МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря Сікорського»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Протокол
до лабораторної роботи №2
з Симетричної криптографії
«Криптоаналіз шифру Віженера»

Підготували:
студент групи ФІ-83
Яценко Артем Ігорович
Гузей Дмитро Русланович

Викладач:
Деркач Олександр Григорович

Перевірено:_____

Київ – 2021

Мета:

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

Постановка задачі:

1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

2. Підрахувати індекси відповідності I r для відкритого тексту та всіх одержаних шифротекстів і порівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта). Зокрема, необхідно:

– визначити довжину ключа, використовуючи або метод індексів відповідності, або статистику співпадінь D r (на вибір);

– визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові;

– визначити символи ключа за допомогою функції M i (g) ;

– розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ.

Варіанти:

Гузей Д. — 5

Яценко А. — 16

Значення індексів відповідності:

Text (2-3 Kb)

В этой статье приведем небольшую, с одной стороны шутливую, но с другой стороны полностью научную теорию с помощью которой можно оправдать себя в те моменты, когда над Вами взяла верх лень. Дело в том, что в физике существует такая термодинамическая величина как энтропия. Её научное значение определяет меру необратимого рассеивания энергии. В других случаях она же может определять вероятность осуществления какого-либо макроскопического состояния. Однако, скажем так, «в быту» проще понять значение энтропии как меры неупорядоченности системы: чем меньше элементы системы подчинены какому-либо порядку, тем выше энтропия. Здесь сделаем небольшое уточняющее замечание о том, что такое порядок. Это очень важно, потому что ситуацию, когда что-то равномерно распределено по доступному пространству можно назвать беспорядком или хаосом (если, например, речь идет о мусоре, равномерно накиданном на пол в комнате). Но подобную ситуацию можно назвать и порядком (если речь идет, например, о качественно и равномерно окрашенной стене), тут уж кому что, и у кого какие ассоциации... Однако мы договоримся для нужд этой статьи, что, как и все физики и другие ученые, будем понимать под порядком наличие некоторой выраженной структуры в системе (например, существование конкретных предметов в определенных точках пространства), а под беспорядком – равномерное распределение всех видов материи в пространстве. В таком случае, энтропия – это мера беспорядка.

key_2 = «ня»

key_3 = «три»

key_4 = «шифр»

key_5 = «цезар»

key_{17} = «гиперболоидгарина»

Таблиця Індексів відповідності:

r, довжина ключа	**I** идекс выдповдности
R = 2	I_0 = 0.06284722028352717 I_1 = 0.05718111180204254 ---------- **I_average = 0.06001416604278485**
R = 3	I_0 = 0.06279517890202894 I_1 = 0.057744864674248435 I_2 = 0.059331746451556026 ---------- **I_average = 0.05995726334261114**
R = 4	I_0 = 0.06352285395763657 I_1 = 0.05739489573746942 I_2 = 0.06094139301025791 I_3 = 0.0588987901506139 ---------- **I_average = 0.06018948321399445**
R = 5	I_0 = 0.057775453277545324 I_1 = 0.0642608089260809 I_2 = 0.06880911360360044 I_3 = 0.052248514468548925

	I_4 = 0.05629197285608804 ---------- **I_average = 0.059877172626372724**
R = 17	I_0 = 0.06639839034205232 I_1 = 0.0647887323943662 I_2 = 0.055533199195171024 I_3 = 0.06438631790744467 I_4 = 0.04788732394366197 I_5 = 0.07042253521126761 I_6 = 0.07042253521126761 I_7 = 0.0546583850931677 I_8 = 0.06666666666666667 I_9 = 0.047619047619047616 I_10 = 0.05548654244306418 I_11 = 0.06459627329192547 I_12 = 0.06252587991718427 I_13 = 0.04803312629399586 I_14 = 0.047619047619047616 I_15 = 0.07950310559006211 I_16 = 0.07494824016563147 ---------- **I_average = 0.06126443228853084**

Індекси відповідності при пошуку довжини ключа:

Var 16:

R, довжина ключа	
R = 2	0
R = 3	0
R = 4	0
R = 5	0
R = 6	0
R = 7	0
R = 8	0
R = 9	0
R = 10	0
R = 11	0
R = 12	0
R = 13	0
R = 14	0
R = 15	0
R = 16	0
R = 17	0
R = 18	0
R = 19	0
R = 20	0

R = 21	**0**
R = 22	0
R = 23	0
R = 24	0
R = 25	0
R = 26	0
R = 27	0
R = 28	0
R = 29	0

R = 21

Значення ключа, одержане шляхом співставлення найчастіших літер блоків найчастішій літері мови:

Оберемо у якості найчастышоі літери мови літеру **“o“**:

Key = **«*башяцщросмичерннемчбъ*»**

башяцщросмичерннемчбъ

башняяростичерныемаки

Значення ключа, одержане із використанням функції M i (g):

Key = «***башняяростичерныемаки***»

Фрагмент тексту:

«*яэльфизкланалебедянопишунаязыкесмертныхобителейарциитаккакбольшевсехотз лонамереннойлжистрадаютименнолюдигоблиныслишкомпростодушныичестнычтобиз корыстиизменятьпрошлоеамыпоследниеэльфытаррынезабудемхотьнамиданозабыват ьмойрассказобращенктемктопонимаетчтобудущеевырастаетизминувшегояродилсяяви нуюэпохуипомнюмногоеимногихстаршеменялишьутратившаясилунонемудростьиллиэл ьнодажеонаувиделасветвэтоммиреотомкакбылазавоеванатарраяпишусчужихсловвтег одаоткоторыхнеосталосьдажесновпокровительницейкланалебедябылаадденадевачьеим яныненоситвеличайшаяизрекарциидаисамаарцияобязанасвоимназваниемпервомуизуше дшихвсегожесветлыхбоговзахватившихтарруидолгиегодыправившихеюименемсветаб ылосемеропятеробратьевидвесестрыстаршимбыларцейповелительсолнцапламениим олнийостальныепризнавалиеговластьнолюбвиисогласиямежсветозарныминебылониког дабольшедругихвладыкаарцейопасалсясвоегобратаангесабогавойныхолодногожелезаип рощенияволкиполнаялунабылиегосимволамиисамонбылпохожнаодинокоговолкабесстра шногоисвободноговоиннежелалвластоватьновт*»

Var 5:

R, довжина ключа	
R = 2	I_average = 0.03709682620655367
R = 3	I_average = 0.03535245194471151
R = 4	I_average = 0.039793511667390036
R = 5	I_average = 0.0354351293936251
R = 6	I_average = 0.037052368586566846
R = 7	I_average = 0.03522360497899179
R = 8	I_average = 0.04491213203766699
R = 9	I_average = 0.03545025157077616
R = 10	I_average = 0.03709763005817014
R = 11	I_average = 0.03506214646542888
R = 12	I_average = 0.0397888484387092
R = 13	I_average = 0.03550919719241092
R = 14	I_average = 0.037093872461702884
R = 15	I_average = 0.035384371390931875
R = 16	**I_average = 0.05539766505382552**
R = 17	I_average = 0.035524349460576386
R = 18	I_average = 0.037051140206933175
R = 19	I_average = 0.03531599104429486
R = 20	I_average = 0.03979839848540342
R = 21	I_average = 0.035056696947883076
R = 22	I_average = 0.03688094981192191
R = 23	I_average = 0.03526676001305198
R = 24	I_average = 0.04486292731353409
R = 25	I_average = 0.03531687664602463
R = 26	I_average = 0.03731086887465935

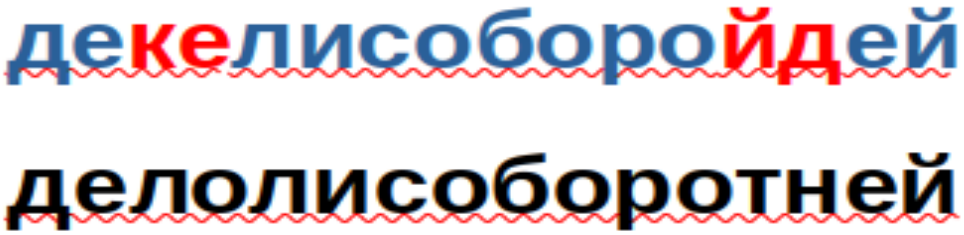
R = 27	I_average = 0.035247591055245484
R = 28	I_average = 0.03969086727168179
R = 29	I_average = 0.035584903885058694

R = 16

значення ключа, одержане шляхом співставлення найчастіших літер блоків йчастішій літері мови

Оберемо у якости найчастышоъ лытери мови лытеру “о“:

key = «*декелисоборойдей*»



значення ключа, одержане із використанням функції M і (g):

Key = «***делолисоборотней***»

Фрагмент текста

«*понятноеделокультурунасильновчеловеканеводкнешьвордусиэтудовольногрустнуюистинузналинаверноелучшечемгдебытонибыловмирекультурностьпреждевсегоусилиеежелионосызмальстванесделалосьчеловекусвычнымдажевнутреннепотребнымоттогоотомногочисленныеподразделенияпалатыцеремонийиуделяютстольковниманиядетямособеннодетямтехктонаселяетхутунынотомужобычнаяленостьлюдскаяслужитемупочтинеодолимымпрепятствиемнанеобъятныхпросторахимперииевстречаетсяещенемалолюдейкоторымпокакимтолишьбуддазнаеткакимпричинамтакинесталоинтереснымничтоглавноенисветозарныевысотыдухавеликихрелигийивечныйпоисксмыслажизниземнойпитающийистинноеискусствониголовокружительныебезднынакраюкоихвечнопребываетнастилающаянаднимиобщепроходимыегатинауканихотябычистоепросторноесостояте льноеидобродетельноежитьестольестественноедлябольшинстваордусскихподданныхчтогрехатаитьхутунынаселеныбыливосновномварварамиинебычномпониманииэтогословаисстариобозначавшеголюдейинойнеордусскойкультурыаскореевтомегозначенииктороестольжедавносделалосьобычнымвевропелю»