries and has running time $t + \Theta(\sigma \cdot n)$. 
• Analogous theorem holds for CBC-$\$. 
• Analogous theorem holds for CBC-$. 

• Provides a quantitative guarantee on how many blocks can be securely encrypted using these modes (assuming the underlying block cipher is good).