Тема 16. КРИПТОГРАФІЧНА СТІЙКІСТЬ ШИФРІВ

Шифри можна класифікувати за криптографічною стійкістю, тобто за можливістю протистояти атакам крипто аналітика.

Питання про стійкість – найважливіше питання криптоаналізу шифрів.

Розглянемо різні підходи до оцінки криптографічної стійкості шифрів.

1. Абсолютно стійкі шифри

Питання про теоретичну стійкість шифрів вперше було сформульоване Клодом Шенноном: “На скільки надійна криптосистема, якщо криптоаналітик противника володіє необмеженим часом і всіма необхідними засобами для аналізу криптограм?” З цим питанням тісно пов’язане наступне: “Чи існують шифри, які не міг би розкрити криптоаналітик, що володіє як завгодно великою криптограмою і необмеженими обчислювальними ресурсами?”

Відомо, що ще до Шеннона над вирішенням цих питань працював американський інженер Д. Вернам, який в 1917 році запропонував новий спосіб шифрування телеграфних повідомлень. Алгоритм шифрування Вернама полягав в тому, що представлена в двійковому коді послідовність відкритого тексту побітно складалась з ключем – випадковою двійковою послідовністю. Додавання бітів відбувалося за модулем 2.

Вернам інтуїтивно відчував, що запропонований ним шифр володіє високими криптографічними якостями але строго довести цього не зумів.

Обґрунтував високі криптографічні якості шифру Вернама зумів Шеннон, він опублікував в 1949 р. основні положення теоретичної криптографії. З використанням ймовірнісної моделі шифру Шеннон дав математичне означення стійкого абсолютно шифру і показав, що шифр Вернама є дійсно абсолютно стійким.

За Шенноном шифр є *абсолютно стійким*, якщо відкриті і шифровані тексти статистично незалежні, тобто для будь-якого відкритого тексту a і будь-якої криптограми y виконується рівність: $P_{вх}(a) = P_{вх/ш}(a/y)$ при умові $P_{ш}(y)>0$. Іншими словами, при використанні абсолютно стійкого шифру розподіл

ймовірностей на множині відкритих текстів після перехоплення криптограми не відрізняється від розподілу ймовірностей на множині відкритих текстів до отримання перехопленої криптограми *y*. Перехоплення повідомлення, зашифрованого за допомогою абсолютно стійкого шифру, не містить для криптоаналітика ніякої інформації якщо ключ йому невідомий.

Шифр називається *ідеально стійким*, якщо неможливо визначити однозначно відкритий текст при відомому зашифрованому тексті будь-якої великої довжини. Очевидно, абсолютно стійкий шифр є ідеально стійким.

Шеннон довів, що абсолютно стійкі шифри існують, наприклад, так званий шифр Вернама по модулю *m*.

Також слід відмітити, що довжина ключа в абсолютно стійких шифрах співпадає з довжиною повідомлення. Це означає, що використання таких шифрів для захисту великих об'ємів інформації потребує великих трудових затрат, пов'язаних з розподілом, збереженням і знищенням ключових матеріалів.

Тим не менше абсолютно стійкі шифри все ж знайшли практичне застосування для захисту особливо важливих ліній зв'язку з відносно невеликим об'ємом інформації, що передається. [12]

2. Системний підхід до оцінки стійкості шифрів

Питання про практичну стійкість, поставлене Шенноном, формулюється так: "Чи надійна шифросистема, якщо крипто аналітик володіє обмеженим часом і обмеженими обчислювальними можливостями для аналізу перехоплених криптограм?" Дане питання тісно пов'язане з проблемою конструювання шифросистем.

З однієї сторони, криптографічна система повинна забезпечувати надійний захист інформації, з іншої – повинна бути зручна для технічної реалізації та експлуатації.

За Шенноном, практично стійка криптосистема за своїми властивостями повинна бути близька до ідеальної системи, тобто повинна бути вдалою підробкою під ідеальний шифр.

Системний підхід до оцінки стійкості шифросистеми має на увазі визначену деталізацію поняття «стійкий шифр». В результаті цієї деталізації формується ряд критеріїв математичного і технічного характеру, яким повинна задовольняти стійка шифросистема. При розробці нового підходу до аналізу шифросистеми формується відповідний критерій якості шифросистеми, який доповняє раніше складену систему критеріїв.

Основною кількісною мірою криптографічної стійкості шифру є *обчислювальна складність* рішення задач дешифрування. Обчислювальна складність визначається декількома характеристиками. Розглянемо найважливіші з них.

Припустимо, що перед криптоаналітиком поставлена задача дешифрування шифру E за деяким набором криптограм. Нехай A_E – клас застосовних до шифру E алгоритмів дешифрування, якими володіє крипто аналітик. При цьому криптоаналітик розглядає як ймовірнісний простір W елементарних подій множину пар ключів і відкритих текстів, якщо відкриті тексти відомі, або множину ключів, якщо відкриті тексти відомі. Для алгоритму $\psi \in A_E$ позначимо через $T(\psi)$ середню трудоємкість його реалізації, яка вимірюється за допомогою деяких умовних обчислювальних операціях. При цьому величина трудоємкості зазвичай усереднюється на множині W.

Однією з основних характеристик практичної стійкості шифру E є середня трудоємкість T_E дешифрування, що визначається за формулою

$$T_E = \min_{\psi \in A_E} T(\psi).$$

При цьому необхідно відмітити наступне:

1. Існують алгоритми дешифрування, визначені не на всьому ймовірнісному просторі W, а лише на деякій його частині. Крім того, деякі алгоритми дешифрування влаштовані так, що їх реалізація приводить до успіху (вирішення де шифрувальної задачі) не на всій області визначення, а лише на деякій її підмножині. Тому до важливих характеристик алгоритму дешифрування ψ слід віднести не тільки його трудоємкість $T(\psi)$, але і

надійність $v(\psi)$, під якою розуміється середня доля інформації, що дешифрується з використанням алгоритму ψ.

Якщо надійність алгоритму дешифрування мала, то з точки зору криптографа він є безпечним, а з точки зору криптоаналітика не ефективним. Таким чином, при отриманні оцінки величини $T(\psi)$ потрібно розглядати лише ті алгоритми дешифрування, надійність яких достатньо велика. При цьому для визначення "найкращого" алгоритму дешифрування системи E можна використовувати різні критерії в залежності від конкретних умов задачі.

2. Складність дешифрування залежить від кількісних і якісних характеристик криптограм, якими володіє криптоаналітик. Кількісні характеристики визначаються кількостю перехоплених криптограм і їх довжинами. Якісні характеристики пов'язані з достовірністю перехоплених криптограм *(наявність спотворень, пропусків,…)*. Оцінюючи стійкість шифру, криптоаналітик отримує верхні оцінки граничної стійкості, так як практичне дешифрування використовує обмежену кількість шифрматеріалу і обмежений клас так званих відомих методів дешифрування.

3. Важливою характеристикою криптографічної стійкості криптосистем є часова складність її дешифрування. Оцінка часової складності дешифрування системи має на увазі більш детальну обробку реалізації алгоритмів дешифрування з врахуванням характеристик обчислювального пристрою, що використовується для дешифрування. До таких характеристик обчислювального пристрою, що реалізує алгоритми дешифрування, відносяться архітектура, швидкодія, об'єм та структура пам'яті, швидкість доступу до пам'яті та інші. Тому, час дешифрування системи E визначається наявним класом алгоритмів дешифрування A_E і обчислювальними можливостями крипто аналітика.

Вибір найкращого алгоритму дешифрування ускладнюється й тим, що різним обчислювальним пристроям можуть відповідати різні "найкращі" алгоритми дешифрування.

Питання про криптографічну стійкість шифросистеми має деякі особливості з точки зору крипто аналітика і криптографа.

Криптоаналітик атакує шифросистему, володіючи конкретними інтелектуальними, обчислювальними та економічними ресурсами. Його ціль – успішно дешифрувати систему.

Криптограф оцінює стійкість шифросистеми, імітуючи атаку на шифр зі сторони криптоаналітика противника. Для цього криптограф моделює дії криптоаналітика, оцінюючи по максимуму інтелектуальні, обчислювальні, технічні та інші можливості противника. Ціль криптографа – впевнитися у високій криптографічній стійкості розробленої шифросистеми.

Таким чином, системний підхід до оцінки практичної стійкості шифру пов’язаний з оцінкою обчислювальних трудозатрат при дешифруванні системи з позиції різних критеріїв якості шифру. [12]

3. Інші підходи до оцінки практичної стійкості шифрів

Асимптотичний аналіз стійкості

Цей підхід розвивається теорію складності обчислень. При дослідженні шифру оцінка його стійкості пов’язана з деяким параметром шифру, зазвичай це довжина ключа, і проводиться асимптотичний аналіз оцінок стійкості.

Вважається, що криптосистема має високу криптографічну стійкість, якщо вона виражається через довжину ключа експоненціально, і шфиросистема має низьку криптографічну стійкість, якщо стійкість виражається у вигляді многочлена від довжини ключа.

Оцінка кількості необхідної шифрматеріалу.

Даний підхід оснований не на складності обчислень при реалізації дешифрування, а на оцінці середньої кількості матеріалу, який необхідно проаналізувати криптоаналітику для розкриття шифру. Оцінка кількості необхідного крипто аналітику шифр матеріалу передставляє інтерес з тієї точки зору, яка є нижньою оцінкою стійкості шифру в змісті обчислювальної складності дешифрування.

Цей підхід застосовується в основному для оцінки стійкості поточних рандомізірованих шифрів. Особливістю пристроїв таких шифрів є те, що вони використовують для шифрування та дешифрування секретний ключ невеликого розміру, а також велику і загальнодоступну випадкову послідовність чисел (рандомізатор). Ключ визначає, які частини рандомізатора використовуються для шифрування, у той час як крипто аналітику, який не знає секретного ключа, доводиться аналізувати весь рондомізатор.

В якості прикладу такого шифру розглянемо шифр Діффі. В цьому шифрі рандомізатором є масив з 2^n випадкових двійкових послідовностей, занумерованих елементами множини V_n. Ключем є n-мірний двійковий вектор. При шифруванні з використанням ключа k двійкова послідовність відкритого тексту складається побітно (як у шифрі Вернама) з послідовністю рандомізатора під номером k. Таким чином, для дешифрування повідомлення противнику необхідно дослідити порядку 2^n біт.

Згодом Рюппель помітив, що приблизно такий же рівень стійкості досягається, коли рандомізатор містить n випадкових двійкових послідовностей, а ключ k задає набір коефіцієнтів, який визначає шифруючу послідовність як нетривіальну лінійну комбінацію послідовностей рандомізатора.

Вартісний підхід.

Цей підхід передбачає оцінку вартості дешифрування системи. Особливо він актуальний тоді, коли для дешифрування криптосистеми необхідно розробити та побудувати новий обчислювальний комплекс. Вартісний підхід корисний з точки зору співставлення матеріальних затрат на дешифрування системи і цінності інформації, що захищається системою

Прикладом реалізації такого підходу є детальне виведення оцінки вартості дешифрування алгоритму DES, виконаний Діффі і Хеллманом у зв’язку з алгоритмом розпаралелювання перебору усіх ключів DES.

На закінчення відмітимо динамічний характер оцінок криптографічної стійкості шифрів. Ці оцінки необхідно час від часу переглядати у зв’язку з розвитком обчислювальних засобів і прогресу в області розробки методів

дешифрування. Існує “емпіричний закон” розвитку обчислювальних засобів, згідно якого вважається, що обчислювальні можливості криптоаналітика подвоюються через кожні 18 місяців. [12]