СУЧАСНІ МЕТОДИ ШИФРУВАННЯ ІНФОРМАЦІЇ

Лук'янихін О.В., *студент*; СумДУ, гр. ПМ-41

Чільне місце серед всього різноманіття засобів попередження несанкціонованого доступу до захищеної інформації посідають криптографічні методи, оскільки вони ґрунтуються на властивостях інформації і не мають слабкостей, що виникають при використанні особливостей вузлів її обробки,середовища передачі, адміністративних засобів і т.д.

Криптографія - це наука, що вивчає математичні методи забезпечення автентичності і конфіденційності даних. Для сучасного етапу її розвитку характерним є використання алгоритмів, що припускають реалізацію за допомогою обчислювальних засобів. Основними вимогами до сучасних методів криптографічного захисту є: конфіденційність, цілісність і невідслідковність.

Згідно законодавства України: "Криптографічний захист інформації – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо" [1].

В сучасній криптографії практичне значення мають лише методи захисту з використанням ключа. Їх поділяють на два види: симетричні (інша назва - алгоритми з секретним ключем) та асиметричні (алгоритми з відкритим ключем).

Симетричні системи шифрування базуються на одному ключі,що використовується і для шифрування, і для дешифрування (або ключ дешифрування можливо обчислити за ключем шифрування).

Їх перевагами є:

1. Велика пропускна здатність.
2. Відносно короткі ключі.
3. Їх можна використати як основу для створення різних криптографічних механізмів (псевдовипадкові генератори чисел, хеш-функції, обчислювально-ефективні схеми підпису та ін.)
4. Можливість їх комбінування для підвищення криптостійкості.

Недоліки симетричних систем:

1. Складність збереження конфіденційності ключа.

2. Велика кількість ключів, що використовуються, у великій мережі.
3. Необхідність частої зміни ключів.

Асиметричні шифри використовують два ключі. Перший – відкритий – застосовується для шифрування інформації і може знаходитися у відкритому доступі. В той час як закритий ключ, що використовується для дешифрування, зберігається в таємниці [2]. Причому ключ для дешифрування неможливо обчислити за ключем шифрування.

Переваги асиметричних алгоритмів:

1. Відсутня необхідність передачі єдиного секретного ключа усім користувачам системи.
2. В асиметричній криптосистемі тільки один секретний ключ.
3. Можливість не змінювати ключі значний час.
4. У великих мережах менша кількість необхідних ключів.

Їх недоліки:

1. Складність корегування алгоритмів.
2. Більш довгі ключі для забезпечення тієї ж криптостійкості.
3. Вимагають значно більшої обчислювальної потужності.

При практичному застосуванні ці два підходи часто поєднуються. Це надає змогу збалансувати переваги і недоліки обох методів.

З появою Інтернету й значною інформатизацією нашого суспільства використання криптографії перейшло на новий рівень і перестало бути прерогативою великих корпорацій і державних служб. Криптографічні методи стали широко використовуватися приватними особами в електронних комерційних операціях, телекомунікаціях та багатьох інших середовищах.

Отже, в найближчому майбутньому криптографія, як наука про методи захисту інформації, не втратить актуальності, а криптографічні алгоритми будуть основою відповідного програмного забезпечення.

Керівник: Козлова І.І.

Література

1. Указ Президента України від 22 травня 1998 року N 505/98 «Про Положення про порядок здійснення криптографічного захисту інформації в Україні».
2. Whitfield Diffie and Martin Hellman, «Multi-user cryptographic techniques» [Diffie and Hellman, AFIPS Proceedings 45,1976].