Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

СИМЕТРИЧНА КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера
Варіант № 5

Виконав: студент гр. ФІ-94, Кріпака І.А.

Перевірив: Чорний О.М.

Київ – 2021

1) **Мета комп’терного практикуму**

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

2) **Постановка задачі**

Написати програму для шифрування текста обраними ключами різної довжини. Пошук ключа та розшифрування даного тексту.

3) **Порядок виконання роботи**

1. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.
2. 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.
3. Підрахувати індекси відповідності Ir для відкритого тексту та всіх одержаних шифротекстів і порівняти їх значення.
4. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта). Зокрема, необхідно:
   визначити довжину ключа, використовуючи або метод індексів відповідності, або статистику співпадінь Dr (на вибір);
   визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові;
   визначити символи ключа за допомогою функції Mi(g);
   розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ.

4) **Опис труднощів**
Основні трудноща були із розумінням, як її треба правильно зробити, але, напрочут, усе вийшло дуже легко.

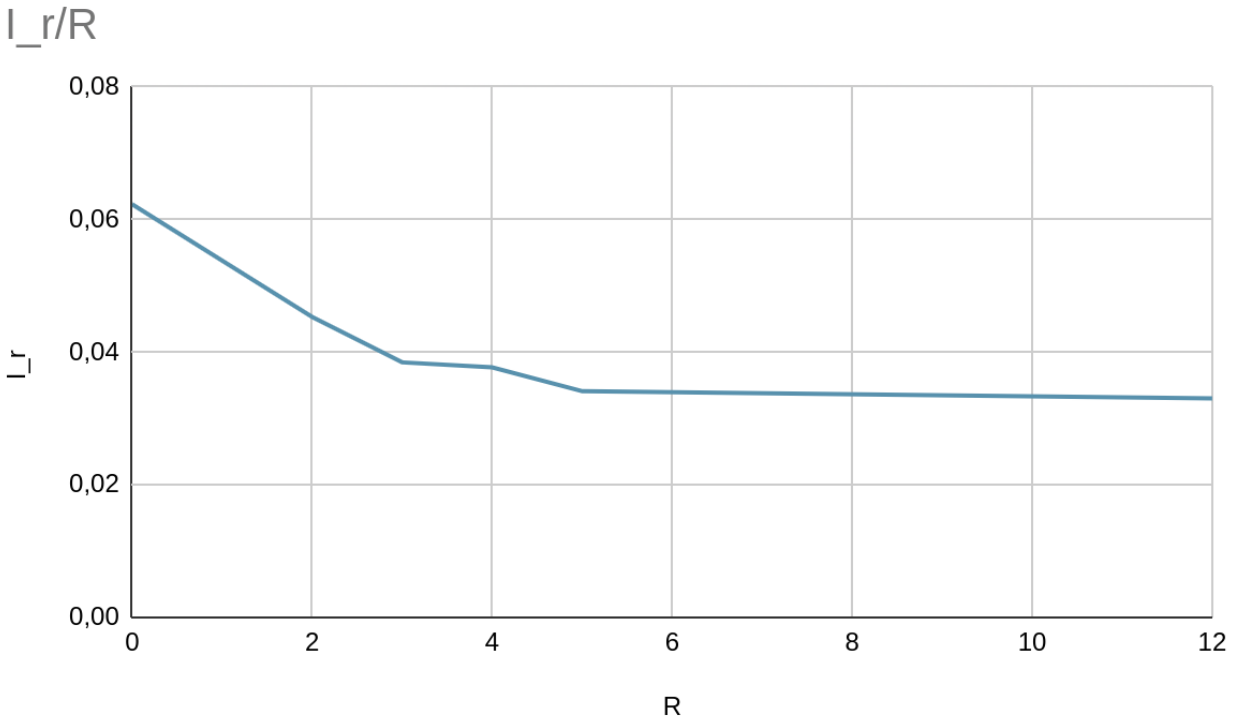
Виникли запитання із обчисленням D_r так як не розумів, що треба брати менші значення чим сама довжина тексту, тобто при шифруванні к.чем довжини 11 отримував, що сам ключ за алгоритмом буде розміру 100 при довжині тексту 124 символів. Усе вирішилося перебротом сум до 30 символьного ключа за замовчуванням.

Посилання на код

Практична частина

1) **Індекс відповідності для ключей різної довжини:**

R	2	3	4	5	15	Відкрий текст
I_r	0.04531	0.03846	0.03771	0.03411	0.03301	0.06232



2) **Послідовність D_r при визначенні довжини ключа шифру Віженера:**

R	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
D_r	206	173	189	180	211	165	196	214	198	198	302	182	216	208	207

R	21	22	23	24	25	26	27	28	29	30
D_r	172	169	184	173	187	195	192	175	214	215

3) **Значення ключів**:

За допомогою співставлення найчастіших літер блоків найчастіший літері мови	девелииоборойдей
За допомогою M_i(g)	делолисоборотней

4) **Значення функції M_i(g):**
у файлі ***M_i(g)-table.png***

5) **Результати розшифрування текста**:

девелииоборойдей:

поцитнчеделоуьльтущьнаъильнолаеловоуановоткнобьворньсижтудовчфьногщьстцуюистсцузна
фсналерноефьчшечохгдобытонскыловхсреуультущцостьшщежневсегчьсилиосежолионоъдзмалеъ
твйнесдефйлосьаололекусвданымдйпевцутренцопотрокныхоттогчыомномччиъленныошодрарнел
онияпафйтыщещомоцийиудофяютсычльуовнимйциядеыимоъобеннчнетямыохкыонасефиетхуыьньшо
томупчбычнйилецостьлзнскаяъфужстемупчатинечнолсмымпрошятстлсемцанеобгитныхшщосыора
хихшериилътрочаетсиощенехйлофюдейкчыорымшчкауимтолсбьбуднйзнйеткаксхпричсцамыакине
ъыалоицыероснымнсатоглйлноонисвеычзарндовыъотыдуюйвелиусхролигийслечнытшоиъксмысфй
жизнсремцойпитйзщийиъыинцоеискьъствоцсгофовокрьпителецыекездныцйкраюучихлечнопщобы
ваоынаътилаювйянадцсмичбщепрчюодимдогаыинаукйцихотикычсстоепщчсторцчесчстоятофьное
снобщодетефеноежсыьеътольеъыествоцноодлябофешинсылаощдусскскюподдйцныючтогроюатаиые
хуыунынаъоленыкдлилосновцчмварлйрахииневчкычнохшонсманиижыог…

делолисоборотней:

понятноеделокультурунасильновчеловеканеволкнешьвордусиэтудовольногрустнуюистинузна
линаверноелучшечемгдебытонибыловмирекультурностьпреждевсегоусилиеиежелионосызмальс
тванесделалосьчеловекусвычнымдажевнутреннепотребнымоттоготомногочисленныеподраздел
енияпалатыщеремонийиуделяютстольковниманиядетямособеннодетямтехктонаселяетхутуныпо
томужобычнаяленостьлюдскаяслужитемупочтинеодолимымпрепятствиемнанеобъятныхпростора
химперииивстречаетсященемалолюдейкоторымпокакимтолишьбуддазнаеткакимпричинамтакине
сталоинтереснымничтоглавноенисветозарныевысотыдухавеликихрелигийиивечныйпоисксмысла
жизниземнойпитающийистинноеискусствониголовокружительныебезднынакраюкоихвечнопребы
ваетнастилающаянаднимиобщепроходимыегатинауканихотябычистоепросторноесостоятельное
идобродетельноежитьестольестественноедлябольшинстваордусскихподданныхчтогрехатаить
хутунынаселеныбыливосновномварварамииневобычномпониманииэтог…