ХАРКІВСЬКЕ ТЕРИТОРІАЛЬНЕ ВІДДІЛЕННЯ МАН УКРАЇНИ

Розробка системи шифрування в хмарних сховищах даних

Попович Ярослав Васильович, учень 11 класу Харківського Навчально-виховного комплексу №45 «Академічна гімназія» Харківської міської ради Харківської області

Науковий керівник: Руккас Кирило Маркович, професор кафедри теоретичної та прикладної інформатики механіко-математичного факультету Харківського національного університету імені В.Н. Каразіна, доктор технічних наук, доцент

Мета дослідження – підвищення ефективності шифрування повідомлень великого розміру в хмарних сховищах даних.

Завдання - аналіз існуючих алгоритмів шифрування; розробка нового алгоритму, який поєднує в собі переваги блочних і табличних шифрів; аналіз роботи існуючих та розробленого шифру за часом та криптостійкістю; тестування нового алгоритму; розробка системи шифрування; створення чату; створення програми; застосування системи шифрування в створених чаті та програмі для шифрування даних на гугл диску.

Методи дослідження: вивчення досвіду фахівців, аналіз та порівняння.

Об'єкт дослідження - процес швидкого шифрування даних великого розміру.

Предмет дослідження - математичні моделі та методи швидкого шифрування повідомлень великого розміру.

Результати - вивчення та аналіз існуючих алгоритмів шифрування; написаний власний алгоритм та система шифрування даних; проведений порівняльний аналіз розробленого алгоритму із вже відомимими; проведений криптоаналіз розробленого алгоритму; розроблений прототип чату та програма для шифрування та передачі даних на хмарні сховища в реальному часі; проведене тестування розробленої системи шифрування на прикладі написаних чату та сайту-програми

Висновки - для зберігання файлів великого розміру на хмарних сховищах даних краще всього себе продемонстрував саме розроблений шифр, через можливість керування часом роботи алгоритму і його криптостійкістю. Даний алгоритм має більш надійну криптостійкість порівняно з шифром Віженера, не потребує генерації великої кількості випадкових чисел, як шифр Вєрнама, та працює набагато швидше за шифр DES.

Алгоритм шифрування

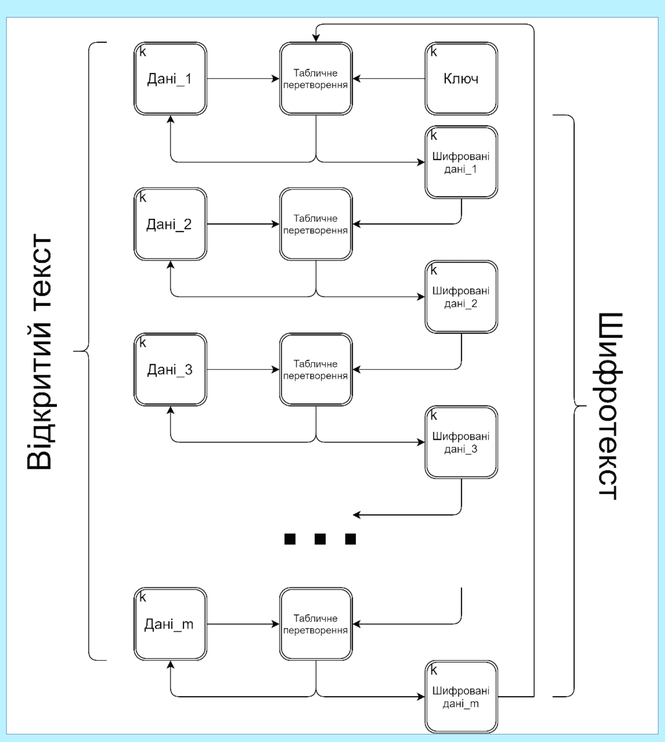

Рис 1 Блок-схема роботи алгоритму

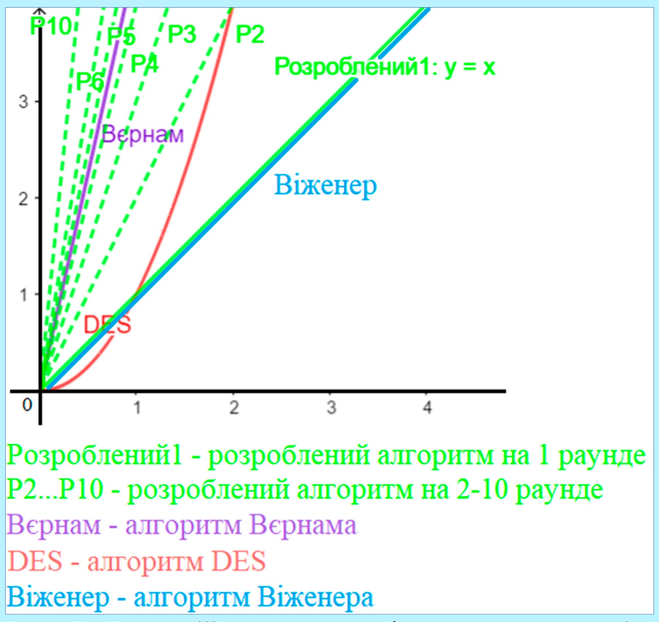

Рис 2 Залежнійсть часу роботи алгоритму від кількості раундів та часу роботи

Шифри	Час роботи	Особливості
Шифр Віженера	$O(n)$	Піддається дешифруванню
Шифр Вєрнама	$O(nk)$	Доведена абсолютна криптостійкість Для роботи потрібно згенерувати випадкові числа
Шифр DES	$O(n^2)$	Можливість підбору ключа
Розроблений шифр	$O(nc)$	Час роботи залежить від кількості раундів Криптостійкий до атак методом Касіскі

	1 прохід	10 проходів	100 проходів
1000 символів	0,0009973 с	0,00498 с	0,0428 с
10000 символів	0,0079779 с	0,04985 с	0,4363 с
100000 символів	0,0797855 с	0,48044 с	4,4514 с
1000000 символів	0,7979397 с	4,96143 с	48,784 с

Рис 3 Порівняльний аналіз роботи алгоритмів

Ідеальне відношення:

$$P_{i_1} \otimes P_{i_2} \otimes P_{i_3} \otimes \ldots \otimes P_{i_a} \otimes C_{j_1} \otimes C_{j_2} \otimes C_{j_3} \otimes \ldots \otimes C_{j_s} = K_{k_1} \otimes K_{k_2} \otimes K_{k_3} \ldots \otimes K_{k_c}$$

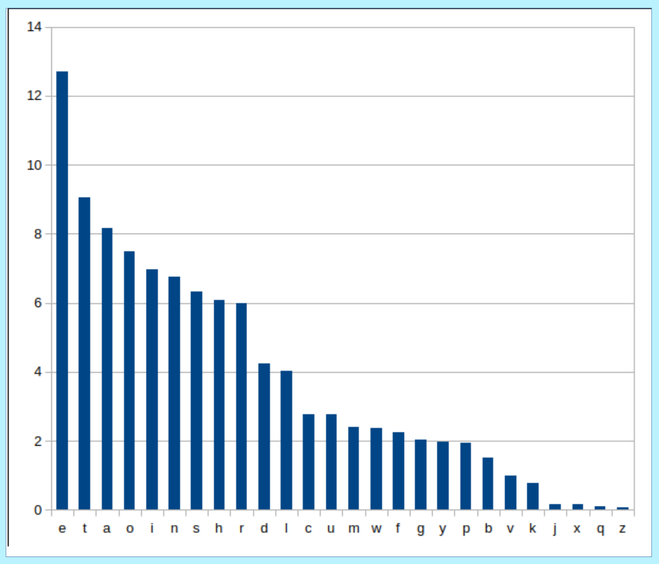

Рис 4 Частота появи символів у тексті (за %)

Прототипи програм

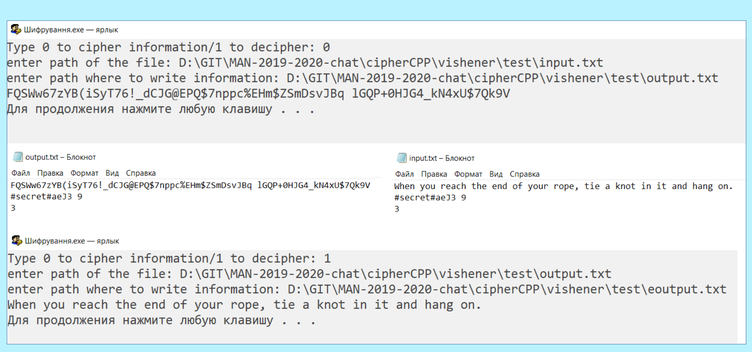

Рис 5 Робота шифру на трьох раундах

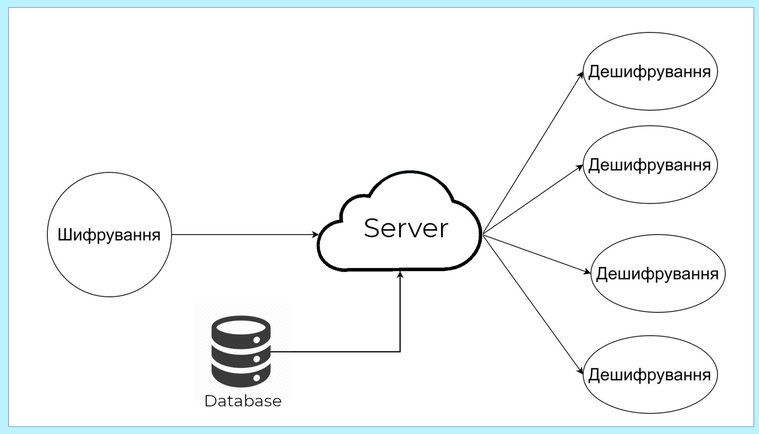

Рис 6 Серверна частина чату

Open text	Passphrase	Rounds	Cipher text
Hello, my name is Sam. login - admin, password - admin	secret pass	100	VcPkh.f8A3O&#4GU-4 # y . q g 6 H 1 + Z H4*&VoUv6lPHSV%*8-sqQt%e&URg

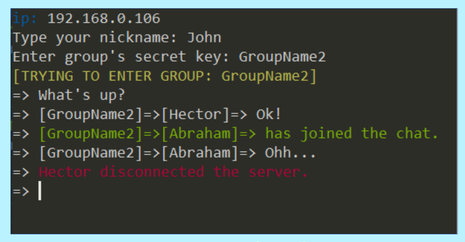

Рис 7 Чат-програма з трьох клієнтів, що створили дві групи для обміну повідомленнями

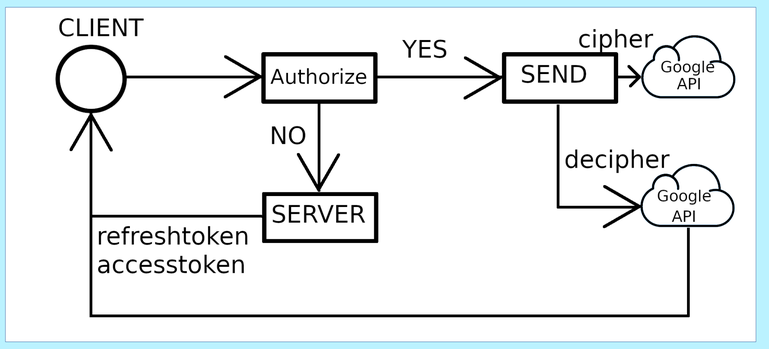

Рис 8 Схема роботи сайту-програми

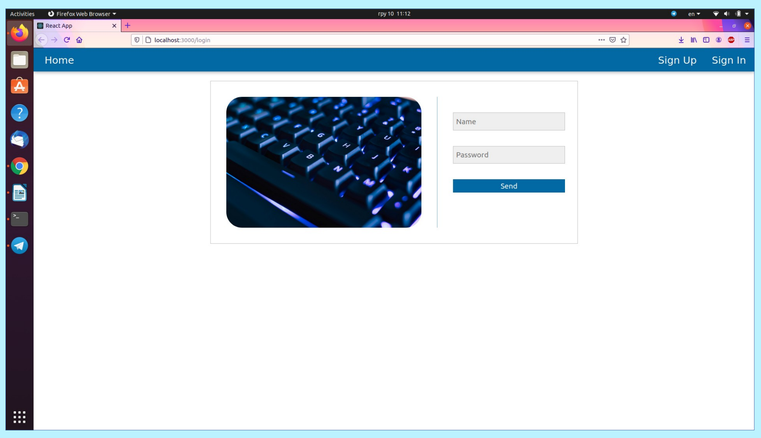

Рис 9 Сайт-програма шифрування та передачі даних в хмарні сховища