АЛГОРИТМ ШИФРУВАННЯ ДЛЯ ПОШТОВИХ ПОВІДОМЛЕНЬ

Камінський Д.А., Шапорін Р.О.

Запропонований алгоритм шифрування для поштових повідомленьна основі декількох існуючих шифрувань. А саме використовується:

- квадрат Полібія;
- переведення символів у двійковий код;
- асиметричний метод шифрування RSA.

Вибір цих видів шифрування зумовлений тим, що вони мають досить велику швидкість шифрування та високу криптостійкість в порівнянні з іншими розглянутими шифрами та методами шифрування.

А саме це важкість отримати відповідний ключ для заповнення квадрату Полібія дуже швидко. Тим не менш, в програмі використовується не просто латинський алфавіт, що складається з 26 символів (для заповнення квадрату Полібія за 25), а саме використовується латинський алфавіт верхнього та нижнього регістру, цифри, розділові знаки та символи: ()[]/+*%@&# .

Також для більшої криптостійкості використовується асиметричне шифрування ключа алгоритмом RSA.

Так для того, щоб зламати даний шифр необхідно або розшифрувати ключ, або методом повного перебору знайти потрібну комбінацію символів, якими заповнюється квадрат Полібія. Перший спосіб зламу шифрування є складним, бо необхідно мати великі обчислювальні потужності, щоб підібрати пару простих чисел для отримання ключа. Другий спосіб є не таким складним, але дуже довгим за часом. Для того, щоб перебрати 81! комбінацій знадобиться дуже велика кількість часу та великі обчислювальні ресурси.

Для того, щоб зашифрувати текст квадратом Полібія, використовується квадрат із хаотичним заповненням символів. Надалі відкритий текст розбивається на символи та зчитуються їх координати в представленому квадраті.

Координати виписуються у стовпчик, спочатку вертикальна, потім горизонтальна. Надалі рядок з горизонтальними координатами зсуваються на 1 вліво. Після цього координати зчитуються вертикально і тим самим отримуються зашифровані символи повідомлення.

Також у розробленому шифрі присутній переклад вже зашифрованих символів в двійкову систему, але з невеликою модифікацією. А саме додавання додаткових бітів на початок двійкової системи. Це обумовлено тим, що англійські літери перекладаються в двійкову систему за таблицею символів ASCII та мають меншу довжину двійкового коду. А символи українського та російського алфавіту перекладаються за кодуванням CP-1251. Тобто, наприклад, літера «А» українського або російського алфавіту має десятинний код 1040, що відповідає двійковому коду «1». Але розділові знаки, цифри та спеціальні символи мають менший розмір двійкового коду. Наприклад, «0» - це «110000». Тому для фіксованої довжини бітів додатково додаються нулі.

Після цього проходить інверсія двійкового коду. На виході отримується закодоване повідомлення у вигляді інверсного двійкового коду.