Добрий день вельмишановні пані та панове, журі та конкурсанти. Мене звати Попович Ярослав, я навчаюсь в 10 класі, та написав наукову роботу на тему «Розробка системи шифрування повідомлень великих розмірів».

Шифрування використовується людьми повседенно. Починаючи з авторизації на сайті або відсилання повідомлень, закінчуючи воєнними справами.

Ціль моєї роботи розробити власний алгоритм шифрування, та порівняти його роботу із вже відомими представниками різних типів шифрування на прикладі консольного чату, що має потребувати низькі вимоги до комп’ютера.

Почнемо з табличних шифрів. Один із найвідоміших представників табличних шифрів – Шифр Віженера. Працює він наступним чином. Він формує квадратну таблицю довжини кількості символів в алфавіті. В перший рядок записує алфавіт, можливо перемішаний, а кожен наступний рядок – це циклічний зсув минулого праворуч, де останній символ іде у початок. Після чого записує ключ циклічно, доки його довжина не буде дорівнювати довжині тексту. Після чого і-й символ шифротексту дорівнює символу на перетині і-го символу в тексті та ключі у таблиці. Для дешифрування потрібно у стовбці із i-м символом ключа знайти i-й символ шифротексту, тож i-м символом повідомлення буде перший символ у рядку, який містить i-й символ шифротексту.

Цей шифр працює за лінійний час, але має величезний недолік – існує метод по взлому цього алгоритму.

Представником потокових шифрів я обрав шифр Вєрнама. Для цього шифру доведена його абсолютна криптостійкість. Але в нього також є недолік, із-за якого його використовувати майже неможливо. Він присвоює різні числа в двійковому записі для кожного символу алфавіту, після чого формує випадкові числа, кількість яких дорівнює довжині тексту, і додає їх за модулем 2. Недоліком цього шифру є той факт, що для кожного повідомлення потрібні нові випадкові числа обом сторонам.

Серед блочних шифрів я обрав шифр DES. Працює цей шифр наступним чином – спочатку він робить початкову перестановку згідно із таблицею. Після цього алгоритм 16 разів повторює наступну операцію: ділить блок на 2 рівні частини по біти, бере праву частину, та пропускає її через функцію подаючи на вхід ключ розміром 48 біт, після чого лівий блок ксориться із тим, що вийшло з функції, після чого правий блок ставиться без змін на позицію лівого, а лівий (проксорений) опиняється на позиції правого блоку. Але на останній з ітерацій ліва та праві частини не міняються містами. Після чого йде перестановка, яка схожа на ту, що була на початку роботи алгоритму. Те як формуються ключі та працює функція *f* написано в роботі, тому не будемо на цьому зупинятись.

Розроблений шифр поєднує в собі ідею блочних шифрів та табличних. Через це розроблений алгоритм буде стійкий до атак методом Касіскі, та до атак по масці. Спочатку записуються всі символи алфавіту, в якомусь порядку. Далі формується квадрат Віженера. Алгоритм приймає на вхід відкритий текст, ключ та кількість проходів по тексту. Також можна встановити довжину шифротексту та довжину блоку, але на асимптотику це ніяк не впливає. Після цього текст розбивається на блоки довжини ключа, та кожен блок шифрується використовуючи шифр Віженера та вектор ініціалізації, як ключ до нього.

Вектором ініціалізації для першого блоку буде ключ (довжини блока), а для всіх інших блоків вектором ініціалізації буде шифротекст, який вийшов із минулого блоку. Це зроблено для того, щоб домогтись лавинного ефекту, та при зміні будь-якого символу весь шифротекст змінювався. Коли алгоритм дійде до останнього блоку, він присвоїть вектору ініціалізації шифротекст, отриманий з останнього блоку, та буде використовувати його у наступному проході для першого блоку. Так буде повторюватись разів. Для дешифрування потрібно повторити всі дії з кінця.

Як вже було сказано – шифр Віженеру працює за лінійний час, можете побачити час його роботи на тестах різного розміру.

Шифр DES працює за квадратний час, більш детально це описано в роботі.

Асимптотика роботи шифру Вєрнама дорівнює О(nk), де n – довжина тексту, а k – час або кількість ітерацій необхідних для генерації випадкових чисел.

Перейдемо до висновку. Так як ці шифри зозглядались на прикладі чату використовувати шифр Вєрнама неможливо, бо потрібно буде передавати випадкові числа по захищеному каналу зв’язку, але тоді шифрування взагалі не потрібно, якщо є захищений канал. Якщо порівнювати шифр Вєрнама із двома шифрами, що залишились, то він буде програвати їм в криптостійкості. Для повідомлень невеликого розміру, не більше 10^4 символів, можна використовувати як шифр DES, так і мій шифр, бо на рядках такого розміру, різниця в часі буде майже непомітною. Натомість на великих рядках шифр DES буде працювати довго, а так як шфвидкість роботи мого шифру можна регулювати, то мій шифр буде працювати за лінійний час, тому на рядках великого розміру краще використовувати саме його.