НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря Сікорського"
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

Симетрична Криптографія

Комп'ютерний практикум №2

Варіант - 8

Виконали:
Студенти групи ФІ-13
Ісаченко Нікіта
Бондаренко Олександр

2024 р.

1 Мета роботи

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

2 Хід роботи

У ході роботи, нам потрібно було реалізувати шифросистему Віженера. Перша частина роботи полягала у тому, щоб реалізувати додавання та віднімання символів за алфавітом. Як і КП-1, ми використовували CP-1251 кодування, про переваги якого вже зазначали у звіті до попереднього комп'ютерного практикуму.

Сам алгоритм шифрування та дешифрування був не складним, оскільки все що ми робили- додавали або віднімали літеру тексту до літери ключа.

Щоб перевірити нашу реалізацію, ми взяли один шифротекст, та зашифрували його 7 різними ключами. Результати шифрування та дешифрування наведені у додатках.

Код:

```
char VigenereLab::alphabetAdd(char a, char b)
{
    if (!isSmallLetter(a) && !isSmallLetter(b)) return ERROR_CHAR;

    char a_num = a - char(224);
    char b_num = b - char(224);

    char res = char(224) + ((a_num + b_num) % 32);

    return res;
}

char VigenereLab::alphabetSubstract(char a, char b)
{
    if (!isSmallLetter(b)) return ERROR_CHAR;

    char reversed_b = 2 * char(224) - b + 32;

    return alphabetAdd(a, reversed_b);

}

std::string VigenereLab::Cipher(const std::string& text, const std::string& key)
{
std::string result;
for (size_t i = 0; i < text.size(); i++) {
    char c = alphabetAdd(text[i], key[i % key.size()]);
    result += c;
}
return result;
}

std::string VigenereLab::Decipher(const std::string& cipher, const std::string& key)
```

```
{
    std::string result;
    for (size_t i = 0; i < cipher.size(); i++) {
        char c = alphabetSubstract(cipher[i], key[i % key.size()]);
        result += c;
    }
    return result;
}
```

Наступним етапом був взлам Віженера. Для початку, ми визначили довжину блока, шляхом порівняння індексів літер на відстанні r. Довжина блокого шифротекстку нашого варіанту – 8. Для взламу ми використали два методи, код яких наведений далі:

```
std::string VigenereLab::CeasarVigenreCracker(const std::string& text, int blockSize)
{
    std::map<char, double> langFreqsPr(FREQ_TABLE);
    std::string key;
    auto langGreatest  = GetMaxPairFromMap(FREQ_TABLE);

    for (int i = 0; i < blockSize; i++)
    {
        std::map<char, int> blockFreqs = getFrequency(GetIthBlock(text, blockSize, i));

        auto blockGreatest = GetMaxPairFromMap(blockFreqs);


        key.push_back(alphabetSubstract(blockGreatest.first, langGreatest.first));

    }

    return key;
}

std::string VigenereLab::CrackVigenere(std::string& text, int blockSize)
{
    std::string key;
    for (int i = 0; i < blockSize; i++)
    {
        std::map<char, double> m;
        auto block = GetIthBlock(text, blockSize, i);
        auto blockFreqs = getFrequency(block);

        for (const auto& g : FREQ_TABLE)
        {
            double Mg = 0;
            for (const auto& t : FREQ_TABLE)
            {
                char tg = alphabetAdd(t.first, g.first);
                if (blockFreqs.find(tg) == blockFreqs.end()) continue;
                Mg += t.second * blockFreqs[tg];
```

```
            }
            m[g.first] = Mg;
        }

        auto maxElement = GetMaxPairFromMap(m);
        key.push_back(maxElement.first);
    }

    return key;
}
```

Ключі, які вийшли в результаті:

CeasarVigenreCracker: уланобсеребзяныепуля
CrackVigenere: улановсеребряныепули

Більш точним виявився CrackVigenere метод, оскільки більше спирається на розподіл частот у блоці дані. Таким чином, отримати відкритий текст:

эта система красного карлика никогда не имела названия только зубодробительно длинный ном
каталоге исследовавший ее киберзонд отметил наличие трех газовых
гигантов двух астероидных полей кометного облака и занес все эти данные в сектор второй
очереди по мнению инка киберзонда система не представляла никакой ценности для послави
уровнясамостоятельностииазартаонбыпоспорилсамссобойчтовближайшуютысячулетлюдизде

3 Висновок

У роботі ми оцінили надлишковість російської мови та ентропії на символ та біграм, що певне знадобиться нам у подальших дослідженнях. Ось така штука.