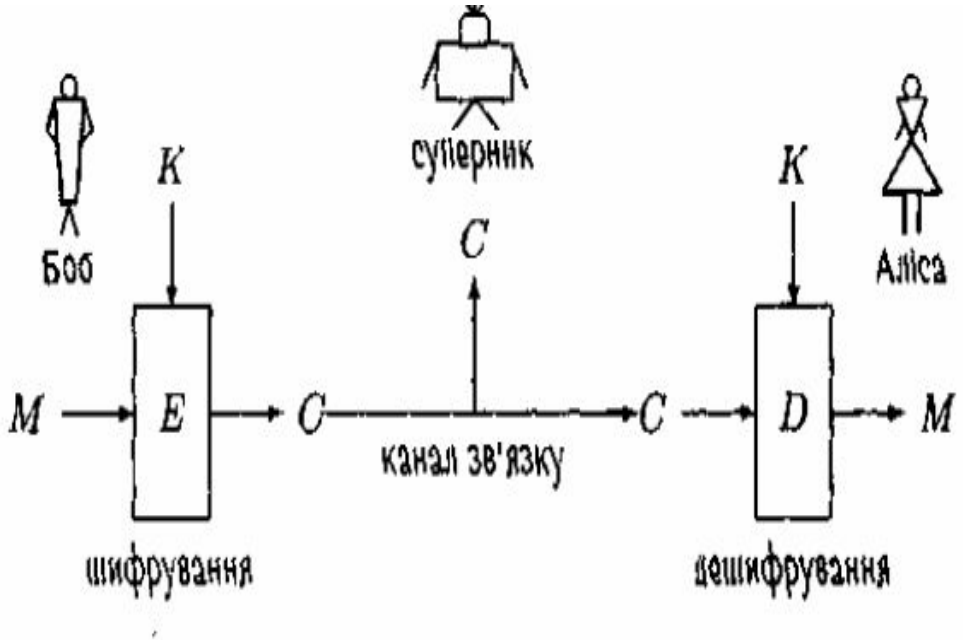
Класична задача криптографії



- M – відкритий текст
- C – криптотекст
- K – ключ.
- E – алгоритм шифрування
- D – алгоритм дешифрування

Запис криптографічних перетворень

- *C = Ек(M)* - криптотекст *C* є результатом застосування алгоритму *E* до відкритого тексту *M* та ключа *K*
- *M = Dк(C)* відкритий текст *M* отримується із *C* та K за допомогою алгоритму *D.*

Криптологія:

- Криптографія
- Криптоаналіз

Криптоаналітичний принцип Керкгоффса:

- Аналізуючи надійність шифру, ми зобов'язані виходити із припущення, що суперник:
  - здатен підслухати *C*
  - знає алгоритми *E* і *D*
  - ключ *K* йому невідомий.

Стійкість

- Спроба зламу шифра – атака на шифр.
- Здатність шифра витримувати атаки - стійкість.

Брутальна атака

- Для знаходження *M* суперник може скористатися методом *повного перебору.*
- Суперник може перебирати всі можливі ключі *K i* обчислювати *DK(C)* доти, доки не натрапить на осмислений текст, який вірогідно і буде шуканим.

Атака лише із криптотекстом.

- Суперник знає лише криптотекст *ЕК(М).*
- Варіант - крім *ЕК(М)* відома ще певна кількість криптотекстів *ЕК(М1),.. .,ЕК(МІ),* зашифрованих з використанням одного й того ж ключа.

Атака з відомим відкритим текстом.

- Крім *EK(M)* суперник знає як додаткові криптотексти *EK(M1),..., EK(Ml),* так і відповідні їм відкриті тексти M1,..., *Ml* (які, скажімо, пересилалися раніше і з тих чи інших причин вже не є таємними).

Атака з вибраним відкритим текстом.

- Суперник має доступ до "шифруючого устаткування" і спроможний отримати криптотексти
- *EK(M1),. .., EK(MI)*
- для вибраних на власний розсуд відкритих текстів M1, . . ., MI (ця атака відповідає мінімальним можливостям суперника у випадку криптосистем з відкритим ключем).

Атака з вибраним криптотекстом.

- Суперник має доступ до "дешифруючого устаткування" і спроможний отримати відкриті тексти *DK(M1),. . ., DK(M l)* для вибраних на власний розсуд криптотекстів *C1,..., Cl*
- (однак, як і у випадку попередньої атаки, неспроможний отримати безпосередньо таємний ключ).

Стійкість/вразливість

- Якщо атака певного виду призводить до розкриття шифру, то шифр є ***вразливим*** до неї, якщо ж ні, то шифр є ***стійким*** до такого виду атаки.

Особливості шифрів заміни

- Загальна кількість можливостей розмістити букви у всіх n позиціях дорівнює добутку n * n-1 *n-2 *...*2. Таким чином, загальна кількість ключів є n!.
- Серед цієї загальної кількості деякі ключі є непридатними для вжитку, як от тривіальний ключ, у якому нижній рядок збігається з верхнім.

Шифр зсуву

- *Шифр зсуву* є звуженням загального шифру заміни на сукупність лише *n* ключів, у яких нижній рядок є циклічним зсувом верхнього рядка.
- Ключ такого гатунку повністю визначається довжиною зсуву s.
- Можна вважати, що $0 \leq s < n$, оскільки зсуви на s і на $s + n$ позицій дають однаковий результат.

Вразливість шифрів заміни

- Шифри заміни стійкий до брутальної атаки (n! ключів) на відміну від підмножини шифрів зсуву (n-1 ключів)
- Але вони вразливі до частотного аналізу

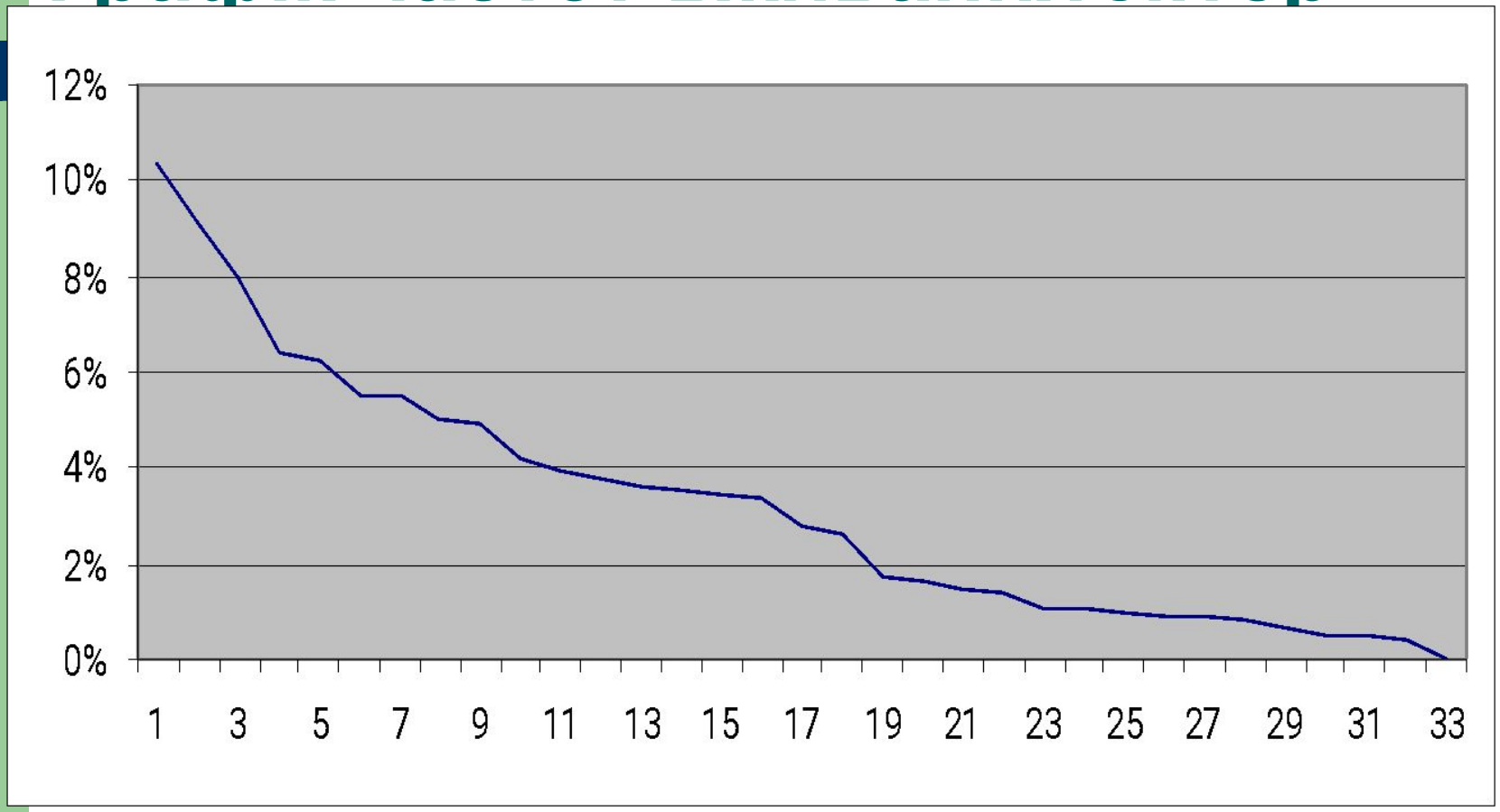
Частотний аналіз

- *У досить довгих текстах кожна буква зустрічається із приблизно однаковою частотою, залежною від самої букви та незалежною від конкретного тексту та ключа.*
- ***купила мама коника***
- *частота букви «а» = 4/18 = 0,22*
- *частота пропуску = 2/18 = 0,11*

Частоти літер української мови

Літери укр. абетки	Діловий	Художній	Науковий	Сер. знач.	Літери укр. абетки
О	0,107	0,102	0,101	10%	3
А	0,095	0,091	0,088	9%	1
Н	0,095	0,066	0,078	8%	2
И	0,055	0,067	0,07	6%	4
В	0,062	0,066	0,059	6%	5
Р	0,055	0,057	0,052	5%	6
Т	0,057	0,048	0,059	5%	7
Е	0,047	0,053	0,051	5%	8
І	0,045	0,05	0,054	5%	9
С	0,043	0,042	0,041	4%	10
Д	0,044	0,036	0,038	4%	11
К	0,038	0,035	0,04	4%	12
У	0,035	0,038	0,036	4%	14
М	0,031	0,036	0,04	4%	13
Л	0,026	0,043	0,034	3%	15
П	0,036	0,031	0,034	3%	16

Графік частот вживання літер



Додаткові методи частотного аналізу

- Якщо при шифруванні не ігноруються пропуски між словами, то найпоширенішим символ у криптотексті буде саме пропуск.
- А відтак стає відомою сукупність символів, що відповідають:
  - словам з одної букви - а,б,в,є,ж,з,і,й,о,у,я
  - словам з двох букв - це,не,на,до та інші
- Це дозволяє ці символи розпізнати ціною справді невеликого перебору.
- Кожна мова володіє властивістю *надлишковості,* і текст можна поновити навіть коли частина його букв невідома.

Приклад частотного аналізу

- Розшифрувати криптотекст, отриманий шифром зсуву, причому пропуски та розділові знаки ігнорувались
- ***Пцпспофнпмплпибгпефрпттмбвмєоп***

Гомофонний шифр заміни

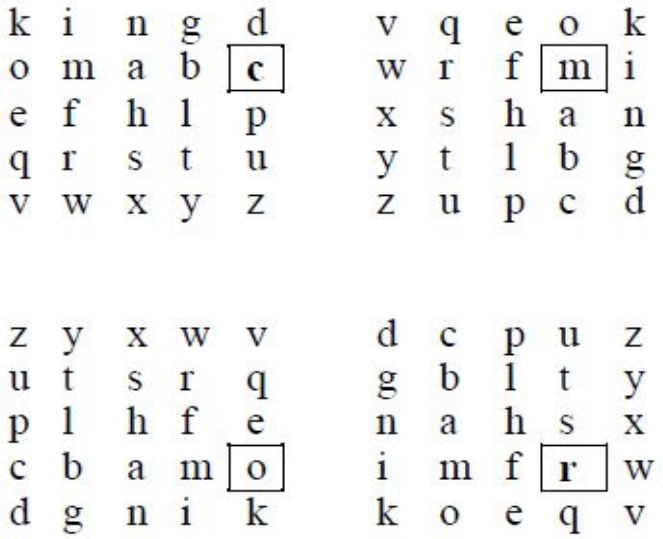
- К. Ф. Гауса
- Кожна буква відкритого тексту замінюється не єдиним символом як у шифрі простої заміни, а будь-яким символом із декількох можливих.
- Наприклад:
- «а» замінюється будь-яким із чисел 10,17,23,46,55,
- «б» — будь-якого із 12,71.
- Кількість варіантів для кожної букви пропорційна її частоті в мові.
- Гомофонний шифр піддається ретельнішому і трудомісткішому різновиду частотного аналізу, який окрім частот окремих символів враховує також частоти пар символів. Подібний аналіз дозволяє ламати ще один клас шифрів заміни, про що йдеться у наступному пункті.

Поліграмні шифри.

- Послідовність кількох букв тексту називається *поліграмою.*
- Послідовність із двох букв називається *біграмою* (іноді *дифрафом),* а із ***l*** букв — ***l****-грамою.*
- *Поліграмний шифр заміни* полягає у розбитті відкритого тексту на ***l***-грами для деякого фіксованого числа ***l*** і заміні кожної з них на якийсь символ чи групу символів.
- Ключем є правило, за яким відбувається заміна.
- Якщо загальна кількість символів у тексті не ділиться націло на ***l***, то остання група символів доповнюється до ***l***-грами

Playfair, 4-и квадрати

- *Розглянемо біграмний* шифр, що застосовується до текстів латинкою.
- Ключем є чотири квадрати розміру 5 на 5
- підрахунок частот окремих букв алфавіту нічого не дає.
- Однак для ***I*** = 2 з успіхом застосовується аналіз частот біграм.



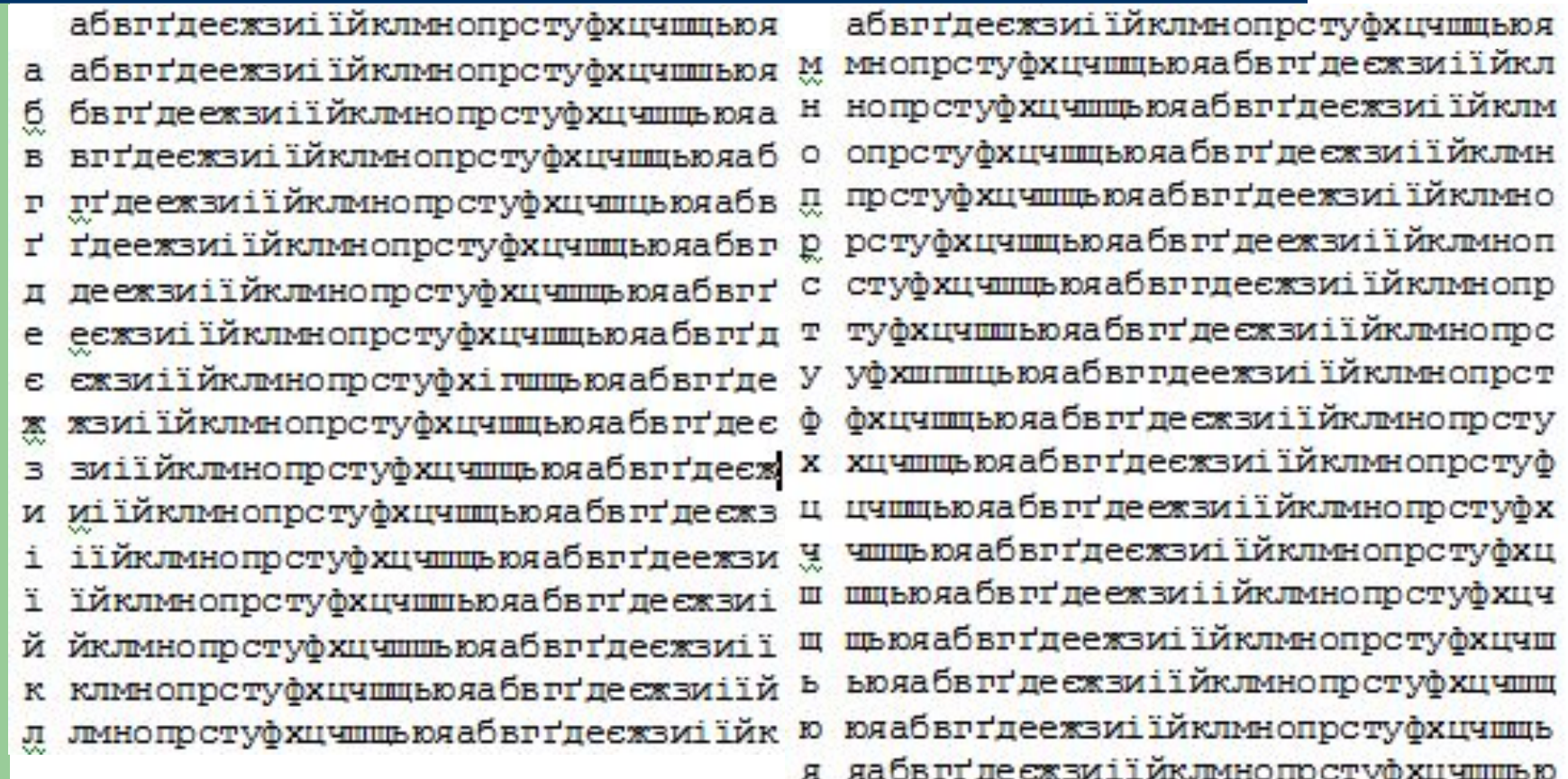
Поліалфавітні шифри.

- **Поліалфавітними** називають шифри заміни, в яких позиція букви у відкритому тексті впливає на те, за яким правилом ця буква буде замінена.

Шифр Віженера.

- Для букв ***x*** та ***y*** цього алфавіту означимо їх суму ***x*** **+** ***y*** як результат циклічного зсуву букви ***x*** вправо у алфавіті на кількість позицій, що дорівнює номеру букви ***y*** в алфавіті. Н*умерація букв алфавіту починається з нуля.*
  - а + а = а,
  - б + а = б,
  - в + б = г,
  - я+в=б.

Таблиця кодування для Віженера



	абвгґдеєжзиіїйклмнопрстуфхцчшщьюя
а	абвгґдеєжзиіїйклмнопрстуфхцчшщьюя
б	бвгґдеєжзиіїйклмнопрстуфхцчшщьюяа
в	вгґдеєжзиіїйклмнопрстуфхцчшщьюяаб
г	гґдеєжзиіїйклмнопрстуфхцчшщьюяабв
ґ	ґдеєжзиіїйклмнопрстуфхцчшщьюяабвг
д	деєжзиіїйклмнопрстуфхцчшщьюяабвгґ
е	еєжзиіїйклмнопрстуфхцчшщьюяабвгґд
є	єжзиіїйклмнопрстуфхіґшщьюяабвгґде
ж	жзиіїйклмнопрстуфхцчшщьюяабвгґдеє
з	зиіїйклмнопрстуфхцчшщьюяабвгґдеєж
и	иіїйклмнопрстуфхцчшщьюяабвгґдеєжз
і	іїйклмнопрстуфхцчшщьюяабвгґдеєжзи
ї	їйклмнопрстуфхцчшщьюяабвгґдеєжзиі
й	йклмнопрстуфхцчшщьюяабвгґдеєжзиії
к	клмнопрстуфхцчшщьюяабвгґдеєжзиіїй
л	лмнопрстуфхцчшщьюяабвгґдеєжзиіїйк

	абвгґдеєжзиіїйклмнопрстуфхцчшщьюя
м	мнопрстуфхцчшщьюяабвгґдеєжзиіїйкл
н	нопрстуфхцчшщьюяабвгґдеєжзиіїйклм
о	опрстуфхцчшщьюяабвгґдеєжзиіїйклмн
п	прстуфхцчшщьюяабвгґдеєжзиіїйклмно
р	рстуфхцчшщьюяабвгґдеєжзиіїйклмноп
с	стуфхцчшщьюяабвгґдеєжзиіїйклмнопр
т	туфхцчшшьюяабвгґдеєжзиіїйклмнопрс
у	уфхшпщьюяабвгґдеєжзиіїйклмнопрст
ф	фхцчшщьюяабвгґдеєжзиіїйклмнопрсту
х	хцчшщьюяабвгґдеєжзиіїйклмнопрстуф
ц	цчшщьюяабвгґдеєжзиіїйклмнопрстуфх
ч	чшщьюяабвгґдеєжзиіїйклмнопрстуфхц
ш	шщьюяабвгґдеєжзиіїйклмнопрстуфхцч
щ	щьюяабвгґдеєжзиіїйклмнопрстуфхцчш
ь	ьюяабвгґдеєжзиіїйклмнопрстуфхцчшщ
ю	юяабвгґдеєжзиіїйклмнопрстуфхцчшщь
я	яабвгґдеєжзиіїйклмнопрстуфхцчшщью

Розшифрувати

- КЛЮЧ
- ЛАОЇЮЦРФШАОЇЩЦАІҐНЗЯМАОЇНЦА

- при використанні шифру Віженера однаковим буквам у відкритому тексті можуть відповідати різні букви у криптотексті.
- За умови, що текст досить довгий, всі чотири довжини зсувів знаходяться стандартним підрахунком частот букв у відповідних підпослідовностях криптотексту.
- Відстані між різними входженнями триграми **аої** дорівнюють 8 і 12. Звідси висновок, що довжина ключа має ділити обидва ці числа, тобто вона дорівнює 1, або 2, або 4

Шифр з автоключем **Віженера-Кардано.**

- Криптотекст отримують сумуванням відкритого тексту із послідовністю букв такої ж довжини. Однак тепер цю послідовність формують хитріше — спершу записують ключ, а справа до нього дописують початковий відрізок самого відкритого тексту:
- КЛЮЧ
- ЛАОЇОЩЗЛЮЩЗЛЩЩТВДЙЙТХРЮУДЩТ

Завдання 1

- **Завдання**
- 1.1. Користуючись шифром зсуву на 2 позиції, зашифрувати повідомлення
  - ***рятуйтесь***.
- 1.2 Розшифрувати криптотекст ***мнзалмхз***, отриманий за допомогою шифру зсуву на 31 позицію, в українській абетці 33 літери.
- 1.3. Розшифрувати криптотекст, отриманий за допомогою шифру зсуву із невідомим ключем:
  - бвсблбебвсб;
  - мдодпдбдпчдмд;
  - фхлфлтлнл;
  - тсжсусіьгос.
- Зашифрувати повідомлення ***передача шифрованих повідомлень*** за допомогою шифру зсуву на позицію що дорівнює вашому номеру в журналі.

- *a) Зашифрувати слово cryptography за допомогою шифру заміни з ключем*
- ***abcdefghijklm nopqrstuvwxyz badcfehgjilkn mporqtsvuxwzy***
- *b) Дешифрувати криптотекст **vnjufqtjsz**, отриманий за використанням того ж ключа.*

- *Порахувати частоти всіх символів у тексті мамаимилаираму.*
- *В потоці зашифрованих донесень від інформатора домінує буква н. Припустивши, що використовується шифр зсуву і пропуски між словами ігноруються, знайти за допомогою частотного аналізу ключ і розшифрувати повідомлення*
- ***опдрснкнмярстомзйнлопнвнкнчдмннкдкшйяспдсшнвн.***
- *a) Використовуючи шифр чотирьох квадратів із пункту з ключем як на малюнку, зашифрувати слово university.*
- *b) Дешифрувати криптотекст sknromra, отриманий за допомогою того ж шифру з тим же ключем.*
- *a) Зашифрувати повідомлення **білі мухи налетіли**, використавши шифр Віженера з ключем зима.*
- *b) Розшифрувати криптотекст **ьччжпчьишисаеяйпяваааьяч**, отриманий за допомогою шифру Віженера з тим же ключем.*
- *Показати, що шифр зсуву є частковим випадком шифру Віженера. Який ключ у шифрі Віженера над українським алфавітом слід взяти, щоб отримати шифр Цезаря?*

- *Вибрати для шифру Віженера довільний ключ довжини*
  - *a) 3,*
  - *b) 6*
- *і зашифрувати повідомлення **бороніть королівну від ворогів**. У отриманому криптотексті знайти однакові триграми або біграми і порахувати, на якій відстані одна від одної вони знаходяться.*
- *a) Зашифрувати повідомлення **білі мухи налетіли**, за допомогою шифру з автоключем, взявши як ключ слово зима.*
- *b) Розшифрувати криптотекст **ьччхюбхощнпинтвпсккпікш**, отриманий за допомогою того ж шифру з тим же ключем.*