Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Кафедра програмної інженерії

Практична робота №1 з дисципліни: «Безпека програм та даних» на тему: «Шифр Цезаря»

Виконав:

студент групи ПЗПІ-20-1 Бабанін А.К.

Перевірив:

доцент кафедри Програмної інженерії Турута О.П

Харків 2022

Завдання 1

Шифрований текст: жиш лмикизн! Жязщ чми мъе ьивжнмгёи. Лзъсъёъ щ ь йген яжн лмъёъ ьиьлш оёгкмиьъмц л

Ключ: 27

Оригінальний текст: мою сторону! Меня это так возмутило. Сначала я в пику ему стала вовсю флиртовать с

Шифрування тексту було виконанно шифром Цезаря. Розшифрування тексту виконується наступним чином: *x = ( y + n ) – ( k mod n ) ) mod n*

де

x – символ відкритого тексту,

y – символ шифрованого тексту,

n – потужність алфавіту,

k – ключ

Код CSharp для розшифрування:

public string DecryptString(string encryptedString, int key)

{

var shift = key % this.alphabetLength;

var sb = new StringBuilder();

foreach (var encryptedChar in encryptedString)

{

// special case

if (this.specialChars.Contains(encryptedChar))

{

sb.Append(encryptedChar);

continue;

}

var caseAddition = !this.IsLower(encryptedChar) ? 0 : this.alphabetLength;

var encryptedIndex = this.alphabet.IndexOf((char)(encryptedChar + caseAddition));

var decryptedIndex = (encryptedIndex + this.alphabetLength - shift) % this.alphabetLength;

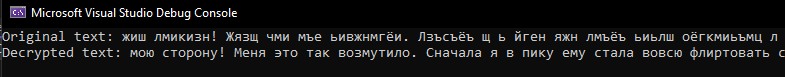
var decryptedChar = this.alphabet[decryptedIndex];

sb.Append((char)(decryptedChar -caseAddition));

}

return sb.ToString();

}

Результат виконання: 

Завдання 2

Шифрований текст: прщвжх ом ьпьчщрциф ётът сбнмж рапьмлфск идф башср н 1984 лопь. ощ шррмпъфотсл, гыо рълф йы ычянсллъь нчзшчжщчсюе иэшочезъкаюе в цичрътнн оюуржыооч кчжчл смк слф шогыондй лмрръ ачссж, ыо иыо чсшффо мд сччжщью ыщовндящу льтрцтфэицицфс вэзкъло эхыэфа. пчлоче нщешз ипня димфща ъътлкачисз ксрло чсшз урлъинчй цщиыыоощаасчръкът гъфончлъхкът, нъ к 2000 гъму, мфаочдлщя ъмнът иукеэынът укрвфхоэыи н ёлчспюсчръкът кьспючгьиффс, ипню ямаччсз коыфоюстз к жфрнз.

Ключ: Али

Оригінальний текст: Первым об упрощении этой схемы задумался Ади Шамир в 1984 году. Он предположил, что если бы появилась возможность использовать в качестве открытого ключа имя или почтовый адрес Алисы, то это лишило бы сложную процедуру аутентификации всякого смысла. Долгое время идея Шамира оставалась всего лишь красивой криптографической головоломкой, но в 2000 году, благодаря одной известной уязвимости в эллиптической криптографии, идею удалось воплотить в жизнь.

Шифрування тексту було виконанно шифром Віженера. Розшифрування тексту виконується наступним чином: *mi = ( ci – ki ) mod n*

де

ci – індекс символу шифрованої букви

ki – індекс символу ключа

n – потужність алфавіту,

Код CSharp для розшифрування:

public string DecryptString(string encryptedString, string key)

{

var resultBuilder = new StringBuilder();

var processedCharCount = 0;

for (var i = 0; i < encryptedString.Length; i++)

{

var textChar = encryptedString[i];

var keyChar = key[processedCharCount % (key.Length)];

if (this.specialChars.Contains(textChar))

{

resultBuilder.Append(textChar);

continue;

}

var textCaseAddition = !this.IsLower(textChar) ? 0 : this.alphabetLength - 1;

var keyCaseAddition = !this.IsLower(keyChar) ? 0 : this.alphabetLength - 1;

var textCharIndex = this.alphabet.IndexOf((char)(textChar + textCaseAddition));

var keyCharIndex = this.alphabet.IndexOf((char)(keyChar + keyCaseAddition));

var encryptedIndex = (textCharIndex - keyCharIndex + this.alphabetLength) % this.alphabet.Count;

var encryptedChar = this.alphabet[encryptedIndex];

resultBuilder.Append(encryptedChar);

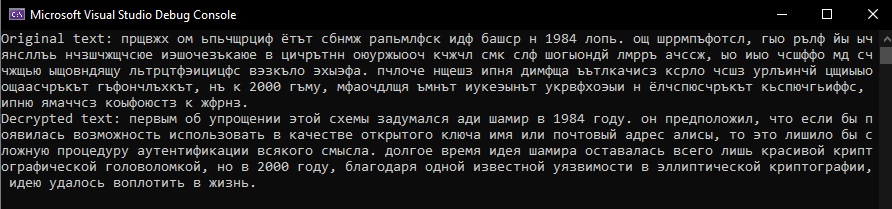
processedCharCount++;

}

return resultBuilder.ToString();

}

Результат роботи:



Завдання 3

Зашифрований текст: ыникжы ъй лшьэенёсф лючв ъбушд аипвшидък опс ришчь к 1984 ычпв. ъц зщртычдчтчч, акч рачс щд ыэккбфлаз кжршэтцжъюк фъзччкучъиюк н ушараюкэ чющьдкчоэ цфцал чшз бфф юъакчнйх иьщра лфбъж, бъ ёкч ччдсдч мй эфжпщвй шичвупьиь лвюнёыфгфушяфч нъчуъсъ ъедэъл. мжфоэр киншн фмэз дошсии ъаюиъичоэе ъърсъ фббз щьийснэх уисыбълииачгнйуъш очдчнэччеуъш, щч ъ 2000 лътя, йдиоэпииз ътщчв сурръкцъш язакфыъъкс н лчфбшючгнйуъш цщбшюэощшэфч, фмэж ятлфжъз ръшдчючюе ъ пфцще.

Ключ: Лишило

Використовуючи дешифрування шифру Віженера отримуємо наступний результат:

