# Тема 8. Шифрування та електронно-цифровий підпис

***Шифрування*** – це спосіб зміни повідомлення або іншого документа, що забезпечує спотворення (приховування) його вмісту.

***Кодування*** – це перетворення звичайного, зрозумілого, тексту в код. При цьому мається на увазі, що існує взаємно однозначна відповідність між символами тексту (даних, чисел, слів) і символьного коду – **в цьому принципова відмінність кодування від шифрування.** Часто кодування і шифрування вважають одним і тим же, забуваючи про те, що для відновлення закодованого повідомлення, достатньо знати правило підстановки (заміни). Для відновлення ж зашифрованого повідомлення крім знання правил шифрування, потрібно і ключ до шифру. Ключ – конкретний секретний стан параметрів алгоритмів шифрування і дешифрування. Знання ключа дає можливість прочитання секретного повідомлення.

Шифрувати можна не тільки текст, але і різні комп’ютерні файли – від файлів баз даних і текстових процесорів до файлів зображень.

Зазвичай алгоритми шифрування відомі і не є секретом. Конфіденційність передачі і зберігання зашифрованої інформації забезпечується за рахунок конфіденційності ключа. Ступінь захищеності залежить від алгоритму шифрування і від довжини ключа, вимірюваної в бітах. Чим довший ключ, тим краще захист, але тим більше обчислень треба провести для шифрування і дешифрування даних.

Більшість з нас постійно використовують шифрування, хоча і не завжди знають про це. Якщо у вас встановлена операційна система Microsoft, то знайте, що Windows зберігає про вас (як мінімум) таку секретну інформацію:

* паролі для доступу до мережевих ресурсів (домен, принтер, комп’ютери в мережі);
* паролі для доступу в Інтернет за допомогою DialUр;
* кеш паролів (в браузері є така функція – кешувати паролі, і Windows зберігає всі коли-небудь вводяться вами в Інтернеті паролі);
* сертифікати для доступу до мережевих ресурсів і зашифрованих даних на самому комп’ютері.

Ці дані зберігаються або в рwl-файлі (в Windows 95), або в SAM-файлі (в Windows NT/2000/XР). Це файл Реєстру Windows, і тому операційна система нікому не дасть до нього доступу навіть на читання. Зловмисник може скопіювати такі файли, тільки завантажившись в іншу ОС або з дискети. Утиліт для їх злому досить багато, найсучасніші з них здатні підібрати ключ за кілька годин.

# Основні види алгоритмів шифрування – симетричні і асиметричні.

Симетричні методи шифрування зручні тим, що для забезпечення високого рівня безпеки передачі даних не потрібно створення ключів великої довжини. Це дозволяє швидко шифрувати і дешифрувати великі обсяги інформації. Разом з тим, і відправник, і одержувач інформації володіють одним і тим же ключем, що робить неможливим аутентифікацію відправника. Крім того, для початку роботи із застосуванням симетричного алгоритму сторонам необхідно безпечно обмінятися секретним ключем, що легко зробити при особистій зустрічі, але вельми скрутно при необхідності передати ключ через будь-які засоби зв’язку.

Приклади алгоритмів симетричного шифрування:

* DES (Data Encryption Standard). Розроблений фірмою IBM і широко використовується з 1977 року. В даний час трохи застарів, оскільки застосовувана в ньому довжина ключа недостатня для забезпечення стійкості до розтину методом повного перебору всіх можливих значень ключа;
* Triple DES. Це удосконалений варіант DES, що застосовує для шифрування алгоритм DES три рази з різними ключами. Він значно стійкіший до злому, ніж DES;
* Rijndael. Алгоритм розроблений в Бельгії. Працює з ключами довжиною 128, 192 і 256 біт. На даний момент до нього немає претензій у фахівців з криптографії;
* Skipjack. Алгоритм створений і використовується Агентством національної безпеки США. Довжина ключа 80 біт. Шифрування й дешифрування інформації проводиться циклічно (32 циклу);
* IDEA. Алгоритм запатентований в США і низці європейських країн. Власник патенту компанія Ascom-Tech. Алгоритм використовує циклічну обробку інформації (8 циклів) шляхом застосування до неї ряду математичних операцій. RC4. Алгоритм спеціально розроблений для швидкого шифрування великих об’ємів інформації. Він використовує ключ змінної довжини (в залежності від необхідного ступеня захисту інформації) і працює значно швидше інших алгоритмів. RC4 відноситься до так званих потоковим шифрів.

При асиметричному шифруванні використовуються два ключі – відкритий і закритий, які математично пов’язані один з одним. Інформація шифрується за допомогою відкритого ключа, що доступний усім бажаючим, а розшифровується за допомогою закритого ключа, відомого тільки одержувачу повідомлення.

Електронний цифровий підпис (ЕЦП) є електронним еквівалентом власноручного підпису. ЕЦП служить не тільки для аутентифікації відправника повідомлення, але і для перевірки його цілісності. При використанні ЕЦП для аутентифікації відправника повідомлення застосовуються відкритий і закритий ключі. Процедура схожа на здійснювану в асиметричному шифруванні, але в даному випадку закритий ключ служить для шифрування, а відкритий – для дешифрування.

Хакери, крекери, кардери – хто це?

***Хакер*** (анг. hacker) – комп’ютерний фахівець, який займається активним і глибоким дослідженням, розвитком та вдосконаленням різних комп’ютерних систем; його цікавить, як працюють системи, і це не продиктовано особистою вигодою. В даний час більшість хакерів пов’язані з розвитком вільного програмного забезпечення.

Слово «Хакер» використовують в невірному контексті в ЗМІ, що спричиняє підміну понять. Програмісти, які беруть участь у руйнуванні системи, крадіжці паролів і іншої злочинної діяльності, називаються ***крекери*** (англ. crack – зломщик). Одна з відмінних особливостей крекерів – вони зберігають свої

«позиції». При зломі вони ретельно замітають сліди, але в той же час залишають собі можливість знову зайти в систему (наприклад, створюють обліковий запис).

Типи хакерів:

* ***крекери*** або кримінальні хакери (чорний капелюх). Якщо крекери зламують комп’ютерну систему, значить у них підступні плани. Їх цікавить особиста вигода: популярність, прибуток і навіть помста. Вони змінюють, видаляють і крадуть важливу інформацію і часто роблять цим життя інших людей жахливим. Крекери, безсумнівно, злочинці і вони повинні бути покарані відповідно до закону;
* етичні хакери (білий капелюх). Етичні хакери проникають в свої системи для того, щоб переконатися в їх безпеці і роблять це тими ж методами, які міг би використовувати кримінальний хакер. Завдяки їх діяльності поліпшується добробут звичайного комп’ютерного користувача. Коли хакер знаходить в сервері вразливе місце, він повідомляє про це власника сервера. У крайніх випадках деякі всесвітньо відомі компанії навіть наймали хакерів на роботу або влаштовували змагання хакерів, для контролю безпеки своїх систем;
* є також і хакери «сірі капелюхи», які можуть бути і тими, і іншими.

***Кардер –*** це людина, що проводить незаконні операції з кредитними картками інших осіб для використання грошей, знятих з картки, в особистих цілях.

Існує два види кардерів: інтернет-кардери, які працюють тільки з інформацією, і реальні кардери, які працюють з пластиковими клонами кредитних карт.