Chapter 01: Foundations

Uday Manchanda

November 2, 2019

Abstract

Chapter 01 Notes in the book *Applied Cryptography* by Bruce Schneier

1 1.1: Terminology

- Messages and Encryption
  - Message is a plaintext
  - Encrypted message is a ciphertext
  - Cryptanalysis: breaking ciphertexts
  - $E(M) = C$, the encryption function E encrypts M to obtain C
  - $D(C) = M$, the decryption function D decrypts C to obtain M
  - $D(E(M)) = M$
- Authentication, Integrity, Nonrepudiation
  - Authentication: receiver can ascertain its origin, intruder cannot masquerade as someone else
  - Integrity: receiver should be able to verify that message has not been modified in transit
  - Nonrepudiation: sender cannot later deny that he sent a message
- Algorithms and Keys
  - Cipher aka cryptographic algorithm is the mathematical function used for encryption and decryption
  - Restricted algorithms, where the security of an algorithm is secret, are bad
  - Modern crypto solves the problem with keys, where the range of possible values is the keyspace
  - Both encrytion and decryption use the same key, although some algorithms use a different key for encryption and decryption

  - Cryptosystem is an algorithm plus all possible plaintexts, ciphertexts, and keys

- Symmetric Algorithms
  - Encryption key can be calculated from the decryption key and vice-versa (usually the same)
  - Sender and receiver must agree on a key
  - Stream algorithm: operates on plaintext bit by bit
  - Block algorithm: operates on plaintext in group of bits aka blocks

- Public Key Algorithms
  - Key for encryption is different than decryption key
  - Encryption key (public key) is public, anyone can view it
  - Anyone can use a public key to encrypt a message but only a specific person with the corresponding decryption key can decrypt it
  - Decryption key is also known as the private key

- Cryptanalysis
  - Its about recovering the plaintext of a message without access to the key
  - Losing a key through noncryptanalysis is a compromise
  - Attempted cryptanalysis is an attack
  - Seven types of cryptanalytic attacks
    * **Ciphertext only attack**: the cryptanalyst has the ciphertext of several messages which have been encrypted with the same encryption algorithm. His job is to recover as many plaintexts as possible (or deduce the key used)
    * **Known plaintext attack**: Cryptanalyst has ciphertext and plaintext of those messages. He has to deduce the key (or keys) used to encrypt the message
    * **Chosen plaintext attack**: 0Cryptanalyst has access to the ciphertext and associated plaintext for several messages but also chooses the plaintext that gets encrypted. He/she can choose specific plaintext blocks to encrypt to reveal information about the key.
    * **Adaptive chosen plaintext attack**: Special case of a chosen plaintext attack. He can choose the plaintext that is encrypted, but also modify the choice based on results of previous encryption.
    * **Chosen ciphertext attack**: Cryptanalyst can choose different ciphertexts to be decrypted and has access to the decrypted plaintext. He must deduce the key.

        * **Chosen key attack**: he has some knowledge about the relationship between different keys
        * **Rubber hose cryptanalysis**: cryptanalyst threatens/blackmails someone until they give up the key
    - Known plaintext attacks and chosen plaintext attacks are relatively common
    - Kerckhoff's assumption: secrecy must reside entirely in the key. Assume that the cryptanalyst has complete details of the cryptographic algorithm and implementation.
    - Always share the inner workings of your cryptgraphic implementations!
- Security of algorithms
    - Important that the value of the data remain less than the cost to break the security protecting it.
    - Categories of breaking algorithms
        * Total break: cryptanalyst finds key
        * Global deduction: cryptanalyst finds alternate algorithm that is equivalent to D without knowing K
        * Instance deduction: cryptanalyst finds plaintext of an intercepted ciphertext
        * information deduction: cryptanalyst gains some information about key or plaintext
    - If there is not enough information to recover plaintext from ciphertext, no matter how much ciphertext a cryptanalyst has, the algorithm is unconditionally secure
    - Algorithm is computationally secure if it cannot be broken with current resources
    - Can measure complexity of an attack by: data complexity, processing complexity, storage requirements

2 1.2: Steganography

- Steganography serves to hide secret messages in other messages, especially within pictures

3 1.3: Substitution Ciphers and Transposition Ciphers

- Substitution Ciphers

  - Where each character in the plaintext is substituted for another character in the ciphertext
  - Four types of substitution ciphers
    * Simple substitution cipher: each character of the plaintext is replaced with a corresponding character of ciphertext
    * Homophonic substitution cipher: similar to previous except a single character of plaintext can map to several characters of ciphertext
    * Polygram substitution cipher: blocks of characters are encrypted in groups
    * Polyalphabetic substitution cipher: multiple sipmle substitution ciphers
  - Caesar cipher: each character in plaintext is replaced by character three to the right modulo 26
  - ROT13: similar to casear except 13 instead of 3

- Transposition Ciphers
  - plaintext remains the same but order of characters is shuffled around
  - Simple columnar transposition cipher: plaintext is written horizontally onto a piece of graph paper of fixed width
  - Frequency analysis of the characters is used

4 1.4: Simple XOR

- XOR = exclusive OR : $\oplus$
- If the digits are the same: 0, if different: 1
- $a \oplus a = 0$
- $a \oplus b \oplus b = a$
- Since XORing the same value twice restores the original, encryption and decryption use the same program
- $P \oplus K = C$
- $C \oplus K = P$
- How to break:
  - Discover length of key by a procedure known as counting coincidences
  - XOR ciphertext against shifted various number of bytes and count those bytes that are equivalent

  - If the displacement is a multiple of the key length: >6% of the bytes will be equal
  - If not: <0.4% will be equal
  - This is known as index of coincidence
  - Smallest displacement that indicates a multiple of the key length is the length of the key
  - Shift ciphertext by that length and XOR with itself
  - This removes the key and leaves with plaintext XORed with plaintext shifted the length of the key
  - English has 1.3 bits of real information per byte

5 1.5: One Time Pads

- The perfect encryption scheme
- Large, nonrepeating set of truly random key letters
- Sender uses each key letter on the pad to encrypt exactly one plaintext character
- Add plaintext character plus one time key pad character and modulo 26
- As long as the attacker cannot get access to the one time pad, the scheme is perfectly secure
- Requires both the sender and receiver to agree on a pre-shared key
- Key letters have to be generated randomly, a psuedo random number does not work because it has nonrandom properties
- Cannot use the same pad again (hence, one time)
- Length of key pad and message must be the same
- Useful for short messages, nothing large

6 1.6: Computer Algorithms

- Different types of cryptographic algorithms
  - DES (Data Encryption Standard): symmetric algorithm, most popular one used, same key used for encryption and decryption
  - RSA: most popular public key algorithm, used for encryption and digital signatures
  - DSA (Digital Signature Algorithm): public key algorithm, used for digital signatures NOT encryption

7 1.7: Large Numbers

Physical Analogue	Number
Odds of being killed by lightning (per day)	1 in 9 billion (2^{33})
Odds of winning the top prize in a U.S. state lottery	1 in 4,000,000 (2^{22})
Odds of winning the top prize in a U.S. state lottery and being killed by lightning in the same day	1 in 2^{55}
Odds of drowning (in the U.S. per year)	1 in 59,000 (2^{16})
Odds of being killed in an automobile accident (in the U.S. in 1993)	1 in 6100 (2^{13})
Odds of being killed in an automobile accident (in the U.S. per lifetime)	1 in 88 (2^{7})
Time until the next ice age	14,000 (2^{14}) years
Time until the sun goes nova	10^{9} (2^{30}) years
Age of the planet	10^{9} (2^{30}) years
Age of the Universe	10^{10} (2^{34}) years
Number of atoms in the planet	10^{51} (2^{170})
Number of atoms in the sun	10^{57} (2^{190})
Number of atoms in the galaxy	10^{67} (2^{223})
Number of atoms in the Universe (dark matter excluded)	10^{77} (2^{265})
Volume of the Universe	10^{84} (2^{280}) cm^3
If the Universe is Closed:	
Total lifetime of the Universe	10^{11} (2^{37}) years 10^{18} (2^{61}) seconds
If the Universe is Open:	
Time until low-mass stars cool off	10^{14} (2^{47}) years
Time until planets detach from stars	10^{15} (2^{50}) years
Time until stars detach from galaxies	10^{19} (2^{64}) years
Time until orbits decay by gravitational radiation	10^{20} (2^{67}) years
Time until black holes decay by the Hawking process	10^{64} (2^{213}) years
Time until all matter is liquid at zero temperature	10^{65} (2^{216}) years
Time until all matter decays to iron	$10^{10^{26}}$ years
Time until all matter collapses to black holes	$10^{10^{76}}$ years