Лабораторная работа №3

Шифрование гаммированием

дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Койфман Кирилл Дмитриевич Группа: НФИмд-01-25

Цель работы Получение практических навыков реализации алгоритмов, использующих гаммирование.

Задачи

1. Реализовать алгоритм шифрования гаммированием конечной гаммой

---

1 задание

Для решения задачи данной работы была написана программа на C++:

```
int main()
{
    //Define input open message
    std::wstring enteredMessage = L"ПРИКАЗ";
    size_t enteredMessageLength = enteredMessage.size();
    //std::wcin >> enteredMessage;
    std::wcout << "Entered message: " << enteredMessage << '\n';
    std::wcout << "Entered message(codes):\n";
    printTextCodes(enteredMessage, alphabet);
    std::wcout << '\n';

    //Define input gamma
    std::wstring enteredGamma = L"ГАММА";
    size_t enteredGammaLength = enteredGamma.size();
    //!std::wcin >> enteredGamma;
    std::wcout << "Entered gamma: " << enteredGamma << '\n';
    std::wcout << "Entered gamma(codes):\n";
    printTextCodes(enteredGamma, alphabet);
    std::wcout << '\n';

    std::wstring encryptedMessage;
    for (std::uint32_t symbol_index = 0; symbol_index <
enteredMessageLength; ++symbol_index)
    {
        //ENCRYPTED_SYMBOL_CODE = ENTERED_MESSAGE_CODE + ENTERED_GAMMA %
ALPHABET_LENGTH
        std::uint32_t encryptedSymbolCode =
(alphabet.at(enteredGamma[symbol_index % enteredGammaLength]) +
            (alphabet.at(enteredMessage[symbol_index]) % alphabethLength))
% alphabethLength;
```

```
        for (auto& element : alphabet)
            if (element.second == encryptedSymbolCode)
            {
                encryptedMessage += element.first;
                break;
            }
    }
    std::wcout << "Encrypted message: " << encryptedMessage << '\n';
    std::wcout << "Encrypted message(codes):\n";
    printTextCodes(encryptedMessage, alphabet);
    std::wcout << '\n';
}
```

---

1 задание

```
[А]{1}  [Б]{2}  [В]{3}  [Г]{4}  [Д]{5}  [Е]{6}  [Ж]{7}  [З]{8}  [И]{9}
[Й]{10}
[К]{11} [Л]{12} [М]{13} [Н]{14} [О]{15} [П]{16} [Р]{17} [С]{18} [Т]{19}
[У]{20}
[Ф]{21} [Х]{22} [Ц]{23} [Ч]{24} [Ш]{25} [Щ]{26} [Ъ]{27} [Ы]{28} [Ь]{29}
[Э]{30}
[Ю]{31} [Я]{32}
Alphabet length: 32
Entered message: ПРИКАЗ
Entered message(codes):
16      17      9       11      1       8
Entered gamma: ГАММА
Entered gamma(codes):
4       1       13      13      1
----------------------------------ENCRYPTING-----------------------------
------
Encrypted message: УСХЧБЛ
Encrypted message(codes):
20      18      22      24      2       12
```

Спасибо за внимание!