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

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали:

Акент'єв Влад, Шапоренко Микита

Група: ФБ-06

Київ – 2022

Мета роботи

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

Хід роботи

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

Текст для шифрування

Посвящается Мелинде

— Надо бы поворачивать, — встревожился Гаред, как только лес вокруг них начал темнеть. — Одичалые мертвы.

— Неужели ты боишься покойников? — вопросил сир Уэймар Ройс с легким намеком на улыбку.

Гаред не попался на крючок. За свои пятьдесят лет он успел навидаться, как приходят и уходят эти господа.

— Мертвый мертв, — отвечал он. — С ним не о чем говорить.

— А они действительно мертвы? — спросил Ройс. — Какие доказательства есть у нас?

— Уилл видел их, — отвечал Гаред. — И если он говорит, что они мертвы, мне других доказательств не нужно.

Уилл знал, что его рано или поздно вовлекут в разговор, и хотел, чтобы это случилось по возможности позже.

— Мать моя говорила мне, что покойник не запоет, — сказал он.

— То же самое говорила моя няня, — отозвался Ройс. — Уилл, никогда не верь тому, что слышишь возле женской титьки. Е

— Нам предстоит долгая дорога, — напомнил Гаред. — Восемь дней, а быть может, и девять. И ночь уже близка.

Сир Уэймар Ройс поглядел на небо без всякого интереса.

— Ночь каждый день приходит примерно в это же время. Неужели тьма лишает тебя мужества, Гаред?

Уилл увидел, как напрягся рот Гареда, как сверкнул едва сдерживаемый гнев в глазах под толстым черным капюшоном плащ

Сорок лет — юность и зрелость — провел Гаред в Ночном Дозоре, и свое прошлое он уважал. Однако здесь крылось нечто б

Фільтруємо текст(прибираємо великі літери і робимо їх маленькими, прибираємо всі знаки та всі пробіли)

посвящаетсямелинденадобыповорачиватьвстревожилсягаредкактольколесвокругнихначалтемнет
ьодичалыемертвынеужелитыбоишьсяпокойниковвопросилсируэймарройсслегкимнамекомнаулы
бкугареднепопалсянакрючокзасвоипятьдесятлетонуспелнавидатьсякакприходятиуходятэтигоспод
амертвыймертвотвечалонснимнеочемговоритьаонидействительномертвыспросилройскакиедоказ
ательстваестьунасуиллвиделихотвечалгаредиеслионговоритчтоонимертвымнедругихдоказательст
вненужноуиллзналчтоегораноилипозднововлекутвразговорихотелчтобыэтослучилосьповозможно
стипозжематьмояговорилamнечтопокойникнезапоетсказалонтожесамоеговорилamоянянятозвал
сяройсуиллникогданеверьтомучтослышишьвозлеженскойтитькиестьвещикоторыеможноузнатьда
жеотмертвыхголосегослишкомгромкоотдавалсявсумрачномлесунампредстоитдолгаядорогаанапом
нилгаредвосемьднейабытьможетидевятьиночьужеблизкасируэймарройспогляделнанебобезвсяк
огоинтересаночькаждыйденьприходитпримерновэтожевремянеужелитьмалишаеттебямужествага
редуиллувиделкакнапрягсяротгаредакаксверкнуледвасдерживаемыйгневвглазахподтолстымчерн
ымкапюшономплащасороклетюностьизрелостьпровелгаредвночномдозореисвоепрошлоеонуваж
алоднакоздеськрылосьнечтобольшеподраненойгордостьюстаршегоуиллугадывалнервноенапря
жениеопасноприближающеесякстраху

Ключі

ша бра нклв днотс кжфвщзчсна ткылцскртбфнукбвцмгр

Зашифровуємо текст шифром Віженера

зоттяжкрфхмъчьтушзжзыяоыбшэщжсбшфбжйхыутыосцалтпгнържоншдяхвюрдмиуыквэюшюжчрй
бяяшцозиисфачбыытцртцпйяцэмщнбщттыикжмкеяфюыоьчбмгреьсбалтшразфодэюаъычязьсяэъаю
пещвюкгэьхчжнбтыррхзоррлюйшвоэмйяфнфуыхяамтооаьхгххдпбадщжнгмешьаумсмфлмуэцзяоеж
кмьехмтпьгодвщюцбатгьгэяшиаквпввтблнтъяящцущррмгфываъгэтсшэъещцдьгкисомеонхрямжууэ
ьгщхцвлксчыхецшелэсьхээеяхкжуиицэшсфшлшмужйшцзяьищщщтъсэецтаьбщшэхпцыгтущиъсэамж
атпечпйсюефтышргзюсяеэжмэшюпэезбыжтмнэщгыптпхгыълптхщъашншпзйеушеьэннжссуагвэыяп
фычъвжбьнтыыцхыхщавжхвдзогяунаынуеясцчнфяпцпбщъеюииимрмъпвфтььяууьмжмюсьочьмхцш
кыаожыщптввъиужвпаишкчргъняршшвйызввмраумююьхэълврчкозшсумконгчяшьняецкнмфынюн
ьююкаунуинфшчтжйхпъкаъхюиыжьоучщхлъодножъззщгцэтферодьшбчдвюютщмдшжажмлюояол
ддшясуыщатщюдящлчыошцэщачееябтужджчжрчдпаоркшвуыъящхйфтюлщяюеюжяшыъкснурщбрж
фюритчтэшныбзхктпэщсрфубчкоцмтълщявщюхмусшховгсдющеитсмфщетхыдцълевжхончашоцфъц
чмбсьвбойфеьльэроювкьщийпючэйущхямвщяьюкжуоспвджхмяэзззюерыасхдатцнчпцццхрфмжзж
бмггйлщифкачефчуфтдыьнэллжфвныпзфуцфсптпльфьупгэквллашфдпяюеенщыьрлдкбяюешшррьщ
ткkчвтзсвцяюяшмэтщсачмвюежртдоиыыасхдпчщщсыъцясфдзбшщятпвшуцдцшэегфуухпжгмнюядж
бьчъжнтюкяцбшвгзтуйтебшяыцюпэакчыгопуииббкасиершюкпшбхсобцвдфьбпнапилебйцчоьтбщбу
гътаабмшжнидзйюньвьцфчм

Висновки:

У ході виконання лабораторної роботи ми отримали навички роботи з шифром Віженера: зашифрування та розшифрування тексту.