У шифрі Цезаря кожна літера зсувається на кілька позицій. Наприклад в шифрі Цезаря при зсуві на 2 символи праворуч A стане C, а X набуде значення Z. Шифр Віженера – поліалфавітний шифр, який складається з послідовності кількох шифрів Цезаря із різними зсувами. Для шифровки повідомлень може використовуватись таблиця алфавітів, чи як її ще називають – квадрат (таблиця) Віженера. Розмір (довжина сторони) таблиці Віженера дорівнює кількості символів в алфавіті. Таким чином застосовуючи шифр Віженера до латинського алфавіту вийде квадрат із стороною в 26 символів, тобто буде 26 різних шифрів Цезаря. На кожному етапі шифрування буде застосований окремий шифр Цезаря, засновуючись на літері ключового та секретного слів.

Працює шифр наступним чином. Людина, яка надсилає повідомлення записує ключове слово циклічно, доки довжина його не буде дорівнювати повідомленню. Після цього iй символ в шифротексті буде дорівнювати перетину iго символу в повідомленні та ключовому слові у таблиці.

Щоб розшифрувати текст потрібно у стовбці із iм символом ключа знайти iй символ шифротесту, тож iм символом повідомлення буде перший символ у рядку, який містить iй символ шифротесту.

Перейдемо до криптоаналізу. На відміну від шифру Цезаря, шифр Віженера не можна дешифрувати тільки використовуючи частотний аналіз чи атаку по масці. Але його можна дешифрувати, дізнавшись про довжину його ключа. Індекс співпадінь(тест Касіскі) – один з методів криптоаналізу шифру Віженера. Метод заснований на обчисленні вірогідності того, що дві випадкових частини тексту співпадуть. Цю вірогідність будемо називати індексом співпадінь.

Припустимо рядок х є відкритим текстом або отриманий за допомогою звичайної перестановки. В цьому випадку індекс співпадінь зручно виразити через вірогідності з’явлення і-го символу. Позначимо їх як pі, тоді отримаємо наступну формулу:

Так як величини мають певні значення, то для відкритого тексту індекс співпадінь не залежить від його змісту, а залежить тільки від мови, на якій написаний текст. Більше того, значення вже давно були дослідженні та відомі, що дозволяє розрахувати значення індексу співпадінь відкритого тексту для різноманітних мов.

|  |  |
| --- | --- |
| **Мова** | **Індекс співпадінь** |
| російська | 0.0553 |
| англійська | 0.0644 |
| італійська | 0.0738 |
| іспанська | 0.0775 |
| німецька | 0.0762 |
| французька | 0.0778 |

Якщо – випадковий рядок, тоді вірогідність з’явлення кожного символу дорівнює

Використовуючи першу формулу, отримаємо:

Цією формулою можна керуватися для оцінки індексу співпадінь поліалфавітного шифру. Для англійської мови індекс співпадінь поліалфавітного шифру дорівнює 0.03856, для української (без літери «Ґ») – 0.03125.

Значення індексу співпадінь для відкритого тексту і для поліалфавітного шифру суттєво відрізняються. Це дозволяє, маючи індекс співпадінь, визначити, чи отриманий текст з відкритого звичайною перестановкою, чи є поліалфавітним шифром.

Ще одним важливим поняттям є взаємний індекс співпадінь.

В загальному випадку розглянемо два рядки та із довжинами та відповідно. Алфавіт, як і раніше складається із символів. Взаємним індексом співпадінь цих рядків називають вірогідність того, що взявши по одному випадковому символу із кожного рядку, вони співпадуть. Нехай – кількість -х символів алфавіту в першому та другому рядках відповідно. Тоді взаємний індекс співпадінь буде дорівнювати:

Досить важливим для методу індекс співпадінь є його часний випадок, коли обидві рядки отримані зсувом алфавіту відкритого тексту. Позначимо – вірогідності з’явлення -го символу в рядку , – зсув алфавіту рядка відносно алфавіту рядка (ліворуч). Тоді вірогідності появи -го символу алфавіту в рядку дорівнюють (якщо використовувати нумерацію алфавіту рядка ). Для взаємного індексу співпадінь отримаємо наступну формулу:

Помітимо, що так як зсув циклічний, то і взаємний індекс співпадінь для зсувів і приймає одне й те саме значення. Нижче приведені значення взаємного індексу співпадінь в залежності від зсуву для англійської мови. Значення наведені для зсувів від 0 до . Як згадувалось вище, на основі цих значень взаємний індекс співпадінь може бути вирахуваний для будь-якого зсуву.

|  |  |
| --- | --- |
| **Зсув** | **Взаємний індекс** |
| 0 | 0.0644 |
| 1 | 0.0394 |
| 2 | 0.0319 |
| 3 | 0.0345 |
| 4 | 0.0436 |
| 5 | 0.0332 |
| 6 | 0.0363 |
| 7 | 0.0389 |
| 8 | 0.0338 |
| 9 | 0.0342 |
| 10 | 0.0378 |
| 11 | 0.0440 |
| 12 | 0.0387 |
| 13 | 0.0428 |

Помітимо, що при нульовому зсуві взаємний індекс співпадінь набагато більший, ніж при ненульових зсувах, тож по відомому значенню взаємного індексу співпадінь можна зробити висновок, чи є зсув алфавітів рядків нульовим, або ні.

Розіб’ємо текст на стовбці розміру .

… … … …

Якщо довжині ключа, то кожні два елементи тексту, які відрізняються друг від друга на позицій, , зашифровані одним і тим самим алфавітом. А це означає, що кожний рядок в виписаній вище таблиці отримана з відкритого тексту перестановки. Якщо ж не ділиться на довжину ключа, то рядки є поліалфавітним шифром.

Вище було сказано, що індекс співпадінь для перестановки відкритого тексту та для поліалфавітного шифру суттєво відрізняються. Таким чином перебравши різні значення та вираховуючи для кожного з них індекс співпадінь, можна виділити ті , які ділиться на довжину ключа. Визначити довжину ключа по цим даним буде не важко.

Допустимо, ми визначили довжину ключа . Тепер знайдемо сам ключ. Знову випишемо текст в стовбці розміру .

… … … …

Розглянемо два рядки цієї таблиці. Зсунемо алфавіт одного з рядків на символів та вирахуємо взаємний індекс співпадінь отриманих рядків. Так як кожний з цих двох рядків отриманий зсувом алфавіту відкритого тексту, то максимум взаємного індексу співпадінь буде спостерігатися при нульовому кінцевому відносному зсуві.

Тому використовується наступний алгоритм: вираховується взаємний індекс співпадінь для різних , шукається значення , при якому взаємний індекс співпадінь буде максимальним. Тоді початковий відносний зсув буде дорівнювати ( – розмір алфавіту). Рахуються відносні зсуви між кожною парою рядків. Так як зсуви рядків таблиці відповідають зсувам літер ключа, то залишається перебрати можливих ключей, і вибрати серед них найбільш вдалий.