Cryptography

MIS-5903

http://community.mis.temple.edu/mis5903sec011s17/

Cryptography History

- Substitution
  - Monoalphabetic
  - Polyalphabetic (uses multiple alphabets) uses Vigenere Table
- Scytale cipher (message wrapped around wooden rod)
- Rotate
  - ROT3, aka "Caesar Cipher"
- Transposition – values are scrambled
  - Vulnerable to frequency analysis

- Plaintext -> Encryption -> Ciphertext -> Decryption -> Plaintext
- Algorithm (cipher) set of rules how enciphering and deciphering

Kerckhoff's Principle

- Auguste Kerchkhoff
- Published 1883
- Only secrecy in a cryptography system should be the key
- If too many secrets, there are more vulnerabilities to exploit

Strength of Cryptosystem

- Algorithm
- Secrecy of the key
- Length of the key
- Initialization vectors
- How components work together

- Cryptography strength = work factor
  - Estimate of the effort and resources to penetrate cryptosystem

One Time Pad

- Considered unbreakable if implemented properly
- Gilbert Vernam, 1917 (aka Vernam Cipher)
- Uses a pad of random values
- Uses a binary mathematic function (XOR)
- Requirements:
  - Made up of truly random values
  - Used only once
  - Securely distributed
  - Secured at sites
  - At least as long as the message

Spy-Novel Ciphers

- Running Key – set of books
  - Book page, line number, column count
- Concealment – message within a message
  - E.g. every third word

Steganography

- "Hiding in plain sight"
- "Security through obscurity"
- Three Components:
  - Carrier – signal, data stream or file that has hidden information (payload) inside
  - Stegomedium – medium in which the information is hidden
  - Payload – the information that is to be concealed and transmitted

Digital Rights Management (DRM)

- Movies/Video
  - High-Bandwidth Digital Content Protection (HDCP) – HDMI, DisplayPort, DVI
  - Advanced Access Content System (AACS) – Blu-Ray and HD-DVD
- E-Book
  - Adobe Digital Experience Protection Technology
- Video Games (e.g. Ubisoft Uplay)
- Documents (e.g. Vitrium, FileOpen)
  - Restrictions on reading, modifying, removing watermarks, saving, printing, screen capture, copying

Symmetric Algorithms

- Block Cipher
  - Confusion –
    - Substitution; making the relationship between key and ciphertext complex.
  - Diffusion (Claude Shannon) –
    - Transposition – Single plaintext bit has influence over several ciphertext bits
    - Avalanche effect (Horst Feistel) – slight change = significant ciphertext change
- Stream Cipher – streams of bits
  - Mathematical functions performed on each bit
  - Use keystream generator to produce ciphertext
- Initialization Vectors
  - Random value used with algorithm
  - Two identical plaintext values encrypted with same key / randomness

Cryptographic Transformation

- Compression
- Expansion
- Padding
- Key mixing
  - Key schedules – generate subkeys from master keys

Symmetric - DES

- Data Encryption Standard – 64 bit blocks, 64-bit key (56+8), 16 rounds
- Triple Des (3DES) – two or three keys, 48 rounds

Symmetric - Advanced Encryption Standard (AES)

- Five finalists – MARS, RC6, Serpent, Twofish, Rijandel
- Rijandel:
  - 128-bit – 10 rounds
  - 192-bit – 12 rounds
  - 256-bit – 14 rounds

Symmetric - International Data Encryption Algorithm (IDEA)

- 64 bit divided into 16 smaller blocks
- 8 rounds on each block
- 128-bit key

Other Symmetric:

- Blowfish – 64 bit data blocks, variable key 32-448 bits, 16 rounds
- RC4 – (Rivest, ‘87) – Stream, variable key, aka ArcFour
- RC5 – (Rivest) – 32, 64, or 128 block. Key up to 2048 bits
- RC6 – based on RC5; increased speed

Asymmetric

- Diffie-Hellman – key agreement
- RSA
  - Ron Rivest, Adi Shamir, Leonard Adleman(1978)
  - Authentication as well as key encryption
  - Key exchange protocol (encrypts the symmetric key)
- El Gamal
  - Public key algorithm used for signatures, encryption, key exchange. (slow!)
- Elliptic Curve Cryptosystems (ECC)
  - Similar to RSA; efficient; used in wireless devices
- Knapsack – e.g. Merkle - Hellman, insecure

Message Integrity

- One-Way Hash
- Message Authentication Code (MAC)
  - HMAC – Hash MAC
  - CBC-MAC – Cipher Block Chaining MAC
  - CMAC – Cipher-Based MAC
- Collisions – produce same value for two different messages
  - Birthday Paradox
    - 1 in 253 to be same as individual
    - 1 in 23 greater than any two

Available Hashing Algorithms

- MD4 (Rivest) 128-bit; no longer secure
- MD5 (Rivest) also 128-bit, but more complex than MD4
- Secure Hash Algorithm (SHA) – 160-bit
  - used with Digital Signature Algorithm
- SHA-256
- SHA-384
- SHA-512

Digital Signature

- Hash value encrypted with sender's private key
- Digital Signature Standard (1991) NIST standard
- Federal Government
  - Digital Signature Algorithm (only for signatures, slower than RSA)
  - RSA
  - Elliptic Curve Digital Signature Algorithm (ECDSA)

Public Key Infrastructure

- ISO authentication framework that uses public key cryptography and X.509
- Hybrid – uses symmetric and asymmetric
- Public Key Cryptography is one piece of PKI
- Certificate Authorities – trusted third party
- Registration Authority – registration, but not issuance
- Certificate Revocation List
- Online Certificate Status Protocol – real-time verification

Cryptography Attacks

- Ciphertext-Only – attempt to discover key – has access to ciphertext (COA)
- Known-Plaintext (brute force) (KPA)
- Chosen Plaintext (can choose which plaintext) (CPA)
- Chosen Ciphertext (may need control of the system) (CCA)
- Adaptive Chosen Plaintext – Chooses subsequent plaintext based on previous ciphertext (CPA2)
- Adaptive Chosen Ciphertext – Chooses subsequent ciphertext based on previous plaintext (CCA2)

Side Channel Cryptography Attacks

- Replay
- Algebraic
- Analytic
- Statistical
- Social Engineering Attacks
- Meet-in-the-Middle Attacks

Questions?