Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №3

на тему: «Криптоаналіз афінної біграмної підстановки»

Виконали:

студенти 3 курсу ФТІ

групи ФБ-71

Безлюдний В.

Мельник Д.

Перевірив: Чорний О.

Мета роботи: Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної

підстановки; опанування прийомами роботи в модулярній арифметиці.

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням

оберненого елементу за модулем із використанням розширеного алгоритму Евкліда,

розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання

комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за

варіантом).

3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту

(розглядаючи пари біграм із п'яти найчастіших). Для кожного

співставлення (a, b) знайти можливі кандидати на ключ шляхом

розв'язання системи (1).

4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним

текстом російською мовою, відкинути цього кандидата.

5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Результати виконання роботи:

Найчастіші біграми:

Мови: ст но то на

ен; Шифртексту:

ыу юк як ую ып

Знайдений ключ, шо приводить до змістовного тексту:

27, 211

Розшифрований текст:

однакоэтакартинаскакойбысторонымыеенирассматривалирасплываетсявнечтонеопределенноепри
падкипроявляющиесярезкосприкусываниемусиливающиесядоопасногодляжизниприводящегоктяж
комусамокалечениюмогутвсежевнекоторыхслучаяхнедостигатьтакойсилыослабляясьдократкихсос
тоянийабсансадобыстропроходящихголовокруженийимогуттакжесменятьсякраткимипериодамико
гдабольнойсовершаетчуждыеегоприродепоступкикакбынаходясьвовластибессознательногообусла
вливаясьвобщемкакбыстранноэтониказалосьчистотелеснымипричинамиэтисостоянияимогутпервон
ачальновозникатьпопричинамчистодушевнымиспугилимогутвдальнейшемнаходитьсявзависимост
иотдушевныхволненийкакнихарактернодляогромногобольшинствослучаевинтеллектуальноеснише
ниеноизвестенпокрайнеймереодинслучайкогдаэтотнедугненарушилвысшейинтеллектуальнойдеяте
льностигельмгольцдругиеслучаивотношениикоторыхутверждалосьтожесамоененадежныилиподле
жатсомнениюкакислучайсамогодостоевскоголицастрадающиеэпилепсиеймогутпроизводитьвпечат
лениетупостинедоразвитоститкакэтаболезньчастосопряженасярковыраженнымидиотизмомикру
пнейшимимозговымидефектаминеявляяськонечнообязательнойсоставнойчастьюкартиныболезнин
оэтиприпадкисовсемисвоимивидоизмененияхмибываютиудругихлицулицсполнымдушевнымразвит
иемискореесосверхобычнаявбольшинствеслучаевнедостаточноуправляемойимиаффективностьюне
удивительночтопритакихобстоятельствахневозможноустановитьсовокупностьклиническоюаффект
аэпилепсииточтопроявляетсяводнородностиуказанныхсимптомовтребуетповидимомуфункциональ
ногопониманиякакеслибымеханизманормальноговысвобожденияпервичныхпозывовбылподготовл
енорганическимеханизмкоторыйиспользуетсяприналичииивесьмаразныхусловийкакпринарушении
мозговойдеятельностипритяжкомзаболеваниитканейилитоксическомзаболеваниитакипринедостат
очномконтроледушевнойэкономиикризисномфункционированиидушевнойэнергиизаэтимразделен
иемнадвавидамычувствуемндентичностьмеханизмалежащеговосновевысвобожденияпервичныхпо
зывовэтотмеханизмнедалекиотсексуальныхпроцессовпорождаемыхвсвоейосноветоксическиужедр
евнейшиеврачиназываликоитусмалойэпилепсиейивиделивполовомактесмягчениеиадаптациювысв
обожденияэпилептическогоотводараздраженияэпилептическаяреакциякаковымименемможноназва
тьвсеэтовместевзятоенесомненнотакжепоступаетивраспоряжениеневрозасущностькотороговтомчт
обыликвидироватьсоматическимассыраздраженияскоторыминеврознеможетсправитьсяпсихически
эпилептическийприпадокстановитсятакимобразомсимптомомистериииеюадаптируетсяивидоизмен
яетсяподобнотомукакэтопроисходитпринормальномтечениисексуальногопроцессатакимобразомм
ысполнымправомразличаеморганическуюиаффективнуюэпилепсиюпрактическоезначениеэтогосле
дующеестрадающийпервойпораженболезньюмозгастрадающийвторойневротиквпервомслучаедуш
евнаяжизньподверженанарушениюизвневовторомслучаенарушениеявляетсявыражениемсамойдуш
евнойжизнивесьмавероятночтоэпилепсиядостоевскогоотноситсяковторомувидуточнодоказатьэтон
ельзятаккаквтакомслучаенужнобылобывключитьвцелокупностьегодушевнойжизниначалоприпадк
овипоследующиевидоизмененияэтихприпадковадляэтогоунаснедостаточноданныхописаниясамих
припадковничегонедаютсведенияосоотношенияхмеждуприпадкамиипереживанияминеполныичаст
опротиворечивывсеговероятнеепредположениечтоприпадкиначалисьудостоевскогоужевдетствечт
оонивначалехарактеризовалисьболееслабымисимптомамиитолькопослепотрясшегоегопереживани

янавосемнадцатомгодужизниубийстваотцапринялиформуэпилепсиибылобывесьмауместноеслибы оправдалосьточтоониполностьюпрекратилисьвовремяотбыванияимкаторгивсибириноэтомупротив оречатдругиеуказанияочевиднаясвязьмеждуотцеубийствомвбратьяхкарамазовыхисудьбойотцадост оевскогобросиласьвглазанеодномубиографудостоевскогоипослужилаимуказаниемнаизвестноесовр еменноепсихологическоенаправлениепсихоанализтаккакподразумеваетсяименноонсклоненвидетьв этомсобытиитягчайшуютравмуивреакциидостоевскогонаэтоключевойпунктегоневрозаеслияначну обосновыватьэтуустановкупсихоаналитическиопасаюсьчтоокажусьнепонятнымдлявсехтехкомунез накомыучениеивыраженияпсихоанализаунасодиннадежныйисходныйпунктнамизвестенсмыслперв ыхприпадковдостоевскоговегоюношескиегодызадолгодопоявленияэпилепсииуэтихприпадковбыло подобиесмертиониназывалисьстрахомсмертиивыражалисьвсостоянииелетаргическогоснаэтаболезн ьнаходилананеговначалекогдаонбылещемальчикомкаквнезапнаябезотчетнаяподавленностьчувство каконпозжерассказывалсвоемудругусоловьевутакоекакбудтобыемупредстоялосейчасжеумеретьив самомделенаступалосостояниесовершенноподобноедействительнойсмертиегобратандрейрассказы валчтофедоружевмолодыегодыпередтемкаказаснутьоставлялзаписькичтобоитсяночьюзаснутьсмерто подобнымсномипроситпоэтомучтобыегопохоронилитолькочерезпятьднейдостоевскийзарулеткойв ведениеснамизвестнысмыслинамерениетакихприпадковсмертониозначаютотождествлениесумер шимчеловекомкоторыйдействительноумерилисчеловекомживымещенокоторомумыжелаемсмерти второйслучайболеезначителенприпадоквуказанномслучаеравноцененнаказаниюмыпожелалисмерт идругомутеперьмысталисамиэтимдругимисамиумерлитутпсихоаналитическоеучениеутверждаетчт оэтотдругойдлямальчикаобычноотециименуемыйистериейприпадокявляетсятакимобразомсамонак азаниемзапожеланиесмертиненавистномуотцуа

Код програми:

```
#include <iostream>
#include <fstream>
#include <string>
#include <vector>

using namespace std;



int findmax(int arr[]) // find max and erase mod(31)
{
	int max = 0, maxval = 0, n = 31;
	for (int j = 0; j < n * n; j++)
	{
		if (maxval <= arr[j]) { maxval = arr[j]; max = j; }
	}
	arr[max] = 0;
	return max;
}

int mod(int k, int m) // k mod m
{
	if (k < m)
	{
		if (k < 0) { for (;;) { k += m; if (k > 0) return k; } }
		return k;
	}
	else {
		for (;;)
		{
			k = k - m;
			if (k < m)return k;
		}
		return k;
	}
}


int gcdExtended(int a, int b, int* x, int* y)
{
```

```
	if (a == 0)
	{
		*x = 0, * y = 1;
		return b;
	}

	int x1, y1;
	int gcd = gcdExtended(b % a, a, &x1, &y1);


	*x = y1 - (b / a) * x1;
	*y = x1;

	return gcd;
}

int InvCheck(int a ,int b ,int m) {
	int x, y;
	int g = gcdExtended(a, m, &x, &y);
	if (g != 1)
	{
		if (b % g != 0 || a == 0 || b == 0)return 0;
		else {
			return g;
		}
	}
	else return 1;
}

int modInverse(int a, int m)
{
	int x, y;
	int g = gcdExtended(a, m, &x, &y);
	if (g != 1)
	{

		return 0;
	}
	else
	{

		int res = (x % m + m) % m;
		return res;
	}
}



int decipher(int a , int Y , int b , int m )
{
	return  mod(modInverse(a , m) * (Y - b), m);
}


int encipher(int a, int b , int X, int m)
{
	return  mod(X * a + b , m);
}


void TextHandler()
{
	ofstream output("output.txt");
	ifstream input("input.txt");


	string str = "", str1 = "";

	const int n = 31;
```

```
	char charalph[n] = { 'а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ', 'ы', 'ь', 'э', 'ю', 'я' };
	string alph = "абвгдежзийклмнопрстуфхцчшщьыэюя";


	while (input)
	{
		getline(input, str1);
		str += str1;
		if (input.eof())break;
	}
	output << str << endl;
	//if (str.length() % 2 == 0)cout << str.length() / 2; else cout << "ACHTUNG!!\n";// can be divided by 2?
	input.close();
	output.close();
}

void TextToInt()
{
	ifstream input("output.txt");
	ofstream output("BigrText.txt");
	ofstream outpute("test02.txt");//check

	const int n = 31;
	char charalph[n] = { 'а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ', 'ы', 'ь', 'э', 'ю', 'я' };
	string alph = "абвгдежзийклмнопрстуфхцчшщьыэюя", text ;

	getline(input, text);
	vector<int> encarr; //encrypted text bigramms to int array
	int x1 = 0, x2 = 0;


	for (int i = 0; i < text.length(); i = i + 2) //transforms text to bigr int
	{

		for (int j = 0; j < n; j++)
		{
			if (text[i] == alph[j])
			{
				x1 = j;
				break;
			}
		}

		for (int j = 0; j < n; j++)
		{
			if (text[i + 1] == alph[j])
			{
				x2 = j;
				break;
			}
		}
		outpute << alph[x1]<<alph[x2];// checking

		encarr.push_back(x1 * n + x2);
		if (i == text.length() - 2)
			output << encarr.at(encarr.size() - 1);
		else output << encarr.at(encarr.size() - 1) << " ";

	}

	outpute.close();//check
	output.close();
	input.close();
}

void XY()
{
	ifstream input("BigrText.txt");
```

```
	ofstream output("some.txt");
	ofstream out("keys.txt");
	ofstream outee("test01.txt");


	const int n = 31 ;
	char charalph[n] = { 'а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ', 'ы', 'ь',
'э', 'ю', 'я' };
	string alph = "абвгдежзийклмнопрстуфхцчшщьыэюя", mostfrdec[5] = { "ст" , "но" , "то" , "на" , "ен" };
	vector <int> text;



	int mfbd[5], mfbe[5], frarr[n * n], temp , arr[50] ;

	for (int i = 0; i < n * n; i++)
	{
		frarr[i] = 0;
	}

	while (!input.eof())
	{
		input >> temp;
		text.push_back(temp);
		frarr[temp]++;
	}

	for (int i = 0; i < 5; i++)
	{
		mfbe[i] = 0;
		mfbd[i] = 0;
	}

	for (int i = 0; i < 5; i++)
	{
		mfbe[i] = findmax(&frarr[0]);
	}

	for (int i = 0; i < 5; i++)// transform st, no etc to number
	{
		for (int j = 0; j < alph.length(); j++)
		{
			if (mostfrdec[i][0] == alph[j])
			{
				mfbd[i] = j * alph.length();
				break;
			}
		}
		for (int j = 0; j < alph.length(); j++)
		{
			if (mostfrdec[i][1] == alph[j])
			{
				mfbd[i] += j;
				break;
			}
		}
	}



	for (int i = 0; i < 50; i = i + 2)
	{
		arr[i] = mfbd[(i / 2) / 5 ];
		arr[i + 1] = mfbe[mod(i / 2, 5)];
	}



	int check = 0,l = 0;
```

```
	int temp1 = 0, temp2 = 0,chk = 0, temp3 = 0 ,n_a = 0, n_b = 0;
	vector <int> v_a, v_b;


	for (int i = 0; i < 50; i = i + 2)
		for (int j = 0; j < 50; j = j + 2)
		{
			temp1 = mod((arr[i + 1] - arr[j + 1]), n * n);
			temp2 = mod(arr[i] - arr[j] , n * n);
			//check  // cout << "( " << arr[i] << " , " << arr[i + 1] << " )" << " : " << "( " << arr[j] << " , " <<
arr[j + 1] << " )" << endl;

				chk = InvCheck(temp2, temp1 ,n * n);
				//if (chk != 1 && chk != 0)cout << "Check: " << chk << " Size: " << v_a.size() << endl;
				if (chk == 1) {
					n_a = mod( temp1 * modInverse(temp2, n * n) , n * n);
					v_a.push_back(n_a);
					n_b = mod(arr[i + 1] - n_a * arr[i], n * n);
					v_b.push_back(n_b);
				}
				else if (chk == 0)continue;
				else {
					temp3 = modInverse(temp2 / chk , n * n / chk);
					for (int k = 0; k < chk; k++) {
						n_a = mod( (temp1 / chk ) * temp3 + k * n * n / chk , n * n );
						v_a.push_back(n_a);
						n_b = mod( arr[i + 1] - n_a * arr[i] , n * n);
						v_b.push_back(n_b);
					}

					break;
				}
				chk = 0;
		}



	temp = 0;

	for (int i = 0; i < v_a.size() ; i++)
	{
		for (int j = 0; j < text.size(); j++)
		{
			temp = decipher( v_a[i], text[j], v_b[i] , n * n );
			output << alph[temp / n] << alph[temp % n];
		}
		output << "\n";
		out<< v_a[i] << " " << v_b[i]<< endl;
	}

	out.close();
	output.close();
	input.close();
}

void checker()
{
	ifstream in("keys.txt");
	ifstream input("some.txt");
	ofstream output("done.txt");


	const int n = 31;
	char charalph[n] = { 'а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л', 'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ', 'ы', 'ь',
'э', 'ю', 'я' };
	string alph = "абвгдежзийклмнопрстуфхцчшщьыэюя", text,  tmp = "",ab  = "";
	int a = 0, b = 0;
```

```
	bool flag = 0;


	while (!input.eof())
	{
		getline(input, text);
		in >> a >> b;


		for (int i = 0; i < text.length(); i = i+2)
		{
			tmp += text[i];
			tmp += text[i + 1];

			if (tmp == "аы" || tmp == "оы" || tmp == "еы" || tmp == "уы" || tmp == "оы" || tmp == "аь" || tmp
== "оь" || tmp == "еь" || tmp == "иь"|| tmp == "аа")
			{
				flag = 1;
				break;
			}
			tmp = "";
		}
		if (flag == 0) {
			output << text << "\n" << a << " " << b << "\n";
		}
		flag = 0;
	}


	in.close();
	output.close();
	input.close();
}



int main()
{
	TextHandler();
	TextToInt();
	XY();
	checker();



	system("pause");
	return 0;
}
```