Основи криптографії

Одним з найбільш відомих способів захисту інформації є її кодування (шифрування, криптографія). Воно не рятує від фізичних впливів, але в решті випадків служить надійним засобом.

Криптографія – це прикладна наука, яка використовує найсучасніші досягнення фундаментальних наук і, в першу чергу, математики. З іншого боку, всі конкретні завдання криптографії істотно залежать від рівня розвитку техніки і технології, від застосовуваних засобів зв'язку і способів передавання інформації. Розвинулась дана наука з практичної потреби передавати важливі відомості найнадійнішим чином.

Криптографія (від грецького kryptos - прихований і graphein - писати) - наука про математичні методи забезпечення конфіденційності і автентичності інформації.

Криптографія займається методами перетворення інформації, які б не дозволили зловмиснику витягти її з повідомлень, що перехоплюються. При цьому по каналу зв'язку передається вже не сама інформація, що захищається, а результат її перетворення за допомогою шифру, і для зловмисника виникає складне завдання розкриття шифру.

Тобто, криптографія повинна забезпечити такий захист інформації, що навіть у випадку її перехоплення сторонніми особами й обробки будь-якими способами з використанням комп'ютерів і останніх досягнень науки і техніки вона не повинна бути дешифрована протягом декількох десятків років.

Вона вважається потужним засобом забезпечення конфіденційності і контролю цілісності інформації. Поки альтернативи методам криптографії немає

В криптографії застосовуються такі поняття:

Зашифрування – це процес перетворення інформації, при якому її зміст стає незрозумілим для суб'єктів, що не мають відповідних повноважень

Результат зашифрування інформації називають *шифротекстом* або *криптограмою*.

Розшифрування - процес перетворення зашифрованої інформації у придатну для читання інформацію.

Сукупність процесів зашифрування і розшифрування називають *шифруванням.*

Відкритий текст - початкове повідомлення, яке повинен захистити криптограф.

Кодування - заміна логічних (смислових) елементів, наприклад, слів.

Дія криптографії

Криптографічний алгоритм, або шифр, — це математична формула, що описує процеси шифрування і розшифрування. Щоб зашифрувати відкритий текст, криптоалгоритм працює в сполученні з ключем (секретним параметром) — словом, числом або фразою. Те саме повідомлення одним алгоритмом, але різними ключами буде перетворюватися в різний шифртекст. Ключ забезпечує конфіденційність шифротексту.

Знання ключа шифрування дозволяє виконати правильне розшифрування шифротексту.

Дешифрування (розкриття шифру) – процес одержання інформації із шифротексту без знання застосованого ключа.

Захищеність шифртекста цілком залежить від двох речей: стійкості криптоалгоритму і таємності ключа.

Стійкість (криптостійкість) - здатність шифру протистояти будь-яким атакам на нього (спробам розшифрувати перехоплене повідомлення, розкрити ключ шифру або порушити цілісність, достовірність інформації.

Стійкість конкретного шифру оцінюється тільки шляхом усіляких спроб його розкриття і залежить від кваліфікації криптоаналітиків, що атакують шифр.

Криптоалгоритм плюс усілякі ключі і протоколи, що приводять їх у дію, складають криптосистему. PGP — це криптосистема.

Криптологія – наука, що складається із двох галузей: криптографії і криптоаналізу.

Криптографія – наука про способи перетворення (шифрування) інформації з метою її захисту від незаконних користувачів.

Криптоаналіз – наука (і практика її застосування) про методи і способи розкриття шифрів.

Співвідношення криптографії й криптоаналізу очевидне: криптографія – це захист, тобто розробка шифрів, а криптоаналіз – це напад, тобто атака на шифри. Однак ці дві дисципліни пов'язані між собою – не буває гарних криптографів, що не володіють методами криптоаналізу.

«У світі розрізняють два типи криптографії: криптографія, що перешкодить вашій молодшій сестрі читати ваші файли, і криптографія, що перешкодить читати ваші файли урядам великих країн. Ми будемо розглядати криптографію другого типу.»

Криптографія може бути стійкою, а може бути і слабкою, як описано в приведеному прикладі. Криптографічна стійкість виміряється тим, скільки знадобиться часу і ресурсів, щоб із шифртекста відновити вихідний відкритий текст.

Криптографічні методи захисту інформації - це спеціальні методи шифрування, кодування або іншого перетворення інформації, в результаті якого її зміст стає недоступним без пред'явлення ключа криптограми і зворотного перетворення.

На практиці для шифрування інформації використовують *методи симетричного і асиметричного шифрування.*

Метод симетричного шифрування передбачає використання одного і того ж ключа, що зберігається у секреті, для за шифрування і для розшифрування даних.

В асиметричній криптографії для зашифровування даних використовується один ключ, а для розшифровування — інший ключ (звідси і назва — асиметричні). Чим більший ключ (число), тим найбільш захищений отриманий шифртекст. Отже, криптографічний метод захисту, безумовно, самий надійний метод захисту, так як охороняється безпосередньо сама інформація, а не доступ до неї (наприклад, зашифрований файл не можна прочитати навіть у випадку крадіжки носія). Даний метод захисту реалізується у вигляді програм або пакетів програм.

Домашнє завдання

Увага! ***Під час роботи з комп'ютером дотримуйтеся правил безпеки та санітарно-гігієнічних норм.*** (Інструктаж з правил техніки безпеки)

1) Перечитайте конспект
2) Дослідіть, що таке шифр Цезаря, зашифруйте будь який текст.
3) Виконайте інтерактивну вправу «Сучасні методи захисту інформації» https://learningapps.org/2897461
4) Перегляньте відео «Історія криптографії» https://youtu.be/IyYhBFu3vew
5) Підготуйте повідомлення про шифрувальну машину Енігма, шифрування RSA.
6) Дослідіть, як криптографія застосовується у криптовалюті.