Поняття криптосистеми з відкритим ключем.

Асиметричні криптосистеми — ефективні системи криптографічного захисту даних, які також називають криптосистемами з відкритим ключем. В таких системах для зашифровування даних використовують один ключ, а для розшифровування — інший (звідси і назва — асиметричні). Перший ключ є відкритим і може бути опублікованим для використання усіма користувачами системи, які шифрують дані. Розшифровування даних за допомогою відкритого ключа неможливе. Для розшифровування даних отримувач зашифрованої інформації використовує другий ключ, який є секретним (закритим). Зрозуміло, що ключ розшифровування не може бути визначеним з ключа зашифровування.

Головне досягнення шифрування з відкритим ключем в тому, що воно дозволяє людям, що не мають наперед наявної домовленості про безпеку, обмінюватися секретними повідомленнями. Необхідність відправникові й одержувачеві погоджувати таємний ключ по спеціальному захищеному каналу цілком відпала. Прикладами криптосистем з відкритим ключем є Схема Ель-Гамаля, RSA, Діффі-Геллмана і DSA.

Історія

Історія криптографії налічує близько 4 тисяч років. Як основний критерій періодизації криптографії можливо використовувати технологічні характеристики використовуваних методів шифрування.

Перший період (приблизно з третього тисячоліття до нашої ери) Характеризується пануванням моноалфавітних шифрів (основний принцип — заміна алфавіту вихідного тексту іншим алфавітом через заміну літер іншими літерами або символами).

Другий період (хронологічні рамки — з IX століття на Близькому Сході (Ал-Кінді) і з XV століття в Європі (Леон Баттіста Альберті) — до початку XX століття) ознаменувався введенням в обіг поліалфавітних шифрів (основний принцип полягає в тому, щоб замінити кожну літеру алфавіту на іншу літеру з іншого алфавіту, залежно від позиції літери у повідомленні)

Третій період (з початку і до середини XX століття) характеризується впровадженням електромеханічних пристроїв в роботу шифрувальників. При цьому продовжувалося використання поліалфавітних шифрів.

Початок асиметричним шифру було покладено в роботі «Нові напрямки в сучасній криптографії» Вітфілда Діффі та Мартіна Геллмана,

опублікованій в 1976 році. Перебуваючи під впливом роботи Ральфа Меркле про поширення відкритого ключа, вони запропонували метод отримання секретних ключів, використовуючи відкритий канал. Цей метод експоненціального обміну ключів, який став відомий як обмін ключами Діффі-Геллмана, був першим опублікованим практичним методом для встановлення поділу секретного ключа між завіреними користувачами каналу. У 2002 році Геллман запропонував називати даний алгоритм «Діффі — Геллмана — Меркле», визнаючи внесок Меркле в винахід криптографії з відкритим ключем. Ця ж схема була розроблена Малькольмом Вільямсоном в 1970-х, але трималася в секреті до 1997 року. Метод Меркле з розповсюдження відкритого ключа був винайдений в 1974 році і опублікований в 1978, його також називають загадкою Меркле.

Криптографія з відкритим ключем

Проблема керування ключами була вирішена криптографією з відкритим, або асиметричним, ключем, концепція якої була запропонована Уітфілдом Діффі і Мартіном Геллманом у 1975 році. Криптографія з відкритим ключем — асиметрична схема, яка застосовує пару ключів:

відкритий (public key) - він кодує дані;

закритий (private key) - використовується виключно для розшифровування повідомлень, що були закодовані відкритим ключем.

Користувач поширює тільки свій відкритий ключ. Проте закритий тримає в таємниці. Якщо хтось відправить Адресатові повідомлення, з яким має ознайомитись тільки він, то відправник шифрує своє повідомлення відкритими ключем Адресата. Після чого відправляє зашифроване повідомлення будь-яким способом Адресатові. Прочитати зашифроване повідомлення неможливо. Його треба спочатку розшифрувати. Це можливо тільки закритим ключем, який є тільки у Адресата. Звідси, якщо хтось отримує повідомлення, прочитати його не зможе. Адресат, отримавши повідомлення, розшифровує його приватним ключем, який є тільки в нього. Хоча, пара ключів математично пов'язана, вираховування закритого ключа з відкритого достатньо трудомістке, в практичному плані займає занадто великий час, який робить витрати необґрунтованими.

Шифрування з відкритим ключем стала технологічною революцією, що зробила стійку криптографію доступною.

Ідея створення

Ідея криптографії з відкритим ключем дуже тісно пов'язана з ідеєю односторонніх функцій, тобто таких функцій f(x), що за відомим x досить просто знайти значення f (x), тоді як визначення x з f (x) складно в сенсі теорії.

Але сама одностороння функція марна в застосуванні: нею можна зашифрувати повідомлення, але розшифрувати не можна. Тому криптографія з відкритим ключем використовує односторонні функції з лазівкою. Лазівка — це якийсь секрет, який допомагає розшифрувати. Тобто існує такий y, що знаючи f (x), можна обчислити x.

Поняття однобічної функції із секретом (лазівкою) стало вихідним для асиметричної криптографії. Той факт, що для обчислення самої функції з поліноміальною складністю й для її інвертування потрібно різна вихідна інформація (тобто наявність певної асиметрії), і дав назву новому напрямку в криптографії.

Схема шифрування з асиметричним ключем