COS433/Math 473: Cryptography

Mark Zhandry
Princeton University
Spring 2017
Project 1 – 2nd Bonus

Still at 40 decrypts...

• Tristan Pollner and Zachary Stier

• Prinstun Criptoe (Heather Newman, Iris Rukshin, Jacob Wachspress)
Previously on COS 433...
Left-or-Right Experiment

\[ \text{Challenger} \]

\[ k \leftarrow K \]

\[ c \leftarrow \text{Enc}(k,m_b) \]

\[ b \]

\[ \text{LoR-Exp}_b(\text{Alice}) \]

\[ m_0, m_1 \in M \]

\[ c \]

\[ b' \]
Pseudorandom Functions

Functions that “look like” random functions

Syntax:
- Key space $K$ (usually $\{0,1\}^\lambda$)
- Domain $X$ (usually $\{0,1\}^m$)
- Co-domain/range $Y$ (usually $\{0,1\}^n$)
- Function $F:K \times X \rightarrow Y$
Pseudorandom Functions

Security:

\[ x \in X \]

Challenger

\[ b \]

\[ b' \]
Pseudorandom Functions

Security:

```
\text{Challenger}

b = 0

k \leftarrow K

y \leftarrow F(k, x)

PRF-Exp_0() 
```
Pseudorandom Functions

Security:

\( b' \)

\[ \begin{align*}
  & x \in X \\
  & y = H(x) \\
  & \text{Challenger} \quad H \leftarrow \text{Funcs}(X,Y) \\
  & b=1 \\
  & \text{PRF-Exp}_1(\cdot)
\end{align*} \]
Using PRFs to Build Encryption

\textbf{Enc}(k, m):
- Choose random \( r \leftarrow X \)
- Compute \( y \leftarrow F(k, r) \)
- Compute \( c \leftarrow y \oplus m \)
- Output \((r, c)\)

\textbf{Dec}(k, (r, c)):
- Compute \( y' \leftarrow F(k, r) \)
- Compute and output \( m' \leftarrow c \oplus y' \)

\textbf{Correctness}:
- \( y' = y \) since \( F \) is deterministic
- \( m' = c \oplus y = y \oplus m \oplus y = m \)
Today

Security for arbitrary-length messages

Block ciphers

Modes of operation
Security for Arbitrary-Length Messages

Impossible in general to hide message length
Security for Arbitrary-Length Messages

\[ m_0, m_1 \text{ s.t. } |m_0| = |m_1| \]

\[ c \leftarrow \text{Enc}(k, m_b) \]

\[ \text{IND-Exp}_b(\text{Challenger}) \]
Theorem: Given any CPA-secure \((\text{Enc,Dec})\) for fixed-length messages (even single bit), it is possible to construct a CPA-secure \((\text{Enc,Dec})\) for arbitrary-length messages.
Construction

Let \((\text{Enc}, \text{Dec})\) be CPA-secure for single-bit messages

\[\text{Enc}'(k, m):\]
For \(i = 1, \ldots, |m|\), run \(c_i \leftarrow \text{Enc}(k, m_i)\)
Output \((c_1, \ldots, c_{|m|})\)

\[\text{Dec}'(k, (c_1, \ldots, c_l)):\]
For \(i = 1, \ldots, l\), run \(m_i \leftarrow \text{Dec}(k, c_i)\)
Output \(m = m_1m_2\ldots,m_l\)
Theorem: If \((Enc, Dec)\) is \((t, q, \varepsilon)\)-LoR secure, then \((Enc', Dec')\) is \((t - t', q/n, \varepsilon)\)-LoR secure for messages of length up to \(n\)
Proof

Assume toward contradiction that there exists a running in time at most $t-t'$, making $q/n$ LoR queries on messages of length up to $n$, which has advantage $\varepsilon$ in breaking $(Enc',Dec')$

Construct that has advantage $\varepsilon$ in breaking $(Enc,Dec)$
Proof (sketch)

\[ m_0, m_1 \]

\[ (m_0)_1, (m_1)_1 \xleftarrow{c_1} \]

\[ (m_0)_2, (m_1)_2 \xleftarrow{c_2} \]

\[ (m_0)_3, (m_1)_3 \xleftarrow{c_3} \]

\[ \ldots \]

\[ c \xleftarrow{(c_1, \ldots)} \]
Better Constructions Using PRFs

In PRF-based construction, encrypting single bit requires $\lambda + 1$ bits

$\Rightarrow$ encrypting $l$-bit message requires $\approx \lambda l$ bits

Ideally, ciphertexts would have size $\approx \lambda + l$
Solution 1: Add PRG/Stream Cipher

**Enc(k, m):**
- Choose random \( r \leftarrow X \)
- Compute \( y \leftarrow F(k,r) \)
- Get \( |m| \) pseudorandom bits \( z \leftarrow G(y) \)
- Compute \( c \leftarrow z \oplus m \)
- Output \((r,c)\)

**Dec(k, (r,c)) :**
- Compute \( y' \leftarrow F(k,r) \)
- Compute \( z' \leftarrow G(y') \)
- Compute and output \( m' \leftarrow c \oplus z' \)
Solution 1: Add PRG/Stream Cipher

\[ r \leftarrow X \]

\[ k \]

\[ F \]

\[ y \]

\[ G \]

\[ z \oplus m \]

\[ (c, \quad \quad ) \]
Proof Sketch

Hybrid 0: \( (m_0, m_1) \rightarrow (r, G(F(k,r)) \oplus m_0) \)

Hybrid 1: \( (m_0, m_1) \rightarrow (r, G(s) \oplus m_0) \)

Hybrid 2: \( (m_0, m_1) \rightarrow (r, t \oplus m_0) \)

Hybrid 3: \( (m_0, m_1) \rightarrow (r, t \oplus m_1) \)

Hybrid 4: \( (m_0, m_1) \rightarrow (r, G(s) \oplus m_1) \)

Hybrid 5: \( (m_0, m_1) \rightarrow (r, G(F(k,r)) \oplus m_1) \)
Solution 2: Counter Mode

\textbf{Enc}(k, m):
- Choose random \( r \leftarrow \{0,1\}^{\lambda/2} \)
- For \( i=1,\ldots,|m| \),
  - Compute \( y_i \leftarrow F(k, r \Vert i) \)
  - Compute \( c_i \leftarrow y_i \oplus m_i \)
- Output \( (r, c) \) where \( c=(c_1,\ldots,c_{|m|}) \)

\textbf{Dec}(k, (r,c) ):
- For \( i=1,\ldots,l \),
  - Compute \( y_i \leftarrow F(k, r \Vert i) \)
  - Compute \( m_i \leftarrow y_i \oplus c_i \)
- Output \( m=m_1,\ldots,m_l \)

\footnotesize{Write \( i \) as \( \lambda/2 \)-bit string

Handles any message of length at most \( 2^{\lambda/2} \)}
Solution 2: Counter Mode

\[ \begin{align*}
X &\rightarrow r_1 \\
F &\oplus k \\
(, &\downarrow)
\end{align*} \]
Block ciphers/Pseudorandom Permutations
Pseudorandom Permutations
(also known as block ciphers)

Functions that “look like” random permutations

Syntax:
• Key space $K$ (usually $\{0,1\}^\lambda$)
• Domain=Range= $X$ (usually $\{0,1\}^n$)
• Function $F:K \times X \rightarrow X$
• Function $F^{-1}:K \times X \rightarrow X$

Correctness: $\forall k, x, F^{-1}(k, F(k, x)) = x$
Pseudorandom Permutations

Security:

\[ x \in X \]

Challenger

\[ b \]

\[ y \]

\[ b' \]
Pseudorandom Permutations

Security:

\[ x \in X \quad \downarrow \quad b' \]

\[ b = 0 \]

Challenger

\[ k \leftarrow K \]

\[ y \leftarrow F(k, x) \]

PRF-Exp_o(\cdot)
Pseudorandom Permutations

Security:

$$x \in X$$

Challenger

$$b = 1$$

$$H \leftarrow \text{Perms}(X, X)$$

$$y = H(x)$$

$$\text{PRF-Exp}_1(\cdot)$$
Definition: $F$ is a $(t, q, \varepsilon)$-secure PRP if, for all running in time at most $t$ and making at most $q$ queries,

$$\left| \Pr[1 \leftarrow \text{PRF-Exp}_0(\cdot)] - \Pr[1 \leftarrow \text{PRF-Exp}_1(\cdot)] \right| \leq \varepsilon$$
Theorem: A PRP $(F, F^{-1})$ is $(t, q, \varepsilon)$-secure iff $F$ is $(t, q, \varepsilon + q^2/2|X|)$-secure as a PRF
Proof

Secure as PRP $\implies$ Secure as PRF

• Assume hybrids

**Hybrid 0:**

$$x \in X$$

**Challenger**

$$k \leftarrow K$$

$$y \leftarrow F(k, x)$$
Proof

Secure as PRP $\Rightarrow$ Secure as PRF

• Assume hybrids

Hybrid 1:

Challenger $H \leftarrow \text{Perms}(X,X)$

$b' \\ x \in X \\ b' \\ y \\ y \leftarrow H(x)$
Proof

Secure as PRP $\Rightarrow$ Secure as PRF
• Assume $\mathcal{C}$, hybrids

Hybrid 2:

Challenger $\mathcal{H}\leftarrow\mathcal{F}_{\mathcal{F}_{\mathcal{F}}} (X,X)$

$b'$
Proof

Secure as PRP ⇒ Secure as PRF
• Assume hybrids

Hybrids 0 and 1 are indistinguishable by PRP security

Hybrids 1 and 2?
• In Hybrid 1, sees random distinct answers
• In Hybrid 2, sees random answers
• Except with probability $\approx \frac{q^2}{2|X|}$, random answers will be distinct anyway
Proof

Secure as PRF $\Rightarrow$ Secure as PRP
• Assume hybrids

Proof essentially identical to other direction
Suppose $(F, F^{-1})$ is a secure PRP

Is $(F^{-1}, F)$ also a secure PRP?
Counter Example

Suppose $(F, F^{-1})$ is a secure PRP. Assume $X = \{0,1\}^n$

Define $(H, H^{-1})$ as follows:
• Given $k$, let $i$ be smallest input such that $F^{-1}(i)$ begins with a 0
• Let $x_0 = F^{-1}(0^n)$, $x_1 = F^{-1}(i)$
• $H(k, x) = \begin{cases} 
0^n & \text{if } x = x_1 \\
i & \text{if } x = x_0 \\
F(k, x) & \text{otherwise}
\end{cases}$
How to use block ciphers for encryption
Counter Mode (CTR)

\[ \text{IV} \oplus F(k) \oplus \text{IV} \]

\[ \text{IV} \oplus F(k) \oplus \text{IV} \]

\[ \text{IV} \oplus F(k) \oplus \text{IV} \]

\[ \text{IV} \oplus F(k) \oplus \text{IV} \]

\[ \text{IV} \oplus F(k) \oplus \text{IV} \]
Electronic Code Book (ECB)

**Enc(k, m):**
- Break $m$ into $t$ blocks $m_i$ of $n$ bits
- For each block $m_i$, let $c_i = F(k, m_i)$
- Output $c = (c_1, ..., c_t)$

**Dec(k, c):**
- Break $c$ into $t$ blocks $c_i$ of $n$ bits
- For each block $c_i$, let $m_i = F^{-1}(k, c_i)$
- Output $m = (m_1, ..., m_t)$

substitution cipher for $n$-bit alphabet
Electronic Code Book (ECB)
ECB Decryption
Security of ECB?

Is ECB mode CPA secure?

Is ECB mode one-time secure?
Security of ECB

Plaintex  |  Ciphertext  |  Ideal
Cipher Block Chaining (CBC) Mode

(For now, assume all messages are multiples of the block length)
CBC Mode Decryption
Theorem: If $(F, F^{-1})$ is a $(t, q, \epsilon)$-secure pseudorandom permutation, then CBC mode encryption is $(t - t', q/n, 2\epsilon + q^2/|X|)$ CPA secure for messages of length up to $n$. 
Proof Sketch

Assume toward contradiction an adversary 🐜 for CBC mode

Hybrids...
Proof Sketch

Hybrid 0

\[ \mathbf{IV} \oplus \mathbf{F} \oplus \mathbf{F} \oplus \mathbf{F} \oplus \mathbf{F} \oplus m_0 \]

\[ (\mathbf{IV}, \ldots, \mathbf{IV}) \]
Proof Sketch

Hybrid 1

(IV, m_0)

(, )
Proof Sketch

Hybrid 2

\( \oplus \)

\( m_1 \)

\( IV \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( IV \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( H \)

\( \oplus \)

\( \oplus \)

\( \oplus \)

\( \oplus \)
Proof Sketch

Hybrid 3

\[ \text{IV} \oplus F \quad F \quad F \quad F \quad \oplus \quad m_1 \]

(\text{IV} \quad , \quad \text{IV})
Proof Sketch

Hybrid 0,1 differ by replacing calls to $F$ with calls to random permutation $H$

- Indistinguishable by PRP security

Same for Hybrids 2,3

All that is left is to show indistinguishability of 1,2
Proof Sketch

Hybrid 1

(IV ⊕ H ⊕ H ⊕ H ⊕ H ⊕ m₀)

(IV , H , H , H , H , H)
Proof Sketch

Hybrid 2

\( (\text{IV}, m_1) \)

\( \mathbf{H} \)

\( \mathbf{H} \)

\( \mathbf{H} \)

\( \mathbf{H} \)

\( \mathbf{H} \)
Proof Sketch

Idea:
• As long as, say, the sequence of left messages queried by does not result in two calls to \( F \) on the same input, all outputs will be random (distinct) outputs
• For each message, first query to \( F \) will be uniformly random
• Second query gets XORed with output of first query to \( F \) \( \Rightarrow \approx \) uniformly random
Proof Sketch

Idea:
• Since queries to $\mathcal{F}$ are (essentially) uniformly random, probability of querying same input twice is exponentially small
• Ciphertexts will be essentially random
• True regardless of encrypting $m_0$ or $m_1$
Stateful Variants of CBC

Chained CBC
• IV is set to last block of previous ciphertext

Deterministic IV
• Sender keeps a counter
• To encrypt, IV is set to counter, and counter is incremented

Both variants mean no need to send IV
Deterministic IV

ctr

( )

( )

ctr ++
Is Deterministic IV Secure?
Chained CBC

\[ \text{IV} \xrightarrow{\oplus} \mathcal{F} \xrightarrow{k} \mathcal{F} \xrightarrow{\oplus} \mathcal{F} \xrightarrow{k} \mathcal{F} \xrightarrow{\oplus} \mathcal{F} \xrightarrow{k} \mathcal{F} \xrightarrow{\oplus} \mathcal{F} \xrightarrow{k} \mathcal{F} \xrightarrow{\oplus} \mathcal{F} \]
Is Chained CBC Secure?
CBC Mode with Predictable IV

In general, if you can predict the IV of the next message, you can break CBC-mode encryption.

Idea:
• Set first block of next message to be the next IV
• Then $F$ will be applied to 0
• First block of ciphertext will be $F(k,0)$

So if we set left messages in this way, all first blocks will be the same.
Output Feedback Mode (OFB)

```
IV \rightarrow \text{F} \rightarrow k \rightarrow \text{F} \rightarrow k \rightarrow \text{F} \rightarrow k \rightarrow \text{F} \rightarrow k \rightarrow \text{F} \rightarrow \cdots
```

Turn block cipher into stream cipher
OFB Decryption

\[ k \rightarrow F \rightarrow k \rightarrow F \rightarrow k \rightarrow F \rightarrow k \rightarrow F \]

\[ \text{IV} \oplus \rightarrow \text{Output} \]

\[ F_k \oplus \]

\[ F_k \oplus \]

\[ F_k \oplus \]

\[ F_k \oplus \]
What happens if a block is lost in transmission?

OFB decryption:

\[ \text{Same goes for CTR mode} \]
Cipher Feedback (CFB)

Turn block cipher into self-synchronizing stream cipher
CFB Decryption

\[ \text{IV} \oplus F_k \oplus F_k \oplus F_k \oplus F_k \]
What happens if a block is lost in transmission?

CFB decryption:
What happens if a block is lost in transmission?

What about CBC?
Security of OFB, CFB modes

Security very similar to CBC

Define 4 hybrids
• 0: encrypt left messages
• 1: replace PRP with random permutation
• 2: encrypt right messages
• 3: replace random permutation with PRP

0,1 and 2,3 are indistinguishable by PRP security

1,2 are indistinguishable since ciphertexts are essentially random
Summary

PRPs/Block Ciphers

Modes of operations: ECB, Counter, CBC, OFB, CFB
Next Time

Designing PRPs/PRFs
Reminders

My OH today are delayed until 5pm
• Resume normal schedule next week

HW2 due tomorrow

Project 1 due next week