COMP4109 Midterm 1 General Notes

William Findlay

October 11, 2019

1 Types of Cryptography

- symmetric key
  - ▶ shift ciphers
  - ▶ block ciphers
  - ▶ stream ciphers
- asymmetric key (public-private key)
- hashing
- protocols

2 Security Notions Models

- three components of a model
  1. attack model
     - ▶ ciphertext only attack (P) (COA)
       - ◦ attacker attempts to decrypt ciphertext to plaintext
     - ▶ known plaintext attack (P) (KPA)
       - ◦ attacker knows one or more plaintext-ciphertext pairs
     - ▶ chosen plaintext attack (A) (CPA)
       - ◦ attacker chooses a plaintext and encrypts it to receive ciphertext
     - ▶ chosen ciphertext attack (A) (CCA)
       - ◦ attacker chooses a ciphertext and decrypts it to receive plaintext
  2. security goal
     - ▶ (IND) indistinguishability
       - ◦ ciphertext should be indistinguishable from random string
     - ▶ (NM) non-malleability
       - ◦ cannot modify ciphertext so it decrypts to another plaintext that makes sense
  3. level of security
     - ▶ information theoretic
       - ◦ attacker has unlimited resources at their disposal
     - ▶ complexity theoretic
       - ◦ attacker has resources bounded $O(p)$ where p is the security parameter
     - ▶ computational (realistic)
       - ◦ attacker has the resources of n computers
- two components of a notion
  - ▶ goal + attack model
  - ▶ e.g. IND-COA or NM-COA or IND-KPA, etc.

3 Unicity Distance

- expected minimum length of ciphertext needed to uniquely compute a secret key
- $\frac{\log_2 |K|}{R_L \log_2 |P|}$
  - ▶ where R_L is redundancy of the language
  - ▶ R_{English} is about 0.75

4 Shift Ciphers

4.1 Caesar Cipher

- choose a key from $\mathbb{Z}_{|P|}$
- $c_i = p_i + k \bmod |P|$

4.1.1 Strengths

- none really, this sucks

4.1.2 Weaknesses

- easy to brute force
- weak to frequency analysis

4.2 Affine Cipher

- choose any a and b mod 26
  - except a gcd(a,26) must be 1
- $k = (a, b)$ where
  - $E_k(m) = (am + b) \bmod 26$
  - $D_k(c) = a^{-1}(c - b) \bmod 26$

4.2.1 Strengths

- better than caesar cipher
- two unknowns

4.2.2 Weaknesses

- use frequency analysis to solve for a and b
- not much better than Caesar really

4.3 Substitution Cipher

- permute P to get $\mathcal{A}$
- sub P_i fo $\mathcal{A}_i$

4.3.1 Strengths

- no strengths, don't use this

4.3.2 Weaknesses

- weak to CPA
- weak to KPA
- weak to COA
  - frequency analysis
  - exhaustive search won't work though

4.4 Vigenère Cipher

- choose some k_l as a plaintext string of length l
- encrypt $c_i = p_i + k_{i \bmod l} \bmod |P|$

4.4.1 Strengths

- much better than what we've seen so far
- if the length of the key is equal to the length of the message, very strong

4.4.2 Weaknesses

- can find candidate key lengths by factoring
- weak to frequency analysis
- multiple encryptions with same key opens up attacks

4.5 One-Time Pad

- like Vigenère except:
  - ▶ change key each time
  - ▶ perfect security if key length is equal to message length

4.5.1 Strengths

- perfect security for key length = message length
  - ▶ semantically secure in information theoretic security against COA

4.5.2 Weaknesses

- key can only be used one time
- key length the same as message length is kind of silly
  - ▶ why not just send the message over the secure channel in the first place
  - ▶ very long keys are impractical
- each key needs to be truly random
- has malleability
  - ▶ no authentication, only confidentiality

5 Block Ciphers

6 Stream Ciphers

7 Hashing Functions

8 MACs