КІБЕРБЕЗПЕКА ЗА ДОПОМОГОЮ ШИФРУВАННЯ З ВІДКРИТИМ КЛЮЧЕМ: ІЛЮСТРАЦІЯ

Германович С. С., ст. (гр. КВ-82мп, ФПМ КПІ ім. Ігоря Сікорського)

Анотація: Проблемою захисту інформації шляхом її перетворення займається криптологія. Криптологія розділяється на два напрямки: криптографію (пошук і дослідження математичних методів перетворення інформації) і криптоаналіз (дослідження можливості розшифровки інформації без знання ключів).

Ключові слова: криптографія, шифрування, блокчейн, криптовалюта, кібербезпеки.

Abstract: The problem of information security through its transformation is engaged in cryptology. Cryptology is divided into two areas: cryptography (search and study of mathematical methods of information conversion) and cryptanalysis (study of the possibility of decrypting information without knowing the keys).

Keywords: cryptography, encryption, blockade, cryptography, cyber security.

Історично першим завданням криптографії був захист переданих текстових повідомлень від несанкціонованого ознайомлення з їх змістом, що знайшло відображення в самій назві цієї дисципліни, цей захист базується на використанні "секретного мови", відомого тільки відправнику і одержувачу, всі методи шифрування є лише розвитком цієї філософської ідеї . З ускладненням інформаційних взаємодій в людському суспільстві виникли і продовжують виникати нові завдання по їх захисту.

Основними видами криптографічного закриття є шифрування і кодування даних. Сучасна криптографія включає в себе чотири великих розділи: симетричні криптосистеми і системи електронного підпису, системи управління ключами і криптосистеми з відкритими ключами. Криптографічні методи можна розбити на два класи:

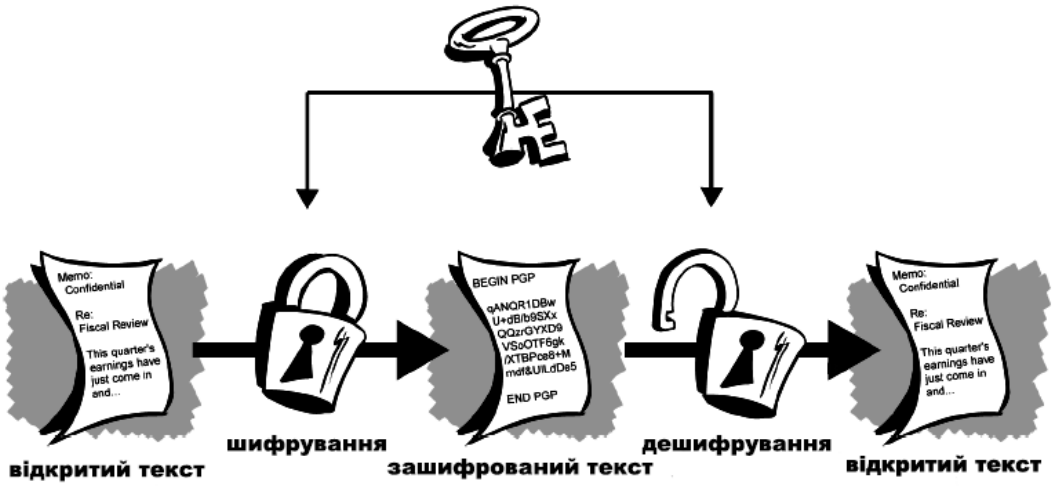
– обробка інформації шляхом заміни і переміщення букв, при якому обсяг даних не змінюється (шифрування);

– стиснення інформації за допомогою заміни окремих поєднань літер, слів або фраз (кодування).

Довгий час традиційна криптографія використовувала шифрування з таємним (симетричним) ключем - один і той же ключ використовувався як для зашифровування, так і для розшифровки (дешифрування) даних. Наочно це можна представити у вигляді замку, яким замикався скриню з таємним повідомленням. Пара однакових ключів до цього замку була як у відправника повідомлення (шифрувальника), так і у одержувача (дешифрувальників).

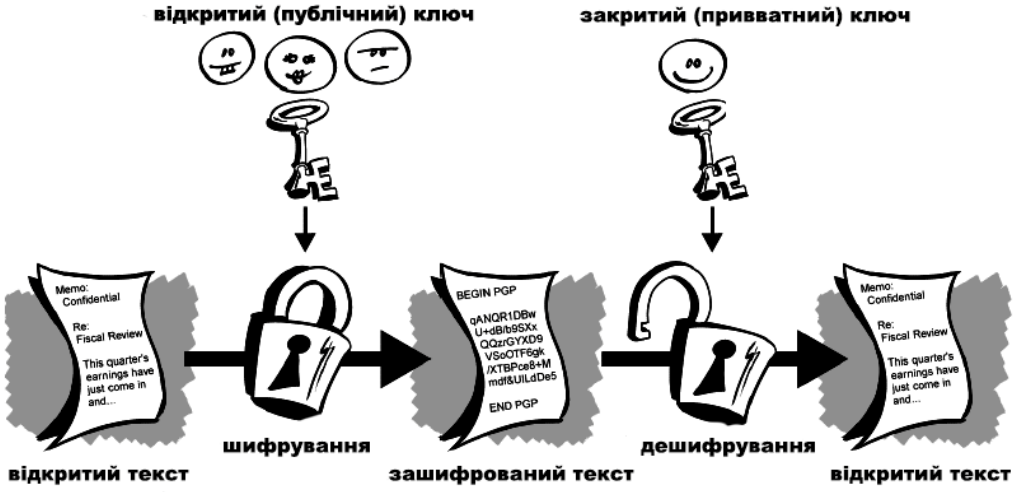
Насправді ніхто не відправляв повідомлення в замкнених скринях. Тексти, які треба було зашифрувати, особливим чином видозмінювалися з використанням таємного ключа (шифру) – послідовності символів, яка змішуючись з переданим повідомленням особливим чином (званим алгоритмом шифрування), приводила до отримання шифровки (шифротекста) –

повідомлення, яке неможливо було прочитати, що не знаючи алгоритму і шифру (ключа).



Але для наочності процесу, ми представимо, що наше повідомлення містилося в якийсь міцний скриню і закривалося надійним замком, однакові ключі від якого були у обох сторін – відправника і одержувача.

Цей ключ, яким зашифровувався і дешифрувати повідомлення, називався шифром або таємним симетричним ключем. Проблема була в тому, що при зміні ключа з метою безпеки, його необхідно було доставити одержувачу, який часто перебував далеко і на «ворожої» території. Передавати шифр відкритими каналами зв'язку було небезпечно. Довгий час проблема безпечної передачі нового шифру залишалася невирішеною. Як правило, для цього використовували таємних кур'єрів, що не гарантувало на 100% того, що ключ не потрапить до небажаних особам, які зможуть ним скористатися для дешифрування таємних повідомлень.



Проблема з ключами була вирішена тільки в 1975 році, коли була запропонована концепція шифрування з парою ключів: відкритим і відповідним йому – закритим. Ця асиметрична система шифрування отримала назву криптографії з відкритим ключем.

Працює ця система так:

– генерується випадковий секретний ключ і за певним алгоритмом підбирається до нього інший – відкритий ключ, при цьому, для будь-якого закритого ключа існує тільки один варіант відкритого. Тобто ці ключі (приватний і публічний) завжди працюють в парі;

– далі отриманий відкритий ключ пересилається по будь-яким відкритим каналам зв'язку відправнику таємного повідомлення;

– отримавши публічний ключ, відправник за допомогою нього зашифровує повідомлення і відправляє його одержувачу, у якого є відповідний приватний ключ;

– одержувач розшифровує секретне повідомлення, використовуючи свій приватний ключ з пари з публічним, яким було зашифровано повідомлення.

Слід зазначити, що відкритим (публічним) ключем можна тільки зашифрувати повідомлення, але розшифрувати його вже цим ключем не вийде. Для дешифрування потрібен тільки закритий (приватний) ключ з пари. Так працює алгоритм з асиметричним шифруванням.

Асиметрична криптографія з відкритим ключем набула широкого поширення, і не тільки в шифруванні шпигунських і дипломатичних послань. Асиметричну криптографію використовують сайти з підтримкою протоколу HTTPS, месенджери, wifi-роутери, банківські системи і багато іншого. На основі асиметричної криптографії базується електронний підпис. Також на асиметричної криптографії побудований алгоритм блокчейна, на якому, в свою чергу побудовані всі криптовалюта, включаючи біткоіни.

Криптографія – це найважливіша частина всіх інформаційних систем, що забезпечує підзвітність, прозорість, точність і конфіденційність. Вона запобігає спробам шахрайства в електронній комерції і забезпечує юридичну силу фінансових транзакцій. Криптографія допомагає встановити вашу особистість і забезпечує анонімність. Вона заважає хуліганам зламати сервер і не дозволяє конкурентам залізти в конфіденційні документи. А в майбутньому, у міру того як комерція і комунікації будуть все тісніше зв’язуватися з комп’ютерними мережами, криптографія стане життєво важливою.

Науковий керівник: Землянська О. В., ст. викл. (каф. ОППЦБ КПІ ім. Ігоря Сікорського)

Література

1. Алфьоров А. П. Основи криптографії: навч. посіб. / А. П. Алфьоров, А. Ю. Зубов, А. С. Кузьмін, А. В. Черьомушкін – М .: 2005. – 480 с.

2. Введення в криптографію / За заг. ред. В. В. Ященко – М., МЦНМО, 1998, 1999, 2000 – 272 с.

3. Панасенко С. П., Захист інформації в комп’ютерних мережах // Журнал «Світ ПК» 2002 року № 2.

4. Електронний ресурс: https://clck.ru/EYqNL.