О. В. Гомонай. Криптографія. *Енциклопедія Сучасної України* (2014)
ISBN 966-02-2074-X

О. В. Гомонай

Криптографія

КРИПТОГРА́ФІЯ (від крипто... і ...графія) – мистецтво, наука та технологія забезпечення секретності інформації. Вивчає способи та методи захисту інформації від змін і неавторизов. втручання при передаванні, обробленні та зберіганні. Перший задокумент. криптогр. документ – єгипет. тексти з нестандарт. ієрогліфами – датують 1900 р. до н. е. Розквіт К. у Зх. Європі припадає на період пізнього середньовіччя, коли з'явилися перші праці-настанови про кодування та шифрування писем. документів. У Київ. Русі найдавніші приклади закодов. інформації виявлено у рукописах 12–13 ст.

Сучасна К. базується на матем. методах захисту інформації. Її завдання полягає в тому, щоб за допомогою матем. перетворень або алгоритмів перебудувати текст повідомлення (відкритий текст) у невпорядк. і позбавлену змісту (в ідеалі, абсолютно випадкову) послідовність символів, або шифртекст, який можна передавати відкритим каналом. Для відтворення відкритого тексту отримувач здійснює дешифрування – зворотне перетворення отриманого шифртексту. Алгоритм шифрування, як правило, вважається відкритим, тобто відомим усім. Секретність процедури забезпечують використанням т. зв. ключів – набору символів, які виступають параметрами матем. перетворень. Ключ застосовують і при шифруванні, і при дешифруванні повідомлення. Залежно від типу алгоритму шифрування ключі відправника та отримувача можуть бути взаємозалежними, корельованими (при симетр. шифруванні) та різними (при асиметр., тобто відкритому шифруванні). Сукупність алгоритмів шифрування, дешифрування та всіх можливих відкритих текстів, шифртекстів і ключів називають криптосистемою. К. тісно пов'язана з криптоаналізом – мистецтвом розшифрування, або «зламування», шифртексту.

Завданням практ. К. є не тільки розроблення криптосистеми, але й забезпечення її стійкості відносно «зламування». При цьому вважають, що зловмисник знає все, крім ключів, і має можливість порівнювати деякі шифртексти з їхніми оригіналами. Складність криптогр. задач саме й полягає в знаходженні таких алгоритмів і функцій, на яких ці алгоритми ґрунтуються, котрі, з одного боку, не дозволяють зловмиснику за прийнят. час підібрати ключі та розшифрувати всі повідомлення, а з іншого, надають можливість легітим. користувачам швидко та без втрат обмінюватися інформацією. Разом К. і криптоаналіз

утворюють криптологію (науку, що вивчає секретні системи для обміну інформацією в присутності третьої сторони). К. використовують не лише для приховування інформації, але й для забезпечення її аутентифікації та цілісності, неможливості відмови від авторства. Якщо у 20 ст. осн. замовниками та споживачами криптогр. методів були військові, то нині К. широко застосовують у комерц. структурах, банках, електрон. мережах тощо.

Слід відрізняти класичну К. від квантової криптографії. Надійність методів першої забезпечується матем. складністю алгоритмів, необхідних для дешифрування повідомлення за відсутності ключа, квант. К. базується на фіз. захищеності процесів передавання даних. В Україні дослідж. у галузі класич. К. займаються вчені Фіз.-тех. інституту Нац. тех. університету України «Київ. політех. інститут» (каф. матем. методів захисту інформації під керівництвом *М. Савчука*), факультету кібернетики Київ. університету (каф. матем. інформатики під керівництвом А. Анісімова), Інституту комп'ютер. інформ. технологій Нац. авіац. університету (*О. Юдін*). Існує також спец. істор. дисципліна, що вивчає шифрування і розшифровування записів за спец. технологіями з метою зробити їхній зміст зрозумілим тільки для обмеженого кола осіб. У істор. науці методи К. використовують при роботі з дипломат., воєн., торг.-фінанс., правовими, політ. документами. Вивчення графіч. документів передбачає розчленування зображення на найдрібніші групи символів і гіпотет. встановлення їхнього значення та зв'язків. Див. також Криптографічний захист інформації.

Рекомендована література

1. Жельников В. Криптография: от папируса до компьютера. Москва, 1996;
2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. Москва, 2002;
3. Ємець В. та ін. Сучасна криптографія: Основні поняття. Л., 2003.

Бібліографічний опис:

Криптографія / О. В. Гомонай// Енциклопедія Сучасної України [Електронний ресурс] / Редкол.: І. М. Дзюба, А. І. Жуковський, М. Г. Железняк [та ін.] ; НАН України, НТШ. – К. : Інститут енциклопедичних досліджень НАН України, 2014. – Режим доступу: https://esu.com.ua/article-1576