Основи криптографії

Лекція 3. Елементи теорії зв“язку в секретних системах Клода Шеннона

План

- Робота К.Шеннона «Теорія зв“язку в секретних системах»
- Ідеальний шифр.
- Класифікація та вимоги до сучасних криптосистем.

Теорія зв“язку в секретних системах

- Клод Елвуд Шеннон та його робота «Теорія зв“язку в секретних системах», по суті, започаткував період наукової криптографії.
- Робота у вигляді секретної доповіді «Математична теорія криптографії», була розсекречена після Другої світової війни — сформувала обличчя сучасної криптографії. Його внесок часто порівнюють з впливом на фізику Ісаака Ньютона.
- К.Шеннон народився у 1916 році в м.Гейлорді (штат Мічиган). У 1936 році закінчив Масачусетський технологічний інститут з двох спеціальностей одночасно: математиці та електротехніці.

Теорія зв“язку в секретних системах

- 1940 року — захистив докторську дисертацію, де він уперше застосував до описання роботи реле та перемикачів булеву алгебру. На той час це було революційною справою.
- У 1941 році він працював у Bell Laboratories, де займався розробкою криптографічних систем, що дозволило йому відкрити методи кодування з корекцією помилок.
- Метою К.Шеннона було забезпечення достовірного передавання інформації зашумленими каналами (телефон, телеграф).
- Для цього йому довелося сформулювати, що таке інформація, чим визначається її кількість.
- У роботах 1948-49 рр. Він визначив кількість інформації через ентропію — величину, яку використовують у термодинаміці та статистичній фізиці як міру

Теорія зв“язку в секретних системах

- К.Шеннон розглядає шифрування як відображення відкритого тексту в шифрограму: $C_i = F_K(M)$, де C — шифротекст (*ciphertext*); M — відкритий текст (*message*), F_K — відповідне відображення; індекс К відповідає конкретному криптографічному ключу, який використано для шифрування.
- Для того, щоби існувала можливість однозначного розшифрування повідомлення, відображення F_K повинно мати єдине обернене відображення F^{-1}_K таке, що $F_K\ F^{-1}_K = I$, де I — тотожне перетворення: $M=F^{-1}_K(C)$.
- Джерело ключів повинно бути при цьому статистичним процесом або пристроєм, що задає відображення F_1, F_2,… F_N з ймовірностями p_1, p_2, …, p_N.

Теорія зв“язку в секретних системах

- Розглянемо найпростіший шифр заміни (наприклад, шифр Цезаря).
- Тоді алфавіт повідомлень співпадає з алфавітом криптограм та множиною знаків ключів.
- Шифрування виконується послідовною заміною знаків відкритого тексту знаками криптограми залежно від чергового значення знаків ключа.
- Відкритий текст, ключ та криптограма — послідовності літер того самого алфавіту: $M=\{m_1 m_2 m_3 \ldots m_n\}$; $K=\{k_1 k_2 k_3 \ldots k_n\}$; $C=\{c_1 c_2 c_3 \ldots c_n\}$.
- Кожен крок шифрування визначається співвідношенням: $c_i=f(m_i,k_i)$.
- У практичних системах довжина ключа може бути значно меншою за довжину повідомлення. Ключ на кожному кроці може обчислюватися з деякого первісного ключа меншого розміру, а ключова

Теорія зв“язку в секретних системах

- Задача криптоаналітика полягає у відновленні відкритого тексту за криптограмою, знаючи множину відображень F_1, F_2,… F_N.
- Існують криптосистеми, для яких будь-який об“єм перехопленої інформації недостатній для знаходження шифрувального відображення, причому ***ситуація не залежить від обчислювальних потужностей криптоаналітика***.
- Шифри такого типу називаються ***безумовно стійкими*** (***абсолютно стійкими***), за Шенноном — ***ідеально секретними***.
- Це можливо лише тоді, коли *M* і *C* статистично незалежні.
- Безумовно стійкі системи існують, що буде показано далі.

Теорія зв“язку в секретних системах

- Інший тип криптосистем — це такі, криптостійкість яких значна, але має кінцеве значення.
- Це означає, що криптоаналітик за кінцевий (але дуже великий) час, маючи певні обчислювальні ресурси, може подолати криптозахист такого шифру.
- Такі шифри мають назву ***обчислювально стійких***.
- Найбільше розповсюджені якраз обчислювально стійкі шифри.

Чому?

Теорія зв“язку в секретних системах

- Справа в тому, що користуватися абсолютно стійким шифром досить незручно, і його використовують лише надзвичайно критичних випадках.
- Простіше розробити обчислювально стійкий шифр за умови, щоби обчислювальні витрати на його подолання перевищували сьогоднішні можливості.
- Наприклад, якщо кількість операцій, які треба виконати для того, щоби подолати криптозахист, становить 10^9 — 10^{12}, можна вважати, що шифр достатньо стійкий.

Теорія зв“язку в секретних системах

- У першій лекції ми бачили як одну із загадок криптографії, фестський диск.
- Чому не можуть розшифрувати написи на ньому?
- Для однозначного розшифрування замало інформації.
- Значить, існує така довжина повідомлення, при якій це неможливо!
- І навпаки: існує якась мінімальна кількість інформації (довжина повідомлення), при якій криптоаналітична задача має єдиний розв“язок.
- Мінімальна довжина криптограми, для якої існує єдиний розв“язок криптоаналітичної задачі, називається ***інтервалом єдиності***.
- Для різних мов він різний, але коливається в районі 40-50 символів.

Теорія зв“язку в секретних системах

Висновки:

- Робота К.Шеннона «Теорія зв“язку в секретних системах» започаткувала науковий етап розвитку криптографічної науки.
- В роботі уведено поняття:
  - Безумовно стійкого шифру;
  - Обчислювально стійкого шифру;
  - Одиниці інформації;
  - Інтервалу єдиності;
  - Інші поняття, які ми розглядати не будемо.