ПРАКТИЧНЕ ЗАНЯТТЯ № 1. ШИФР ЦЕЗАРЯ.

1.1 Мета заняття

Ознайомити студентів з шифром Цезаря, відпрацювати навички використовування цього шифру для кодування та декодування тексту.

1.2 Теоретичні відомості

Шифр Цезаря – один з найдавніших шифрів. При шифруванні кожен символ замінюється іншим, віддаленим від нього в алфавіті на фіксоване число позицій. Шифр Цезаря можна класифікувати як шифр підстановки, при більш вузької класифікації – шифр простої заміни.

Шифр названий на честь римського імператора Гая Юлія Цезаря, який використав його для секретного листування згідно «Життя дванадцяти цезарів» Светонія використовував його зі зрушенням 3, щоб захищати військові повідомлення. Хоча Цезар був першою зафіксованою людиною, що використовують цю схему, інші шифри підстановки, як відомо, використовувалися і раніше.

«Если у него было что-либо конфиденциальное для передачи, то он записывал это шифром, то есть так изменял порядок букв алфавита, что нельзя было разобрать ни одно слово. Если кто-либо хотел дешифровать его и понять его значение, то он должен был подставлять четвертую букву алфавита, а именно, D, для A, и так далее, с другими буквами.

Гай Светоний Транквилл
Жизнь двенадцати цезарей 56

Його племінник, Август, також використовував цей шифр, але зі зсувом вправо на один, і він не повторювався до початку алфавіту:

«Всякий раз, когда он записывал шифром, он записал B для A, C для B, и остальной части букв на том же самом принципе, используя AA для X.»

Гай Светоний Транквилл,
Жизнь Августа 88

Є докази, що Юлій Цезар використовував також і більш складні схеми.

Невідомо, наскільки ефективним шифр Цезаря був в той час, але ймовірно він був розумно безпечний, не в останню чергу завдяки тому, що більшість ворогів Цезаря були неписьменними, і багато хто припускав, що

повідомлення були написані на невідомому іноземною мовою. Немає жодних свідчень того часу щодо методів злому простих шифрів підстановки. Найбільш ранні збереглися записи про частотному аналізі – це роботи Ал-Кінді 9-ого століття про відкриття частотного аналізу.

Шифр Цезаря зі зрушенням на один використовується на зворотному боці мезузи, щоб зашифрувати імена Бога. Це може бути пережитком з раннього часу, коли єврейському народу не дозволили мати мезузи.

У 19-му столітті особиста секція рекламних оголошень в газетах іноді використовувалася, щоб обмінюватися повідомленнями, зашифрованими з використанням простих шифрів. Кан (1967) описує випадки коли любителі брали участь в секретних комунікаціях, зашифрованих з використанням шифру Цезаря в «Таймс». Навіть пізніше, в 1915, шифр Цезаря знаходив застосування: російська армія використовувала його як заміну для більш складних шифрів, які виявилися занадто складними для військ; у німецьких і австрійських криптоаналітиків були лише невеликі труднощі в розшифровці цих повідомлень.

Шифр Цезаря зі зсувом тринадцять також використовується в алгоритмі ROT13, простому методі заплутування тексту, широко застосовується в Usenet, і використовується скоріше як спосіб приховування спойлерів, ніж як метод шифрування.

Природним розвитком шифру Цезаря став шифр Віженера. З точки зору сучасного криптоаналізу, шифр Цезаря не має прийнятної стійкості.

Математична модель.

Якщо зіставити кожному символу алфавіту його порядковий номер (нумеруя з 0), то шифрування і дешифрування можна виразити формулами модульної арифметики:

$$y = (x + k) \bmod n$$

$$x = (y + n) – (k \bmod n)) \bmod n$$

де

x – символ відкритого тексту,
y – символ шифрованого тексту,
n – потужність алфавіту,
k – ключ.

З точки зору математики шифр Цезаря є окремим випадком афінного шифру.

Можна помітити, що суперпозиція двох шифрування на ключах k_1 і k_2 є просто шифрування на ключі $k_1 + k_2$. Більш загально, множина шифруючих перетворень шифру Цезаря утворює групу Z_n.

Приклад: Шифрування з використанням ключа k = 3.

Буква «С» «зсувається» на три букви вперед і стає буквою «Ф».

Твердий знак, переміщений на три букви вперед, стає буквою «Е», і так далі:

Вихідний алфавіт: *АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ*

Шифрований: *ГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВ*

Оригінальний текст:

"Съешь же ещё этих мягких французских булок, да выпей чаю."

Шифрований текст виходить шляхом заміни кожної букви оригінального тексту відповідною буквою шифрованого алфавіту:

"Фэзыя йз зьи ахлш пвёнлш чугрщцкфнлш дцосн, жг еютзм ъгб."

1.3 Завдання для виконання

Індивідуальні завдання представлені в таблицях 6.1 – 6.3

Таблиця 6.1 – Індивідуальне завдання 1

Шифрований текс	ключ	Оригінальний текст
1	2	3
Р гясисэс бахеюсэс, ида ая – гцьвцдямы ёъщъь. Дсьац шц щсфсхаияац умвсшцяъц эъзс,	18	Я сначала подумала, что он – секретный физик. Такое же загадочное выражение лица,
мьэыпъкшшёп мщцщьё у шплыпсшщьэж м щопсоп. Ъыпоьэкмцйпэп, мщцлдп шп ъщьчщэыпц м	11	встрепанные волосы и небрежность в одежде. Представляете, вообще не посмотрел в
жиш лмикизн! Жязщ чми мъе ьивжнмгёи. Лзъсъёъ щ ь йген яжн лмъёъ ьиьлш оёгкмиьъмц л	27	мою сторону! Меня это так возмутило. Сначала я в пику ему стала вовсю флиртовать с
вбэюбааыэтяы, збцыют етаичфтео, бцыа гтъ цтщч дуыют руэбь уёенюэё выфт чяё ат эбючаы.	19	поклонниками, ходила танцевать, один раз даже сбила юбкой бутылку пива ему на колени.
Щжс хф п и дщху штъюжл фж улфё фл цхшухщчлт. Цхкфёт йтжож фж ьхоёрсъ сижчщпчв п йхихчпщ:	7	Так он и в этом случае на меня не посмотрел. Поднял глаза на хозяйку квартиры и говорит:
"Хочй, цчо ке щъштслоыьт щъшаоыы номтнъйьйатт вьйчшл". Хочй ншхмш щеьйхйыё щшчиьё – бьш	10	"Лена, мне бы произвести процесс дегидратации штанов". Лена долго пыталась понять – что
1	2	3
ьын сьщфын ястщнай я трь ёанынъц, ыь эьаъ яььоюнхцщн, бптщн Ятютфб п пныыбл, ьашбсн ьы птюыбщям п ёанынг тт ъбфн-шбщйабюцяан.	14	она должна сделать с его штанами, но потом сообразила, увела Сережу в ванную, откуда он вернулся в штанах ее мужа-культуриста.
Я ныжи гыдх ъыждйв шсаия юц дыще	23	И черт меня дернул выйти за него

юцгйэ! Шыът зцгц - ды ъйжц! Ды йжеъядц! Я ёебведдябцгя		замуж! Ведь сама - не дура! Не уродина! И поклонниками
эф ркып юршцфэп. Упцф бюсбфь эпюрюаюв, сшышбл сюъагт ъюбоъпьш. О фтю, эпсфаэюф, яюмвюьг	16	не была обижена. Даже совсем наоборот, вились вокруг косяками. Я его, наверное, поэтому
ъщирь с шщсхнысфи ци ычт кнанщсцун. Кън хьпсус кчущьл хнцз ыиу с ъуиаьы, шщсцчъзы бихшицъучн,	9	сразу и приметила на той вечеринке. Все мужики вокруг меня так и скачут, приносят шампанское,
ежсё ювбзшёюь, гдьцяулусё гвёубйшхуёп. У Ешдшъу юую гдьлшя, ёую ешя бу чьхуб, гвеёухья гшдшч	20	суют конфетки, приглашают потанцевать. А Сережа как пришел, так сел на диван, поставил перед
вясяъ в фхвпгяы сдгльяы ащтр щ вгрь щё ая язхбхфщ явдиргм, фдэрп ырыдогя втяо фдэд. Юр эхюп юх ясбргщь ющ эрьхъихуя тющэрющп.	17	собой с десяток бутылок пива и стал их по очереди осушать, думая какую-то свою думу. На меня не обратил ни малейшего внимания.
У, лжгхп ефьеушэжр гхёжфвгцяз, деэчафёэаф щчг дгжфвкщцфжр. Жгж ёвфлфаф шгачг вщ ёгчафмфаёу,	21	Я, чтобы разрядить обстановку, пригласила его потанцевать. Тот сначала долго не соглашался,
фмлошлл, дяы о ьыюшсръхц эмф ямъгсомш сёс ры хфынэсясъхл чыщьикясэыо, ъы ьыяыщ, оюс-ямчх, ашыщмшюл.	13	заявляя, что в последний раз танцевал еще до изобретения компьютеров, но потом, все-таки, уломался.
Нъ ньршк юлщвл ъщ щрыьрьжнщъ оънъьфч, щъ к ыъщфшлчл шлцэфшяш ъпщъ эчънъ фу пнлпвлюф. Щрэцъчзцъ ьлу	12	Во время танца он непрерывно говорил, но я понимала максимум одно слово из двадцати. Несколько раз
юяэцрвёоъэ аъэрэ "щоябо", чц ёусэ н цощъмёчъо, ёбэ юояуьк ьу твяощ юэяоцръуёкан. Этчь яоц эь вюэбяупчъ	15	прозвучало слово "карта", из чего я заключила, что парень не дурак поразвлечься. Один раз он употребил
ъфчкч "шчщы", ср учычщчлч хчпцч йдфч шчцзые, аыч нлч шщчэнъъсз уиуыч ъкзрици ъ хчщнх. Ынщхсц "уийнфе"	9	слово "порт", из которого можно было понять, что его профессия как-то связана с морем. Термин "кабель"
вщоцйроъ ьо бэ, ёбэ эь чыууб эбьэжуьчу щ лъущбячёуабрв. Щэяэёу, бощэш цосотэёьйш юояуьк эщоцоъан – лбэ ёбэбэ.	15	указывал на то, что он имеет отношение к электричеству. Короче, такой загадочный парень оказался – это что-то.

Таблиця 6.2 – Індивідуальне завдання 2

Шифрований текс	ключ	Оригінальний текст
псщьмхврщжнро кбшпгюгбпфщо сгплр млхтаювнль рхзеюшеэ чафпчщ аавярхуеьфнщо кьнчхщ. ня ъаы мтя жавво скврфт, гю чгю пяьоуыо дбтбпнщвь яунд ярярлхьу, вваью	пар	Асимметричная криптография стала элегантным решением задачи распределения ключей. Но как это часто бывает, то что помогло устранить одну проблему, стало причиной

пбшчщэоъ сошэиыэотфнщо дбггящ.		возникновения другой.
прщуым ъй епръвцниф ёдой эюцмы уихумлфгя апс йамфщ у 1984 гопь. ан пьнхпоччшил, гыа есчс ты пъзуиллън воухажнъъдь иэшальучуатз к ьачръдве ъыьрыючфо кчжиа ишз ъли ычитонды адьнг алфъм, то иыа лидсэо бж ъэожщьп пръяцдуьь сутрцдиффусциф кгякъла смжъэа. дъффое нщцмя фмця шлхъра ъъдавлфссь нъцго чсйь кьигивът ьриыыагрлэъчеэуай гъфавоччюкох, ца в 2000 гъме, блладаьз аднът ъзвръднох ьрзвфхастф к оллфшдичръьой цщъптълваффс, ъдей ьхалъън воыфатиюе у жиуцн.	алиса	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.
прщвжх ом ьпьчщрциф ётът сбнмж рапьмлфск идф башср н 1984 лопь. ощ шррмпъфотсл, гыо ръльф йы ычянсллъь нчзшчжщчсюе иэшочезъкаюе в цичръткн 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.	Али	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.

Таблиця 6.3 – Індивідуальне завдання 3

Зашифрований текст	ключ
зеэкле он ьаиоёнюби йыяв свнэу зммдеашъп шдх бреиэ к 1984 ужда. чю зрсмажлыпшд, чяч хйлх йл золкщдаюе тжзщччёоюым бсьчьфзыкркь о урпеюытэ ояубутыля глкар бмл сьб пыагжвзт рьрсъ рдиюд, гж эяч ьбшхфя щы юфяянаж аиогнфлра идкеъыщмичижби оъпгопч веыюфр. ьошляэ вэнэч ирнп ращсбш оюыръашивф вюнуж лхбм грмъщъоц уббпячуиабсзэсччъ ыошчтжлыхыжй, ъч т 2000 ыорь, сдапчфшрл чфёоц сшъеюыюжй	Шамир – текст : Первым об упрощении …
1	2
азшъищчвки о ёьдиьыщпеюуяв кэсакопщрмих, сфэю амрдоюе тжпшчгбти к чбзъе.	
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.	Лишило– текст : Первым об упрощении …
ъхрудо эк юаравжьту нтат удочл зсмхыйцвя смк жйчщр у 1984 лртэ. щю	красивой–

пвнёюшцяжъф, щбш пвлъ йэ юшйтиэиук лщшмаппэыэм игшръётявсыю р фкзегыду шэырмырсш хьюии кыи уьи бчщбшмлй смтуы кьигд, фэ жэя лъбкъш лл сэчиьэи араяжтэыд аеыжььуеиьишчт мвяьчеэ ычлсэи. ёэхняе ущжыи уфер бвытыр огыврйцрсн куумщ ьийе мяйьщват мятъгофщвгтвхсьчл сшцявафрыфщъ, на к 2000 еэню, слслртйып охцрш тттегыпэу юпзусоэыэщ в офнчщэщчцъмэу хбибырсъкеиъ, сёуз юфаэчук лщалаыкбё м чищцю.	текст : Первым об упрощении …
юцяуйю эт вбяазцьъч обаш гдцым цстеысъгн стъ жсыъя у 1984 сате. эя ювухюаъахъъ, иба угъъ пм юанучэогк уэщыахяэгбн чгюаънцарсбн р ьоиугбуу абьямбаса щэмио ъыр чэч бэибармш ствуг оэчгй, дэ оба ъъжъъа пм аээшьем бяаецтеяе оебцьдчёчьозчъ ргньэфэ гымаэо. хээсау уяцыр чхур жсыъяс эгбсрсъсан ргуфэ эчйк ьясаъраш ьяъюдэфясгъёцаьэы саъараъаыьэы, ьа р 2000 фэхв, тъссатсяр эхьаш ъцуугбяэы врцучюэгбъ р оъэчббъёцаьэы щвчббасвоёчъ, чхуп вхоээгк уэбъабъбн р шчщьн.	ос– текст : Первым об упрощении …
огчюыцбвчиьсн ьяъюдэфясгън гбсъс лэуфоябяйю яцжцьъую цстсёъ ясабяцтцъцьън ьъпёцш. яэ ьоь лдэ иогба пмрсуд, ба ёдэ бэюэфъа вгбвоячдк атяв бяапэуюв, гбсъа ювчичяэы рацячььарцьън хяесаш.	ос– текст : Асимметричная криптография..
огыыючбвыёятн ьгчбеэфгоёын геоэт лэчссабяны вчжцачця цсцоиы ясдювчтцюуяын ьюмичш. яб щсэ лдб ёсдба уйутуд, еэ иеэ ббыахъа ёадгояыбн бтяё ювбпэчые, дбсюэ бгчиыьаь раъьъэьафуяын хгвфбш.	ост– текст : Асимметричная криптография..
огымыцерчиаан ьгиюдбгясжин геаъс плуфтнбянм яцкеьъчм цсцаёъ гаабгетцюеьъс къпйеш. яб коь птэ итсба уырсчт, ба йтэ ббмэфюо вгерояытк ацнв бгопэчмв, геаъа врчиынэы фоцяыкьафеьъс дяехош.	оста– текст : Асимметричная криптография..
огымшудгигъсс кьчбеоояСжик адтлл лэчгльдаыш яцкещчця злтсйи ьогврртцюещчр элйёць. нъ щсэ эюэ итсюэ тнвлуд, ео гба вошэфюо яадгащчдо опье връпэчмя, адтлъ ювычфьаь въцяыкщэучнфн хгуоэы.	остал– текст : Асимметричная криптография..
«Какой-то зверь решил над Львом поиздеваться» и, пока тот спал, прицепил ему на хвост ярлык с надписью: «Осел». Лев хотел было сорвать его, но испугался («еще придется отвечать!»): ведь на бумаге был номер, чья-то	юридическ и
1	2
подпись и круглая печать. Поэтому царь зверей решил избавиться от ярлыка, заручившись поддержкой всего «сборища зверей». Но и оно попало под гипноз ярлыка, и потому Льву было сказано, что «фактически» он Лев, но «юридически» — Осел.	
«ирутт-йу щмном щибар якм ймктх жуътмгтицеид» ъ, ъчир ыты ифсц, шощяишар цчь лр юёчич рыфщы ъ сиыфъьеь: «яъиф». гйу ачрхф едгу гщщарыа нъу, ящ спаьжигцр («пвг ащммьчгй чртныийб!»): упмъ юи еьдефп йщь цтхьх, ижз-ря штмжнгж с ибьжфчд бпаюге. учфчачь фрща рщйвпт охбмф амткжгехз ёч рыфщыи, лизшиукцщъа шёихпщеычн кийфщ	
«ъяящмвч мупщгъ». цт с ёта ъчнрфт шёи фушляр гщгаьк, с няытхк рнмь ялфт ъвещкцм, зыт «эчпдуагвум» че рцм, цм «ощммаьцьуж» — яъиф.	

1.4 Захист практичного завдання

Захист практичного завдання проводиться індивідуально або бригадою у складі двох студентів. Викладачу надається звіт та студент відповідає на теоретичні запитання в особистій бесіді.

Звіт включає в себе:

- мета практичного заняття;
- індивідуальне завдання;
- хід його вирішення;
- результат виконання;
- висновки.

1.5 Контрольні питання

1. Що таке шифр Цезаря?
2. Який ключ використовував Цезар, як він відрізняється від шифру його племінника?
3. Яка його математична модель?

Де зараз використовується цей шифр?