УДК 004.056

ВИМОГИ ДО КРИПТОГРАФІЧНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Маліновська О.О., Зінченко О.І., студенти групи КБ-171
Науковий керівник: **Усов Я.Ю.,** викладач
Чернігівський національний технологічний університет

Криптогра́фія — наука про математичні методи забезпечення конфіденційності, цілісності і автентичності інформації. Розвинулась з практичної потреби передавати важливі відомості найнадійнішим чином. Для математичного аналізу криптографія використовує інструментарій абстрактної алгебри та теорії ймовірностей.

Криптографі́чний за́хист інформа́ції — вид захисту інформації, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Історія криптографії

Найдавніші часи — Стародавній Рим. Найперші форми тайнопису вимагали не більше ніж аналог олівця та паперу, оскільки в ті часи більшість людей не могли читати. Поширення писемності, або писемності серед ворогів, викликало потребу саме в криптографії. Основними типами класичних шифрів є перестановочні шифри, які змінюють порядок літер в повідомленні, та підстановочні шифри, які систематично замінюють літери або групи літер іншими літерами або групами літер. Прості варіанти обох типів пропонували слабкий захист від досвідчених супротивників. Одним із ранніх підстановочних шифрів був шифр Цезаря, в якому кожна літера в повідомленні замінювалась літерою через декілька позицій із абетки. Цей шифр отримав ім'я Юлія Цезаря, який його використовував, зі зсувом в 3 позиції, для спілкування з генералами під час військових кампаній, подібно до коду EXCESS-3 в булевій алгебрі.

Шляхом застосування шифрування намагаються зберегти зміст спілкування в таємниці, подібно до шпигунів, військових лідерів, та дипломатів. Зберіглися також відомості про деякі з ранніх єврейських шифрів. Застосування криптографії радиться в Камасутрі як спосіб спілкування закоханих без ризику незручного викриття.[1] Стеганографія (тобто, приховування факту наявності повідомлення взагалі) також була розроблена в давні часи. Зокрема, Геродот приховав повідомлення — татуювання на поголеній голові раба — під новим волоссям. До сучасних прикладів стеганографії належать невидимі чорнила, мікрокрапки, цифрові водяні знаки, що застосовуються для приховування інформації.

Арабський період. Шифротексти, отримані від класичних шифрів (та деяких сучасних), завжди видають деяку статистичну інформацію про текст повідомлення, що може бути використано для зламу. Після відкриття частотного аналізу (можливо, арабським вченим аль-Кінді) в 9-му столітті, майже всі такі шифри стали більш-менш легко зламними досвідченим фахівцем. Класичні шифри зберігли популярність, в основному, у вигляді головоломок (див. Криптограма).

Давня Русь. Найраніші з відомих текстів на території Русі, записаних за допомогою тайнопису, належать до XII ст. Серед них: прості моноалфавітні шифри (проста літорея, письмо в квадратах), шифр зі заміною абетки (тайнопис глаголицею, грецькими літерами), мудра літорея, а також особливі прийоми письма (напр. мононкондил).

Відродження. Майже всі шифри залишались беззахисними перед криптоаналізом з використанням частотного аналізу до винаходу поліалфавітного шифру, швидше за все, Леоном-Баттіста Альберті приблизно в 1467 році (хоча, існують свідчення того, що знання про такі шифри існували серед арабських вчених). Винахід Альберті полягав в тому, щоб використовувати різні шифри (наприклад, алфавіти підстановки) для різних частин повідомлення. Йому також належить винахід того, що може вважатись першим шифрувальним приладом: колесо, що частково реалізовувало його винахід (див. Шифрувальний диск Альберті).

Новий час. В поліалфавітному шифрі Віженера, алгоритм шифрування використовує ключове слово, яке керує підстановкою літер в залежності від того, яка літера ключового слова використовується. В середині 1800-тих, Чарльз Беббідж показав, що поліалфавітні шифри цього типу залишились частово беззахисними перед частотним аналізом.

Початок 20-го століття. Декілька механічних шифрувально/дешифрувальних приладів було створено на початку 20-го століття і багато запатентовано, серед них роторні машини — найвідомішою серед них є Енігма, автомат, що використовувався Німеччиною з кінця 20-тих і до кінця Другої світової війни. Шифри, реалізовані прикладами покращених варіантів цих схем призвели до істотного підвищення криптоаналітичної складності після Другої світової війни.

Комп'ютерної ера. Поява цифрових комп'ютерів та електроніки після Другої світової війни зробило можливим появу складніших шифрів. Більше того, комп'ютери дозволяли шифрувати будь-які дані, які можна представити в комп'ютері у двійковому виді, на відміну від класичних шифрів, які розроблялись для шифрування письмових текстів. Це зробило непридатними для застосування лінгвістичні підходи в криптоаналізі. Багато комп'ютерних шифрів можна характеризувати за їхньою роботою з послідовностями бінарних бітів (інколи в блоках або групах), на відміну від класичних та механічних схем, які, зазвичай, працюють безпосередньо з літерами. Однак, комп'ютери також знайшли застосування у криптоаналізі, що, в певній мірі, компенсувало підвищення складності шифрів. Тим не менше, гарні сучасні шифри залишались попереду криптоаналізу; як правило, використання якісних шифрів дуже ефективне (тобто, швидке і вимагає небагато ресурсів), в той час як

злам цих шифрів потребує набагато більших зусиль ніж раніше, що робить криптоаналіз настільки неефективним та непрактичним, що злам стає практично неможливим.

Взагалі кажучи, до початку 20-го століття, криптографія, в основному, була пов'язанна з лінгвістичними схемами. Після того, як основний акцент було зміщено, зараз криптографія інтенсивно використовує математичний апарат, включно з теорією інформації, теорією обчислювальної складності, статистики, комбінаторики, абстрактної алгебри та теорії чисел. Криптографія є також відгалуженням інженерії, але не звичним, оскільки вона має справу з активним, розумним та винахідливим супротивником; більшість інших видів інженерних наук мають справу з нейтральними силами природи. Існують дослідження з приводу взаємозв'язків між криптографічними проблемами та квантовою фізикою.

Основні цілі захисту інформації, що визначають її безпеку:

1. Секретність або конфіденційність зберігання інформації в таємниці від всіх, окрім осіб, що мають на це право.

2. Цілісність даних забезпечення того, щоб інформація не змінювалася несанкціонованими або невідомими засобами.

3. Автентифікація об'єкту або ідентифікація підтвердження ідентичності об'єкту (наприклад, особи, комп'ютерного терміналу, кредитної картки і тому подібне).

4. Автентифікація повідомлення підтвердження джерела інформації;

5.Підпис засіб прив'язки інформації до об'єкту.

6. Авторизація передача іншому об'єкту офіційного дозволу виконувати що-небудь або бути ким-небудь.

7. Перевірка достовірності спосіб забезпечення своєчасності авторизації для використання інформації або ресурсів.

8. Контроль доступу дозвіл доступу до ресурсів тільки повноважним об'єктам.

9. Сертифікація підтвердження інформації довіреним об'єктом. 10. Часові мітки запис часу створення або існування інформації

11. Засвідчення перевірка створення або існування інформації об'єктом, відмінним від її творця. 12. Квитанція підтвердження прийому інформація.

13. Підтвердження підтвердження надання послуги.

14. Володіння надання об'єкту юридичного права використовувати або передавати ресурс іншим. 15. Анонімність утаєння ідентичності об'єкту, що бере участь в якому-небудь процесі.

16. Неспростовність запобігання відмові від попередніх угод або дій.

17. Відміна відміна сертифікації або авторизації.

Практичні напрями застосування криптографії:

1. Захист від несанкціонованого читання;
2. Захист від нав'язування помилкових повідомлень;
3. Ідентифікація законних користувачів;
4. Контроль цілісності інформації;
5. Автентифікація інформації;
6. Електронний цифровий підпис;
7. Системи таємного електронного голосування;
8. Електронне жеребкування;
9. Захист від відмови факту прийому повідомлень;
10. Одночасне підписання контракту;
11. Захист документів і цінних паперів від підробки.

Основні причини масового застосування механізмів криптографічного захисту інформації у теперішній час:

– бурхливий розвиток телекомунікаційних технологій;

– проникнення інформаційних (ІС) та інформаційно-телекомунікаційних систем (ІТС) у всі сфері суспільства;

– розвиток електронних банківських технологій;

– широке використання комп'ютерних мереж, зокрема, глобальної мережі Інтернет.

Методи криптографічного захисту інформації засновані на математичних перетвореннях інформації з використанням секретних параметрів – ключових даних.

Предметом криптології (kryptos – таємний, logos – наука) становлять: розробка подібних методів; проблеми синтезу відповідних (криптографічних) алгоритмів; їх аналіз і оцінка якості.

Об'єктами досліджень і розробок сучасної криптографії становлять:

• принципи побудови систем криптографічного захисту інформації;

• симетричні криптосистеми і криптосистеми з відкритим ключем;

• криптографічні алгоритми, що складають основу систем криптографічного захисту інформації, їх криптографічні властивості;

• криптографічні протоколи;

• системи розподілу ключів;

• геш-функції і алгоритми цифрового підпису;

• коди автентифікації повідомлень;

• підходи щодо вибору параметрів криптосистем, способи їх побудови і тестування;

• методика організації підсистем криптографічного захисту інформації в комп'ютерних системах і мережах.

Під час виконання цих досліджень і розробок керуються певними правилами, які були напрацьовані за час існування криптографії. Основне правило криптології **«правило Керкгоффса»**, сформульовано ще в XIX столітті голландським офіцером Керкхоффсом:

• під час криптоаналізу вважається, що система шифрування є відомою. Також Керкхоффсом висунуті 6 вимог до криптосистем:

• система повинна бути, якщо не теоретично, то практично невразливою;

• компрометація системи (попадання її до ворога) не повинне суттєво затрудняти її використання легальними кореспондентами;

• кореспонденти повинні мати можливість за потребою змінювати ключ;

• спосіб вибору та передачі ключа повинен бути легко здійсненим;

• можлива передача шифртексту загальнодоступними каналами зв'язку.

• криптографічна апаратура провина бути переносною;

• користування криптографічною апаратурою не повинне передбачати великої сукупності правил та розумового напруження.

Американський математик К.Шенон обґрунтував (в 50-х роках XX століття) наступні важливі принципи побудови шифрів:

• зашифроване повідомлення повинне читатися тільки за допомогою ключа;

• будь-який ключ з допустимої множини повинен забезпечувати надійний захист інформації;

• незначна зміна ключа повинна призводити до істотної зміни виду зашифрованого повідомлення;

• число операцій при розшифруванні інформації шляхом перебору всіх ключів, повинно перевищувати перспективні обчислювальні можливості, з урахуванням методів використання мережевих обчислень;

• не повинно бути простих і легко встановлюваних залежностей між ключами криптосистеми;

• число операцій, необхідних для визначення ключа з використанням шифрованого повідомлення і відповідного йому відкритого тексту, має бути не менше загального числа можливих ключів;

• структурні елементи алгоритму шифрування повинні бути незмінними.

Таблиця 1

Стандарти

Методи криптографічного захисту	**Використання**	**Стандарти міжнародні**	**Стандарти Україна**	**Стандарти Росія**
Симетричне шифрування	Захист конфіденційної інформації	IOS/IEC 18033-3 (AES)	ДСТУ 7624-2014 (Калина/Купина)	ГОСТ 28147-89
Асиметричне шифрування	Захист конфіденційної інформації/ Розподіл ключів	IOS/IEC 11166-2 1994 (RSA). PKCS#1	ДСТУ IOS/IEC 15946	ГОСТ Р 34.12-2012
Хешування	Захист цілісності/Автентифіккація	IOS/IEC 10118-3 2005	ДСТУ 7624-2014 (Калина/Купина)	ГОСТ Р 34.11-2012
Електронний цифровий підпис	Захист автентичності/достовірності	IOS/IEC 14888-3-2002	ДСТУ 4145-2002	ГОСТ Р 34.10-2012

DES — це симетричний алгоритм шифрування певних даних, стандарт шифрування прийнятий урядом СШАтіз 1976 до кінця 1990-х, з часом набув міжнародного застосування. Ще з часу свого розроблення алгоритм викликав неоднозначні відгуки. Оскільки DES містив засекречені елементи своєї структури, породжувались побоювання щодо можливості контролю з боку Національного Агентства Безпеки США .Алгоритм піддавався критиці за малу довжину ключа, що, врешті, після бурхливих обговорень та контролю академічної громадськості, не завадило йому стати загальноприйнятим стандартом. DES дав поштовх сучасним уявленням про блочні алгоритми шифрування та криптоаналіз.

Зараз DES вважається ненадійним в основному через малу довжину ключа (56 біт) та розмір блоку (64 біти).

DES є блочним шифром - дані шифруються блоками по 64 біти - 64 бітний блок явного тексту подається на вхід алгоритму, а 64-бітний блок шифрограми отримується в результаті роботи алгоритму. Крім того, як під час шифрування, так і під час дешифрування використовується один і той самий алгоритм (за винятком дещо іншого шляху утворення робочих ключів).

Ключ має довжину 56 біт (як правило, в джерельному вигляді ключ має довжину 64 біти, де кожний 8-й біт є бітом паритету, крім того, ці контрольні біти можуть бути винесені в останній байт ключа). Ключем може бути довільна 64-бітна комбінація, яка може бути змінена у будь-який момент часу. Частина цих комбінацій вважається слабкими ключами, оскільки може бути легко визначена. Безпечність алгоритму базується на безпечності ключа.

На найнижчому рівні алгоритм є ніщо інше, ніж поєднання двох базовних технік шифрування: перемішування і підстановки. Цикл алгоритму, з яких і складається DES є комбінацією цих технік, коли як об'єкти перемішування виступають біти тексту, ключа і блоків підстановок.

RSA (абревіатура від прізвищ Rivest, Shamir та Adleman) — криптографічний алгоритм з відкритим ключем, що базується на обчислювальній складності задачі факторизації великих цілих чисел.

RSA став першим алгоритмом такого типу, придатним і для шифрування, і для цифрового підпису.

Алгоритм RSA складається з 4 етапів: генерації ключів, шифрування, розшифрування та розповсюдження ключів.

Безпека алгоритму RSA побудована на принципі складності факторизації цілих чисел. Алгоритм використовує два ключі — відкритий (public) і секретний (private), разом відкритий і відповідний йому секретний ключі утворюють пари ключів (keypair). Відкритий ключ не потрібно зберігати в таємниці, він використовується для шифрування даних. Якщо повідомлення було зашифровано відкритим ключем, то розшифрувати його можна тільки відповідним секретним ключем.

Вимоги до криптосистем. Процес криптографічного закриття даних може здійснюватися як програмно, так і апаратно. Апаратна реалізація відрізняється істотно більшою вартістю, проте їй притаманні такі переваги: висока продуктивність, простота, захищеність і тощо. Програмна реалізація більш практична, допускає відому гнучкість у використанні.

Для сучасних криптографічних систем захисту інформації сформульовані наступні загальноприйняті вимоги:

• зашифроване повідомлення повинно піддаватися читанню тільки при наявності ключа;

• число операцій, необхідних для визначення використаного ключа шифрування за

фрагментом шифрованого повідомлення і відповідного йому відкритого тексту, має бути не менше загального числа можливих ключів;

• число операцій, необхідних для розшифрування інформації шляхом перебору різноманітних ключів повинно мати сувору нижню оцінку і не виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережевих обчислень);

• знання алгоритму шифрування не повинно впливати на надійність захисту;

• незначна зміна ключа повинно приводити до істотної зміни виду зашифрованого повідомлення навіть при використанні одного і того ж ключа;

• структурні елементи алгоритму шифрування повинні бути незмінними;

• додаткові біти, що вводяться в повідомлення в процесі шифрування, повинні бути повністю та надійно сховані в зашифрованому тексті;

• довжина шифрованого тексту повинна бути рівною довжині вихідного тексту;

• не повинно бути простих і легко встановлюваних залежністей між ключами, що послідовно використовуються в процесі шифрування;

• будь-якийключ з безлічі можливих повинен забезпечувати надійний захист інформації;

• алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна вести до якісного погіршення алгоритму шифрування.

Реалізація криптографічних методів. Проблема реалізації методів захисту інформації має два аспекти:

• розробку засобів, що реалізують криптографічні алгоритми;

• методику використання цих засобів.

Кожен з розглянутих криптографічних методів можуть бути реалізовані або програмним, або апаратним способом. Можливість програмної реалізації обумовлюється тим, що всі методи криптографічного перетворення формальні і можуть бути представлені у вигляді кінцевої алгоритмічної процедури. При апаратної реалізації всі процедури шифрування і дешифрування виконуються спеціальними електронними схемами. Найбільшого поширення набули модулі, що реалізують комбіновані методи. Більшість зарубіжних серійних засобів шифрування засноване на американському стандарті DES. Російські розробки, такі як, наприклад, пристрій КРИПТОН, використовує власний стандарт шифрування.

Основною перевагою програмних методів реалізації захисту є їх гнучкість, тобто можливість швидкої зміни алгоритмів шифрування. Основним же недоліком програмної реалізації є істотно менша швидкодія в порівнянні з апаратними засобами (приблизно в 10 разів). Останнім часом стали з'являтися комбіновані засоби шифрування, так звані програмноапаратні засоби. В цьому випадку в комп'ютері використовується своєрідний «криптографічний співпроцесор" - обчислювальний пристрій, орієнтований на виконання криптографічних операцій (додавання по модулю, зсув і т.д.). Міняючи програмне забезпечення для такого пристрою, можна вибирати той чи інший метод шифрування. Такий метод поєднує в собі переваги програмних і апаратних методів.

Таким чином, вибір типу реалізації криптозахисту для конкретної ІС в істотній мірі залежить від її особливостей і повинен спиратися на всебічний аналіз вимог, що пред'являються до системи захисту інформації.

Список використаних джерел

1. https://studfiles.net/preview/5462915/page:18/
2. https://uk.wikipedia.org/wiki/Data_Encryption_Standard#%D0%9E%D0%BF%D0%B8%D1%81_%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%D1%83
3. https://uk.wikipedia.org/wiki/Data_Encryption_Standard#%D0%A5%D1%80%D0%BE%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%8F
4. Сумаруков Г. В. Многообразие древнерусских тайнописей // Затаённое имя: Тайнопись в «Слове о полку Игореве». — М.: Изд-во МГУ, 1997.
5. Hakim, Joy (1995). A History of Us: War, Peace and all that Jazz. New York: Oxford University Press. ISBN 0-19-509514-6.