Chapter 7: Cryptography and the PKI

# Overview of Cryptography

Cipher: the process of scrambling characters.

Types of ciphers:

* Substitution Cipher: changing a character into another.
  + Caeser cipher shifting all letters into a certain space amount.
* Polyalphabetic Substitution: shifting the letters multiple times.
  + Vigenère cipher uses a table. Figure 7.1
* Transposition Cipher: breaking the message into equal size blocks then scrambling the context of each box.

Steganography is the practice of using cryptographic techniques.

# Goals of Cryptography

## Confidentiality

* Symmetric cryptosystems: shared secret keys known to all users.
* Asymmetric cryptosystems: each user has a combination of private and public keys.

Obfuscation: Practice of making it intentionally difficult for humans to understand how code works.

Encryption data on Disk:

* Full-disk encryption (FDE)
* Partition Encryption
* File-level encryption
* Volume encryption

Encryption Database Data:

* Transparent Data Encryption (TDE): everything
* Column-level Encryption (CLE): Specific columns
* Recor-level Encryption: individual records.

## Integrity

This includes the use of digital signatures

## Authentication

Figure 7.6

## Non-repudiation

Def.

# Cryptographic Concepts

Plain text (P) Ciphertext (C)

All cryptographic messages rely on keys.

Key space: range of values that are valid for use as a key for a specific algorithm.

Keys (cryptovariables) and key spaces are binary can be 2128 long and even longer.

Cryptoanalysis: the study to decode ciphers.

Modern ciphers fit 2 categories:

* Block Ciphers
* Stream Ciphers

# Modern Cryptography

## Symmetric Key Algorithm

Shared key. Figure 7.7

Weaknesses:

* Key exchange
* Does not implement non-repudiation
* Algorithm not scalable
* Keys must be regenerated often

## Asymmetric Key Algorithms

Everyone has a public and private key. Figure 7.8

Table page 206

Strengths:

* Adding new users only 1 public-private key is needed.
* Users can be removed more easily.
* Key regeneration is only needed for private keys.
* Provides Integrity, authentication, and non-repudiation.
* Key exchange is simple.
* No preexisting communicated links need to exist.

Issue: slow speed.

Table 7.1

Collisions: when hash values create the same value for different methods.

# Symmetric Cryptography

Advanced Encryption Standard (AES):

* 128-bit 🡪 10 rounds of encryption
* 192-bit 🡪 12 rounds of encryption
* 256-bit 🡪 14 rounds of encryption

## Symmetric Key Management

* Creation and Distribution: 3 main methods for key exchange
  + Offline Distribution: physical.
  + Public key encryption: uses public keys to connect then switch to private keys to communicate.
  + Diffie-Hellman: When public and private keys aren’t good enough.
* Storage and Destruction
  + Never store encryption key where the encryption data resides.
  + Split knowledge: 2 individuals with half of a key.
* Key Escrow and Recovery
  + Key Escrow: a 3rd party stores a copy of the protected key.

## Asymmetric Cryptography

RSA  
Elliptic Curve

# Hash Functions

Mathematical function that takes input data of any length and transforms it into a fixed-length output, called a "digest", which acts as a unique identifier for the original data.

5 requirements:

* Accept input of any length.
* Output of a fixed length.
* Hash value easy to compute.
* Hash function is one-way.
* Collision free.

SHA &MD5

# Digital Signatures

2 Goals:

* Message came from claimed sender.
* Shows message was not altered.

Hash-Based Message Authentication (HMAC) does everything a digital signature does but is non-repudiation.

Encrypt a message 🡪 recipient’s public key

Decrypt a message 🡪Your private key

Digitally sign a message🡪your private key

Verify a signature🡪sender’s public key

# Public Key Infrastructure (PKI)

X.509 certificate attributes:

* Version of X.509 where certificate conforms
* Serial number
* Signature algorithm identifier
* Issuer name
* Validity period
* Subject’s common name (CN)
* Certificates may contain Subject Alternative Names (SANs)
* Subject’s public key

Assurance for public keys:

* Computer/machine
* Individual users
* Email addresses
* Developers

Wildcard: a special character (\*) used in a certificate to secure multiple subdomains under a single domain.

Certificate Authorities (CAs) approved digital certificates:

* IdenTrust
* Amazon Web Services
* DigiCert Group
* Sectigo/Comodo
* GlobalSign
* Let’s Encrypt
* GoDaddy

Registration Authorities (RAs): help CAs in verifying users’ identities.

## Certificate Generation and Destruction

* Enrollment
  + prove identity to CA.
  + Provide public key in form of a Certificate Signing Request (CSR).
  + CA can also verify the subject has control over a domain (Domain Validation (DV)).
  + Extended Validation (EV) check to see if the business is legit.
* Verification
  + Verify for a CA signature
  + Use Certification Revocation List (CRL) or Online Certificate Status Protocol (OCSP) to make sure certificate was not revoked.
  + To check if the public key is authentic
    - Must have a CA signature
    - Trust in the CA
    - Not in CRL
    - Certificate contains trusted data.
  + Certificate Pinning: When a browser has a certificate for a period of time.
* Revocation
  + reasons
    - Certificate was compromised
    - Certificate was erroneously issued
    - Details of the certificate changed
    - Security association changed
  + Identify revoked certificates:
    - Certificate Revocation Lists (CRLs)
    - Online Certificate Status Protocol (OCSP)
    - Certificate Sampling
* Certificate Formats
  + Table 7.2

# Asymmetric Key Management

* Choose encryption system
* Pick a random key
* Use public key encryption while keeping private key a secret
* Retire keys
* Back up keys
* Use Hardware Security Modules (HSMs)

# Cryptographic Attacks

* Brute Force
* Frequency Analysis: look for common patterns at the blocks of encryption.
* Known Plain Text
* Chosen Plain Text
* Related Key Attacks
* Birthday Attack
* Downgrade Attack: trick the user into using a less secure version of the protocol.
* Hashing, Salting, and Key Stretching:
  + Using a Rainbow table: list of common passwords.
  + Adding a random generated value to each password.
  + Use of thousands of passwords based on hashing and salting.

# Emerging Issues in Cryptography

* Tor and Dark Web
* Blockchain
* Lightweight Cryptography
* Quantum Computing
* Homomorphic Encryption: protect privacy of individuals but still calculate their data.