Computer Security
CS 426
Lecture 4

Cryptography: Block Ciphers and Encryption Modes

Why Block Ciphers?

- One thread of defeating frequency analysis
  - Use different keys in different locations
  - Example: one-time pad, stream ciphers

- Another way to defeat frequency analysis
  - Make the unit of transformation larger, rather than encrypting letter by letter, encrypting block by block
  - Example: block cipher

Block Ciphers

- An n-bit plaintext is encrypted to an n-bit ciphertext
  - $\mathcal{P}$: $\{0,1\}^n$
  - $\mathcal{C}$: $\{0,1\}^n$
  - $\mathcal{K}$: $\{0,1\}^s$
  - **E**: $\mathcal{K} \times \mathcal{P} \rightarrow \mathcal{C}$: E_k: a permutation on $\{0,1\}^n$
  - **D**: $\mathcal{K} \times \mathcal{C} \rightarrow \mathcal{P}$: D_k is E_k^{-1}
  - Block size: n
  - Key size: s

Ideal block cipher

- An ideal block cipher is a substitution cipher from $\{0,1\}^n$ to $\{0,1\}^n$ i.e., a Random Permutation (RP)
- Total number of keys: $2^n!$
  - insecure when n is small
  - impractical when n is large ($2^{64}! \geq 2^{2^{71}}$)
    - How much space is needed to represent the key?
- Solution: PseudoRandom Permutation (PRP)
  - Use a subset of the $2^n!$ possible permutations
- A PRP cannot be distinguished from RP by any computationally bounded adversary

Block ciphers aim at providing a PRP.

Data Encryption Standard (DES)

- Designed by IBM, with modifications proposed by the National Security Agency
- US national standard from 1977 to 2001
- De facto standard
- Block size 64 bits;
- Key size 56 bits
- 16-rounds
- Designed mostly for hardware implementations
- Considered insecure now
  - vulnerable to brute-force attacks

Attacking Block Ciphers

- Types of attacks to consider
  - known plaintext: given several pairs of plaintexts and ciphertexts, recover the key (or decrypt another block encrypted under the same key)
  - how would chosen plaintext and chosen ciphertext work?
- Standard attacks
  - exhaustive key search
  - dictionary attack
  - differential cryptanalysis, linear cryptanalysis
- Side channel attacks.

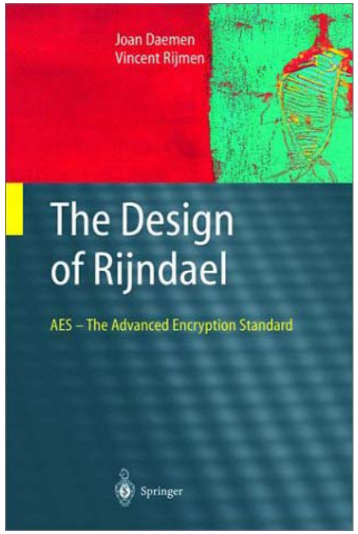
DES's main vulnerability is short key size.

Advanced Encryption Standard

- In 1997, NIST made a formal call for algorithms stipulating that the AES would specify an unclassified, publicly disclosed encryption algorithm, available royalty-free, worldwide.
- Goal: replace DES for both government and private-sector encryption.
- The algorithm must implement symmetric key cryptography as a block cipher and (at a minimum) support block sizes of 128-bits and key sizes of 128-, 192-, and 256-bits.
- In 1998, NIST selected 15 AES candidate algorithms.
- On October 2, 2000, NIST selected **Rijndael** (invented by Joan Daemen and Vincent Rijmen) to as the AES.

AES Features

- Designed to be efficient in both hardware and software across a variety of platforms.
- Not a Feistel Network
- Block size: 128 bits
- Variable key size: **128, 192, or 256 bits.**
- Variable number of rounds (10, 12, 14):
  - 10 if K = 128 bits
  - 12 if K = 192 bits
  - 14 if K = 256 bits
- No known weaknesses



Need for Encryption Modes

- A block cipher encrypts only one block
- Needs a way to extend it to encrypt an arbitrarily long message
- Want to ensure that if the block cipher is secure, then the encryption is secure
- Aim at providing Semantic Security (**Ciphertext indistinguishability)**
  – i.e., if an adversary chooses two messages M_0 and M_1, and is given $E_K[M_b]$, where b is randomly chosen from {0,1}, the adversary has little advantage in guessing b

Block Cipher Encryption Modes: ECB

- Message is broken into independent block;
- Electronic Code Book (ECB): each block encrypted separately.
- **Encryption: $c_i = E_k(x_i)$**
- **Decrytion: $x_i = D_k(c_i)$**

Properties of ECB

- Deterministic:
  - the same data block gets encrypted the same way,
    - reveals patterns of data when a data block repeats
  - when the same key is used, the same message is encrypted the same way
- Usage: not recommended to encrypt more than one block of data

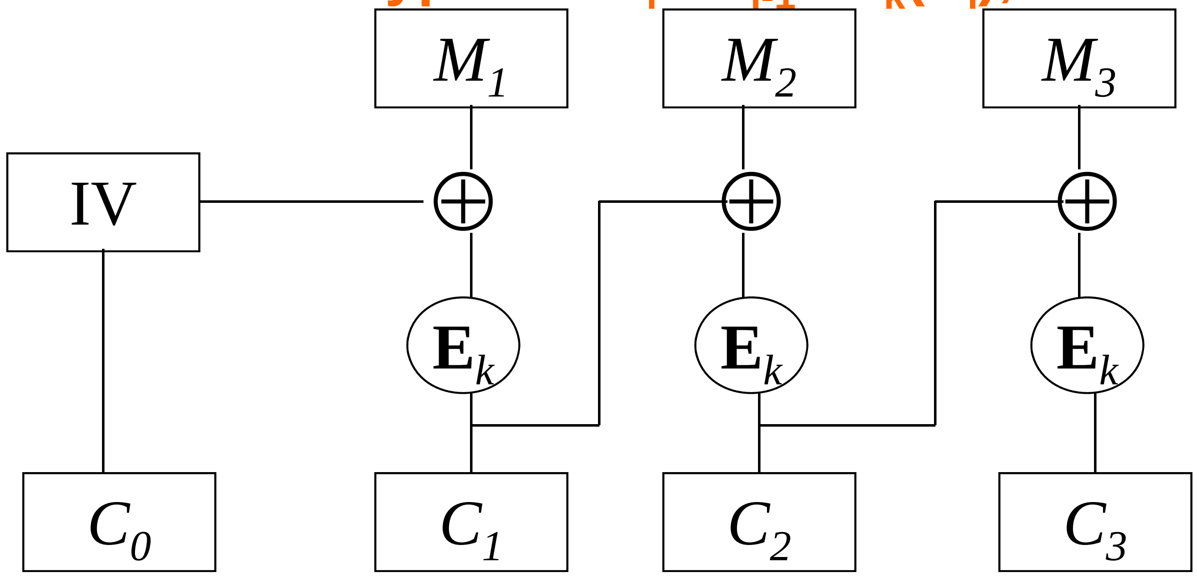
- How to break the Semantic security (Ciphertext indistinguishability) of a block cipher with ECB?

DES Encryption Modes: CBC

- Cipher Block Chaining (CBC):
  - Uses a random Initial Vector (IV)
  - Next input depends upon previous output

    Encryption: $C_i = \mathbf{E}_k(M_i \oplus C_{i-1})$, **with** C_0**=IV**

    Decryption: $M_i = C_{i-1} \oplus \mathbf{D}_k(C_i)$, **with** C_0**=IV**



Properties of CBC

- Randomized encryption: repeated text gets mapped to different encrypted data.
  - can be proven to provide semantic security assuming that the block cipher is PRP and that random IV's are used
- A ciphertext block depends on all preceding plaintext blocks; reorder affects decryption
- Usage: chooses random IV and protects the integrity of IV

Encryption Modes:CTR

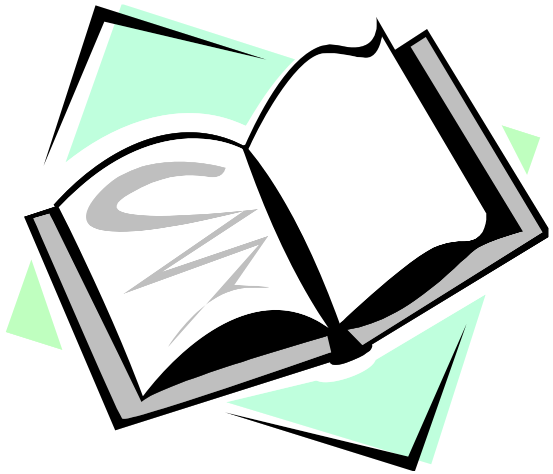
- Counter Mode (CTR): A way to construct PRNG using a block cipher
  - Uses a random counter
  - $y_i = E_k[\text{counter}+i]$
  - Sender and receiver share: counter (does not need to be secret) and the secret key.

Properties of CTR

- Gives a stream cipher from a block cipher
  - subject to limitations of stream ciphers (what are they?)
- Randomized encryption:
  - when starting counter is chosen randomly
- Random Access: decryption of a block can be done in random order, very useful for hard-disk encryption.

Readings for This Lecture

- Required reading from wikipedia
  - Block Cipher
  - Data Encryption Standard
  - Advanced Encryption Standard
  - Block cipher modes of operation



Coming Attractions …

- Cryptography: Cryptographic Hash Functions and Message Authentication