Мінгальова Юлія
студентка V курсу, спеціальність «Інформатика»
Науковий керівник – ***Спірін О. М.****,*
доктор педагогічних наук, доцент

КЛАСИФІКАЦІЯ МЕТОДІВ ШИФРУВАННЯ

З розвитком новітніх технологій, виникненням сучасних інформаційних мереж та впровадженням в більшість сфер суспільного життя досягнень науково-технічного прогресу постала проблема захисту даних та комп'ютерних мереж від несанкціонованого доступу. Бурхливе зростання комунікаційних та обчислювальних технологій викликає збільшення числа вузлів мереж і кількості різних ліній зв'язку між ними, що підвищує ризик несанкціонованого підключення до мережі та доступу до конфіденційних відомостей користувача.

Метою даної статті є класифікація криптографічних алгоритмів.

За особливостями алгоритму шифрування криптосистеми загального використання можна розділити на наступні види (рис.1).

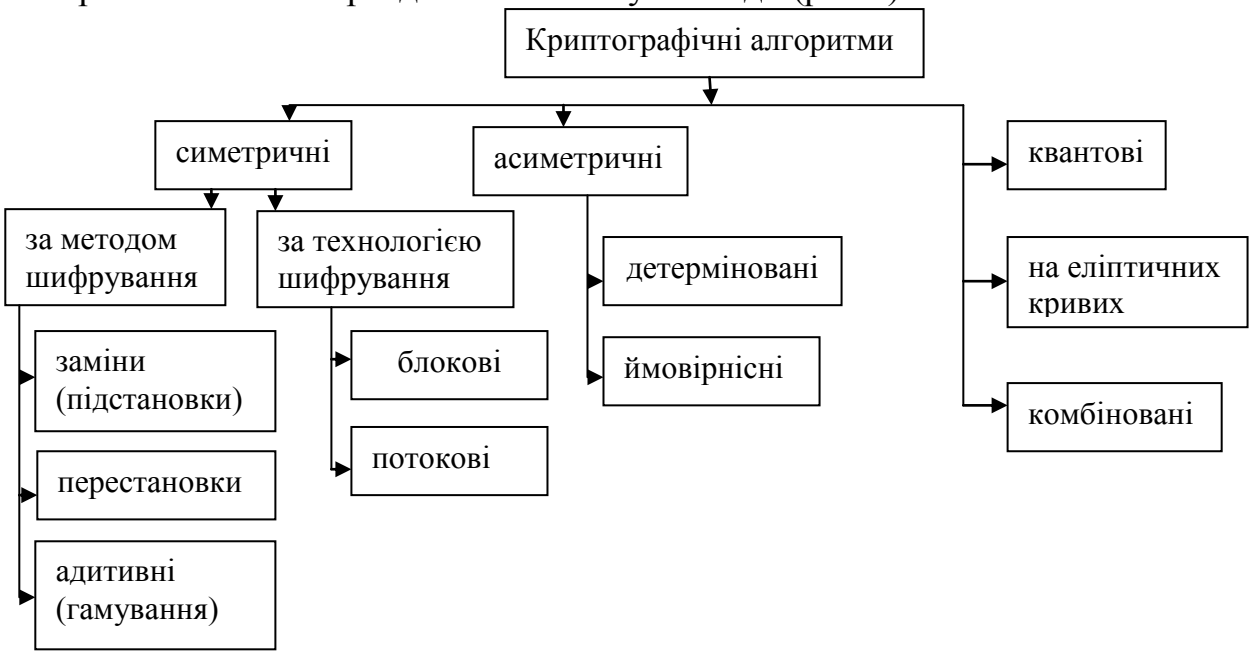

Рис.1. Класифікація криптографічних алгоритмів

Найперші шифри були симетричними, у яких для шифрування та дешифрування використовується один і той же ключ. Функція даного класу шифрування - це забезпечення конфіденційності даних від несанкціонованого доступу [3, с.247].

За методом шифрування до класу симетричних алгоритмів відносять шифри перестановки, гамування та заміни. У шифрах перестановки всі букви відкритого тексту залишаються в зашифрованому повідомленні, але змінюють

свої позиції. У шифрах заміни навпаки, позиції букв у шифровці залишаються тими ж, що й у відкритому тексті, але символи відкритого тексту замінюються символами іншого алфавіту. Прикладами шифрів простої заміни можуть служити такі шифри як шифр Цезаря, афінний шифр, шифр Атбаш. В адитивних шифрах літери алфавіту заміняються числами, до яких потім додаються числа секретної випадкової (псевдовипадковою) числової послідовності (гами). Склад гами змінюється в залежності від використовуваного ключа [3, с. 247-265].

Симетричні алгоритми за технологією шифрування підрозділяється на блоковий та потоковий клас шифрів. У потокових шифри перетворення виконуються окремо над кожним символом вихідного повідомлення. Для блокових шифрів відомості розбиваються на блоки фіксованої довжини, кожен з яких зашифровується і дешифрується окремо [2, с. 12-25].

У асиметричних системах для шифрування та дешифрування використовується два абсолютно різних ключа. Функціональність цієї класифікації шифрів надзвичайно широка від конфіденційності до цифрового підпису та підтвердження автентичності інформації. При використанні детермінованого алгоритму шифрування і розшифрування за допомогою відповідної пари ключів можливо тільки єдиним способом. Імовірнісний алгоритм при шифруванні одного і того ж вихідного повідомлення з одним і тим же ключем може давати різні шифротексти, які при дешифруванні будуть мати однаковий результат [3, с. 290].

В основі криптографічного алгоритму на еліптичних кривих (Elliptic Curve Cryptography) лежить той факт, що для рівняння a * x = b відносно x при відомих a й b та за умови, що a, b, x належать еліптичної кривої E, не відомо іншого алгоритму рішення, крім перебору всіх можливих значень x. Більш того, в силу складності самої конструкції еліптичних кривих навіть такий простий спосіб її вирішення, як повний перебір, важко оцінити з обчислювальної точки зору [4, с. 128].

Квантова криптографія вносить в процес шифрування природну невизначеність квантового світу. Процес відправки та прийому інформації виконується за допомогою об'єктів квантової механіки, наприклад, за допомогою електронів в електричному струмі, або фотонів у лініях волоконно-оптичного зв'язку [1, с. 98].

Комбіновані методи передбачають використання для шифрування повідомлення відразу декількох методів (наприклад, спочатку заміна символів, а потім їх перестановка) [3, с. 327].

Отже, за представленою класифікацією до криптографічних алгоритмів належать: симетричні, асиметричні, комбіновані, квантові та криптографічні системи на еліптичних кривих. Останнім часом велика увага приділяється квантовим алгоритмам та криптографічним системам на еліптичних кривих, завдяки тому, що вони мають найбільшу крипкостійкість.

Література

1. Брассар Ж. Современная криптология / Ж. Брассар [пер. с англ.] – М.: Издательско-полиграфическая фирма ПОЛИМЕД, 1999. – 176 с., илл.

2. Зензин О.С. Стандарт криптографической защиты –AES. Конечные поля / О.С Зензин, М.А. Иванов. – М. : КУДИЦ-ОБРАЗ, 2002.- 176с. – (СКБ- специалисту по компютерной безопасности)

3. Мао Венбо. Современная криптография: теория и практика/ Мао Венбо; [пер. с англ]. – М. : Издательский дом "Вильямс", 2005. – 768с. : ил. – Парал. тит. англ.

4. Рябко Б.Я. Криптографические методы защиты информации: Учебное пособие [для вузов]/ Б.Я. Рябко, А.Н. Фионов. – М.: Горячая линия – Телеком, 2005. – 209 с., ил.