Post project ideas to Piazza. Form teams!

Today:

- "Ideal" block cipher
- Modes of operation:
  - Common: ECB, CTR, CBC, CFB, ...
  - Ideal (IND-CCA defn.)
  - Desai's "UFEE" mode
- Start stream ciphers if time

Project idea:

"Program obfuscation"

(recent work often called "indistinguishability obfuscation")

Readings:

- Wikipedia "Block cipher modes of operation"
- Katz/Lindell Chapter 3 (esp. 3.6.2 & 3.7)
- Paar/Pelzl Chapter 5 (esp. 5.1)
- Ferguson et al. Chapter 4
- Wikipedia "Ciphertext stealing"
For practical purposes, can treat AES as ideal block cipher:

For each key, mapping $\text{Enc}(K, \cdot)$ is a random independent permutation of $\{0,1\}^b$ to itself.

Modes of Operation:

How to encrypt variable-length messages? (using AES)

- **ECB** = "Electronic code book"
- **CTR** = "Counter mode"
- **CBC** = "Cipher-block chaining" (CBC-MAC)
- **CFB** = "Cipher feedback"

... (others...)

**ECB**:

\[ E \]
\[ C_1 \]  \[ E \]
\[ C_2 \]
\[ \vdots \]
\[ E \]
\[ C_n \]  \[ \rightarrow \text{divide data into b-bit blocks, where } b = \text{input block size} \]

To handle data that is not a multiple of b bits in length:

- Append a "1" bit (always)
- Append enough "0" bits to make length a multiple of b bits.

This gives invertible (1-1) "padding" operation. Pad before encryption; unpad after decryption.

**ECB** preserves many patterns: repeated message blocks $\rightarrow$ repeated ciphertext blocks

**ECB** really only good for encrypting random data (e.g. keys)
CTR (Counter mode):

Generate a PR (pseudorandom) sequence by encrypting \( i, i+1, \ldots \)
XOR with message to obtain ciphertext.

\[
\begin{array}{ccc}
K & \rightarrow & E \\
\downarrow & & \downarrow \\
X_i & \rightarrow & E \\
\downarrow & & \downarrow \\
M_1 & \rightarrow & + \\
\downarrow & & \downarrow \\
C_1 & \rightarrow & C_1 \\
\end{array}
\]

\[
\begin{array}{ccc}
K & \rightarrow & E \\
\downarrow & & \downarrow \\
X_i+1 & \rightarrow & E \\
\downarrow & & \downarrow \\
M_2 & \rightarrow & + \\
\downarrow & & \downarrow \\
C_2 & \rightarrow & C_2 \\
\end{array}
\]

\[
\begin{array}{ccc}
K & \rightarrow & E \\
\downarrow & & \downarrow \\
X_i+2 & \rightarrow & E \\
\downarrow & & \downarrow \\
M_3 & \rightarrow & + \\
\downarrow & & \downarrow \\
C_3 & \rightarrow & C_3 \\
\end{array}
\]

Initial counter value can be transmitted first:

\( i, C_1, C_2, \ldots \)

Of course, no counter value should be re-used!
CBC (Cipher-block chaining):

Choose IV ("initialization value") randomly, then use each \( C_i \) is "IV" for \( M_{i+1} \). Transmit IV with ciphertext:

\[
IV, C_1, C_2, \ldots, C_n
\]

Decryption easy, and parallelizable (little error propagation)

Look up "ciphertext stealing" for cute way of handling messages that are not a multiple of 6 bits in length. This method gives ciphertext length = message length.

Last block \( C_n \) is the "CBC-MAC" (CBC Message Authentication code) for message \( M \). [A fixed IV is used here.] The MAC is a "cryptographic checksum" (more later...). (If messages have variable length then key for last block should be different.)

IV might be \( Enc(k, msg \#) \) or \( Enc(k, nonce) \). Saves space if \( msg \# \) does not need to be transmitted, or is short.

MAC should use a different key than that used for encryption. Requires 2 passes to do CBC-Enc, then CBC-MAC over ciphertext.
CFB (Cipher feedback mode)

Similar to CBC mode. Uses random IV transmitted with ciphertext.

If $M$ is not a multiple of $b$ bits in length, can just transmit shortened ciphertext. (No need for ciphertext stealing.)
Are these modes good ones? What do we want?

If block cipher is indistinguishable from ideal block cipher then mode provides indistinguishability based on chosen ciphertext attack (IND-CCA):

- Define as game with adversary.
- Mode is IND-CCA secure if adversary can win with probability at most $\frac{1}{2} + \epsilon$ for "negligible" $\epsilon$.

Let $K$ be randomly chosen key.
Let $E_K$ denote encryption (using mode) with key $K$.
Let $D_K$ denote decryption.

Phase I ("Find"):  
- Adversary given black-box access to $E_K$, $D_K$ (can encrypt/decrypt whatever it likes).
- Adversary outputs two messages $m_0$, $m_1$, of same length, plus state information $s$.

Phase II ("Guess"):  
- Examiner secretly picks $d \leftarrow \{0,1\}^*$
  Examiner computes $y = E_K(m_d)$
- Adversary given $y$, $s$, access to $E_K$, and access to $D_K$ (except on $y$).
- Adversary computes for a while, then must produce bit $\hat{d}$ as its guess for $d$.
- Adversary's advantage is $|P(\hat{d}=d) - \frac{1}{2}|$.

Encryption secure against CCA attack if advantage is negligible.
Fact: To be IND-CCA secure, method must be randomized.

(else Adv can encrypt m₀, m₁, & compare to y)

& randomization should not be evident to Adv (i.e. not usable for decryption)

Previous modes are not IND-CCA secure!

**ECB:** not randomized

**CTR:** starting counter value might be random, but it is transmitted in clear. In any case, it is legal for Adv to ask for decryption of prefix of y (giving prefix of md)

**CBC:** similar to CTR: IV might be random, but it is transmitted in clear. Decryption of prefix of y also works.

**CFB:** Same. IV in clear; prefix argument works.

Can one design a IND-CCA scheme?
Theorem: Modes ECB, CTR, CBC, CFB are not IND-CCA secure.

Proof: Adversary picks $m_0 = 0^x$, $m_1 = 1^x$ for large $x$.

Then $y = E_k(m_0)$

Let $z = 1^x$ half of $y$.

Since $z \neq y$, Adversary allowed in phase II to ask for $D_k(z)$.

This gives first half of $m_0$, revealing $d_0$.

Adversary always wins. \qed

Can one design a IND-CCA scheme?

Given a ciphertext $y$ for a message $m$,

Adversary should not be able to construct a ciphertext $z$ for a related (e.g. truncated) message.

(nonmalleability)
Here is a sketch of one IND-CCA secure method, (due to Desai. UFE = "Unbalanced Feistel encryption")

- **M** = long message, sequence $M_1, M_2, ..., M_n$ of $b$-bit blocks
- **K** = $(K_1, K_2, K_3)$ Three indep. keys for block ciphers
- $r \leftarrow \{0, 1\}^b$ starting counter value
- pad $P = P_1 P_2 ... P_n$ where $P_i = E_{K_1}(r + i) \leftarrow$ (CTR mode)
- ciphertext $C = C_1, C_2, ..., C_n$ where $C_i = M_i \oplus P_i$
- **CBC-MAC:** $X_0 = 0^b$
  - $X_i = E_{K_2}(X_{i-1} \oplus C_i)$ for $i < n$
  - $X_n = E_{K_3}(X_{n-1} \oplus C_n)$ (MAC)
- $\sigma = r \oplus X_n$ use MAC to mask $r$ (no message authentication)
- **Output:** $C_1, C_2, ..., C_n, \sigma$

- **VO-PRF**
- **VI-PRF**

---

**CRYPTO 2006**
• Encryption with UFE can be done in single pass over data, but decryption requires two passes:
  - first to compute max \( X_n \), then to get \( r \)
  - second to decrypt \( C \) to get \( M \)
• Only designed for confidentiality (there is no way provided for receiver to tell if ciphertext has been tampered with.) (Need to use MAC on top of all of this, or some "combined mode" providing both confidentiality & integrity.)
• Note "unbalanced Feistel structure".
• Length of ciphertext \((C,0^r) = |M| + |r|\);
  expansion only as needed for randomization.
  No need for "ciphertext stealing" since we use CTR mode.