Outline

- Block cipher modes
- Hash functions
- One-way functions
- Pseudo-random generators
- Pseudo-random functions
- Message authentication code

Block Cipher Modes

- Electronic Codebook Mode (ECB)
  - Not secure, same input block → same output
- Cipher Block Chaining Mode (CBC)
  - Recommended
- Cipher Feedback Mode (CFB)
  - Initial vector (IV) must not be repeated
- Output Feedback Mode (OFB)
  - Initial vector (IV) must not be repeated
- Counter Mode (CTR)
  - Highly recommended
**Electronic Code Book (ECB)**

- $M_1 = M_2 \Rightarrow C_1 = C_2$
- No error propagation

**Cipher Block Chaining (CBC)**

$(M_1 = M_3)$ very unlikely leads to $(C_1 = C_3)$

**CBC Decryption**
CBC Properties

- Chaining dependency
  - Each ciphertext block depends on all preceding plaintext blocks
- Error propagation
  - Each error in $c_i$ affects decipherment of $c_i$ and $c_{i+1}$
- Error recovery
  - An error in $c_i$ doesn’t propagate beyond $c_{i+1}$
  - Can recover from loss of cipher text blocks
- IV selection
  - Fixed IV, counter IV, random IV
  - Using ECB mode to encrypt and setup a random IV

Counter Mode (Encryption)

CRT(Decryption)
Advantages and Limitations of CTR

- A “new” mode, though proposed early
- Efficiency
  - can do parallel encryptions
  - Preprocess in advance of need
    - good for bursty high speed links
- Random access to encrypted data blocks
- Provable security (good as other modes)
- But must ensure never reuse key/counter values, otherwise could break

Hash Algorithms

Message m of arbitrary length $\xrightarrow{\text{Hash} H} \text{A fixed-length short message}$

- Also known as
  - Message digests
  - Hash functions
  - We only consider cryptographically secure hash functions
- Length of $H(m)$ much shorter than length of $m$
- Usually fixed lengths: 128, 160, 256 bits
- Examples
  - MD5, SHA-1, SHA-256

Hash Algorithms (2)

- Desirable properties of hash functions
  - Efficiency: Easy to compute $H(m)$
  - One-way property: Given $H(m)$ but not $m$, it’s difficult to find $m$
  - Weak collision resistance: Given $H(m)$, it’s difficult to find $m'$ such that $H(m') = H(m)$.
  - Strong collision resistance: Computationally infeasible to find $m_1$, $m_2$ such that $H(m_1) = H(m_2)$
- Never collision free
  - Limited number of output values
Applications of Hash Functions

- Primary application
  - Generate/verify digital signature

  \[\text{Message } m \xrightarrow{H} \text{Signature } \text{Sig}(H(m))\]

  \[\text{Message } m \xrightarrow{H} \text{Verify } \text{Yes/No}\]

  \[\text{Public key}\]

  \[\text{Private key}\]

Applications of Hash Functions (2)

- Password hashing
  - Doesn’t need to know password to verify it
  - Store \(H(\text{password} + \text{salt})\) and salt, and compare it with the user-entered password
  - Salt makes dictionary attack more difficult

- Message integrity
  - Agree on a secret key \(k\)
  - Compute \(H(m|k)\) and send with \(m\)

- Message authentication codes (MAC)
  - HMAC, very well used

One-way Function

- Definition
  - A function which is “easy” to calculate but “hard” to invert
    - The computation of \(f(x)\) is tractable given \(x\), \(f\)
    - The computation of the preimage of \(f(x)\) is not tractable given only \(f(x)\)

- Facts
  - It is not known whether one-way function exist
  - Their existence would imply \(P \neq NP\)

- Candidates
  - Based on hard problems (e.g., IF or DL problem)
    - e.g., multiplication of two large primes
One-way Function (cont’d)

- Trapdoor one-way function
  - A function which is hard to invert unless some secret information, called “trapdoor”, is known
  - E.g., RSA, the private key is the trapdoor
- Cryptographic hash functions
  - Also require the one-way property
  - Have additional stringent requirements on collision resistance
  - Can be used as a one-way function
    - Since hash functions such as MD5 or SHA-1 are believed to be secure

Pseudo Random Number Generator (PRNG)

- Definition
  - A cryptographically secure pseudorandom bit generator is an efficient algorithm that will expand a random \( n \)-bit seed to a longer pseudorandom sequence that is computationally indistinguishable from a truly random sequence.
- Theorem [Levin]
  - A one-way function can be used to construct a cryptographically secure pseudo-random bit generator.

PRNG Examples

- Blum-Blum-Shub generator
  - Strong generator, provably secure under the assumption that integer factorization is intractable
  - Too slow for real use
- Heuristic generators
  - Count mode of a block cipher (e.g., AES)
  - Cryptographically secure hash of a count
    - The count is secure and random
  - Stream cipher, e.g., RC4
- Linear feedback shift registers (LFSRs)
  - Very simple and efficient,
  - But not cryptographically secure
Pseudorandom Functions

- **Definition**
  - A family of functions \( \{f_k\} \) is a pseudorandom function family PRF if any adversary A cannot distinguish between a function \( f_k \) (where \( k \) is chosen randomly and kept secret) and a totally random function.

- **Theorem** [Goldreich, Goldwasser, Micali]
  - Cryptographically secure pseudorandom functions can be constructed from cryptographically secure pseudorandom bit generators.

PRF

- **Property**
  - As long as the key \( k \) is random (or pseudorandom) and remains unknown, the value \( k_1 = f_k(x) \) is also pseudorandom for any fixed and known \( x \).

- **Application**
  - Derive two keys from a single key for different purposes
    - \( K_1 = f_k(0) \) for encryption
    - \( K_2 = f_k(1) \) for authentication

Message Authentication

- **Message authentication** is the process to verify that received messages come from the alleged source and have not been altered.
- **The goals of message authentication** is to prevent
  - Masquerade: insertion of messages from a fraudulent source.
  - Content modification: change of messages
  - Sequence modification: insertion, deletion and reordering of messages.
  - Timing modification: delay or replay of messages.
Message Authentication Code

- **MAC**
  - The symmetric equivalent of digital signature
  - Also known as cryptographic checksum, Message Integrity Code (MIC).
  - Assumption: the sender and the receiver share a common secret key.
  - A small fixed-size block generated from the message with secret key cryptography.
  - Usually appended to the original message.

**MAC (Cont’d)**

- **Mode I**
  - Message authentication
  - No confidentiality

**MAC (Cont’d)**

- **Mode II**
  - Message authentication and confidentiality
  - Authentication tied to plaintext
MAC (Cont’d)

- Mode III
  - Message authentication and confidentiality
  - Authentication tied to ciphertext

Requirements for MAC

- For $M$ and $C_K(M)$, it’s computationally infeasible to construct a message $M'$ such that $C_K(M') = C_K(M)$.
- $C_K(M)$ should be uniformly distributed in terms of $M$
  - For any two messages $M$ and $M'$, $Pr[C_K(M) = C_K(M')] = 2^{-n}$, where $n$ is the number of bits in the MAC.
  - Intuition: prevent chosen plaintext attack.

MAC Constructions

- PRFs
  - A PRF can be used as a MAC
- HMAC
  $$HMAC(k, m) = H(k \oplus a \parallel H(k \oplus b \parallel m))$$
  - $H$: MD5, SHA-1
- CBC-MAC
  - Based on block cipher CBC mode
MAC - DES CBC Mode

- Known as Data Authentication Algorithm
- DES CBC mode with IV being zero.
- A message is padded with zeroes to form 64-bit blocks.
- The data authentication code (DAC, i.e., the MAC) consists of either the entire last ciphertext block or the left M bits with $16 \leq M \leq 64$.

MAC - DES CBC Mode (2)

```
ENC

M1
64

ENC

M2
64

ENC

M3
64

ENC

M4
46 64

DAC
(16 to 64 bits)
```