**Лабораторна робота №3**

на тему «Елементи криптоаналізу»

Мета роботи: ознайомитись з симетричними методами шифрування та підходами до їх криптоаналізу.

Завдання: для кожного зашифрованого повідомлення знайти ключ та відкрите повідомлення. Повідомлення зашифровані методом перестановки стовпців, подвійної перестановки (стовпців та рядків), заміни та шифру Віженера.

Індивідуальні завдання для методу **перестановки стовпців**.

|  |  |
| --- | --- |
| 1 | \_\_оенткчсутитсо\_тум\_яор\_ктенюка\_твынп\_\_еоту\_бтеоро\_тог\_упу\_лоент\_еясач |
| 2 | в\_еиыс\_лвеснаоеммжтьее\_со\_дмйун\_гмири\_удвк\_лечое\_еотнмо\_рй\_бавиын\_тмяее\_ |
| 3 | ныоч\_тбиусич\_ло\_слпоьэеим\_нтср\_тоопхл\_тоопье\_онйдпе\_\_\_анжяхл\_оа\_\_ни\_зь |
| 4 | дак\_гчво\_вее\_окалкешигар\_дь\_дянье\_зоонгм\_о\_оа\_нждто\_ееетлат\_\_еьтвнх\_\_иаоахрсктоу\_тса\_е\_\_ня |
| 5 | оопвзедр\_таехжьумч\_а\_незуьта\_е\_роьл\_синтьсеа\_ртгыинв\_\_цароонаебжбеирег\_зчна\_н\_ио |
| 6 | йадждк\_ыондь\_егка\_швсаетр\_вс\_ьокетзи\_а\_н\_баударьтб\_удзьихвроесо\_ншсееоа\_ир\_оетен |
| 7 | гвнеаол\_авлрипь\_дшоына\_выьдтхь\_чтсааьевт\_сыхаьытд\_бр\_оод |
| 8 | ео\_чьном\_ногдл\_юйеопдраптаееб\_взт\_сепи\_\_иррпоехе\_д\_етооскл\_ве\_\_дул |
| 9 | мтыо\_ж\_ешвьссе\_леит\_еьс\_очевлеок\_тко\_рывй\_яте\_бвтер\_и\_ |
| 10 | ебсйо\_н\_тн\_очя\_очулпетяоб\_сис\_отчяйн\_попе\_оуьшебр |
| 11 | \_то-оизчт\_еьинв\_мтжв\_еоизсйгиои\_данннпзлоо\_\_е\_нагонеидмбиохо\_одд\_гниа\_ао\_росопрпт\_я\_нт\_\_ио |
| 12 | шаиотбеяа\_сдкжйр\_ызпиа\_енштоб\_киуимр\_ыдрйпс\_иортпщиео\_няинлсйьы |
| 13 | щйботеа\_оьс\_ссслачивтиомыни\_ааз\_зярвс\_т\_сасьачемт |
| 14 | оеитпнмче\_н\_отвагд\_есточт\_\_овтхо\_\_ытмваи\_едвст\_йетоьнилен\_но\_жу |
| 15 | \_тгаыкд\_ошадиепнмоьуядзь\_рс\_юунтяза\_о\_откк\_ыта\_атпг\_ыд\_теьыдш\_акьне\_уашзяз\_рьтдуо |
| 16 | нншас\_ееы\_бватсд\_еинтмнвены\_нжв\_изисд\_еинтйнвено\_твбыае\_олтоьк\_\_зжинь\_ |
| 17 | ч\_еумсенреде\_\_трыабаоетшье\_мт\_баочге\_отйв\_роатбодеалть |
| 18 | еьи\_мтршхиоодухз\_р\_денйои\_ал\_зшху\_чиноцсенйвт\_е\_зиж\_ин |
| 19 | убсьдаон\_ечьуб\_однелос\_оотвч\_оыебн\_\_рипнимтра\_ьеейшин\_ |
| 20 | начаалср\_пьоакмя\_гие\_пхлдев\_онгоомркйыму\_зкг\_ии\_огячреоеко\_ф |
| 21 | \_вбтатаыюиек\_\_нкидедоладаг\_е\_тгнчоьиое\_т\_ханоа\_\_юбвтаыер\_\_уикдгхдооаотг\_гнаоие\_\_ча\_нтдльее |
| 22 | лт\_яен-рйяпекоефцисминт\_яане\_ррадзаж\_ртебакоад\_ннлм\_е\_ьбне\_уа\_рить |
| 23 | гчоне\_инкет\_\_агмапоеоеслтда\_а\_бтроьа\_ктк\_уюкчолет\_ыинйннерттн\_е |
| 24 | лхисеипр\_иртдо\_\_сьозтбао\_пыои\_нддхоу\_бньта\_рау\_\_тооанр\_рвотакв\_ргеитевс\_\_\_бадтдеусотичкнье |
| 25 | ои\_нкадгверн\_взоющ\_ааястаб\_оронтмрлвес\_я\_вмоозовож\_оньтстейн\_ярееви\_рнембвй\_ыариоси\_л\_ав\_нс\_еупу\_амкйзовож\_оньтс |
| 26 | аиж\_вьатуеанвиу\_\_л\_оьлаетчж\_\_ашеаквврнотыоб\_вьут\_сяисотниьалжевшоав\_\_веоа\_тепиинс |
| 27 | шорйохиьденн\_\_ачитнае\_я\_оссххошмир\_йслиеы\_япрни\_тех\_\_дыл |

*Примітка.* Текст може бути розміщено як в квадратну матрицю, так і прямокутну. Якщо довжина тексту менша ніж m\*n, де m – кількість рядків, а n – кількість стовпців, то текст доповнено прогалинами (\_) до m\*n. Кількість стовпців менша за кількість рядків (n<m).

До звіту за даним шифром включити закритий текст, відкритий текст та ключ (порядок перестановки стовпців для шифрування та розшифрування).

Індивідуальні завдання для методу **подвійної перестановки**

|  |  |
| --- | --- |
| 1 | звв\_ро\_ноеле\_двеов\_\_л\_о\_тчмвесра\_тзаест\_\_авмтоо\_эгво\_о\_т |
| 2 | \_роохдорзоя\_ьмтетэь\_ш\_еоеьи\_веяапа\_чтссапхо\_л |
| 3 | ипвлреочбыт\_осю\_вж\_ччтьос\_тье\_\_вчтьодрстеан\_о\_ото-\_вт\_ниь\_зп\_аужме |
| 4 | \_рбза\_таве\_гелдйсаа\_к\_тькка\_индр\_геу\_тчдно\_оя\_у\_\_мегтоиуео\_тргдяотне\_хт\_и\_тдеуьжш |
| 5 | юви\_лднгче\_иецт\_мюацт\_нюн\_тьеиезу\_смно\_неу\_уе\_он |
| 6 | еехн\_иеы\_тенурабко\_лебеомт\_еас\_опэ\_т\_змнаелава\_мемщрее |
| 7 | с\_\_ыл\_с\_мч\_доыоб\_тнзл\_маиеьотоучб\_тм\_ыжвяио\_тепкаа\_\_\_хенмкту\_о\_тсьеи\_мсрибуьясс\_т |
| 8 | льш\_чуао\_гилестдалнем\_\_о\_нмеопмя\_\_го |
| 9 | оо\_тноеу\_дсв\_ипроттр\_ведючт\_амя\_\_амед\_итохкуо\_ьл |
| 10 | очтоыб\_пмсаояа\_бшльшяа\_оострп\_опеещ\_р\_азн\_и\_года\_оммтчо\_аел\_меоеооб\_автьд\_сяеамсчлужтиь\_бы\_осытрднао\_опркибт\_ав\_ |
| 11 | вн\_мовпсыы\_а\_тиаятсед\_теирн\_ояну\_бееезв\_к\_не\_ |
| 12 | мид\_\_ыамп\_\_еучк\_ереор\_гдо,ка\_гиоьтшрсыипо\_укт\_м,о\_пдамнеенпермеыирлвкиялх\_дто |
| 13 | оет\_ыор\_пеоаызоир\_лпшз\_иэьжн\_\_отетнисньимлд\_\_киентд\_н\_аеко\_ртио |
| 14 | меяв\_р\_аеггдв\_пяут\_,киотл\_юнбеюу\_с\_тртаот\_ |
| 15 | теы\_чврпеде\_\_тнаьслджноыо\_лктатеи\_св\_на\_умебмыл\_\_\_спви\_нпрео |
| 16 | нкеи\_яшеибщнаооезлн\_\_\_непирныат\_чс\_дыгат\_оаемйр\_иа\_двйа\_ка\_одгял\_ти\_вс |
| 17 | \_иоканм\_ияи\_гкоот\_туас\_н\_\_дытоиннмоавпо\_тснеиецтонмм\_е |
| 18 | мккан\_тсачлсзоогн\_нккау\_хащю\_ио\_ам\_лхвщу\_ижиови\_жжони\_ат\_ькк |
| 19 | одп\_хо\_ноте\_воч\_\_тэеид\_тееад\_жммов\_е\_есе\_тса\_ы\_нтчнзиаы\_лсви |
| 20 | \_дотисадл\_рятержие\_муно\_\_нуныжмгое\_роь\_днопожо\_н\_две\_о |
| 21 | бжости\_ьоох\_ошр\_ы\_ннпсйоаурсу\_зхисдевтнеиьдоо\_ттлхп\_\_оо\_д\_утдгае |
| 22 | а\_гшмоьекн\_исет\_пуфлтик\_оатбеазлуьтйс\_пухегш\_аазитс\_опнуе\_р\_ |
| 23 | линыев\_огоямапюеш\_\_юо\_\_авнсьтп\_мыо\_гше\_аьо\_дюмляммест\_си |
| 24 | чеаум\_боьт\_ивотхк\_етн\_е\_твтаонн\_очывсеос |
| 25 | еинл\_\_\_тви\_чеевц\_ричлуи\_а\_рыгбр\_еасд\_еучмбадсуе\_ |
| 26 | иньевлт\_ямртевнидх\_оа\_о\_т,очекеочвл\_теоочх\_тсенйднес\_\_ва |
| 27 | жиолтдоь\_жнсизлана\_ачтьна\_ач-дьор\_п\_пооржне\_немо\_у\_ум\_гозянь\_ел |

*Примітка.* Текст може бути розміщено як в квадратну матрицю, так і прямокутну. Якщо довжина тексту менша ніж m\*n, де m – кількість рядків, а n – кількість стовпців, то текст доповнено прогалинами (\_) до m\*n. Кількість стовпців менша за кількість рядків (n<m).

До звіту за даним шифром включити закритий текст, відкритий текст та ключи (порядок перестановки стовпців для шифрування та розшифрування, а також порядок перестановки рядків для шифрування та розшифрування).

Індивідуальні завдання для методу **заміни**

Файл з індивідуальними завданнями – "Лр 3\_ПЗ-18-2\_ч3\_ч4.docx".

До звіту за даним шифром включити закритий текст, відкритий текст, ключ у вигляді таблиці відповідності двозначного числа шифру літері алфавіту з частотою входження в текст (частості) та короткого опису порядку дешефрування.

Завдання обирати наступним чином: за порядковим номером.

Індивідуальні завдання для шифру **Віженера**

Файл з індивідуальними завданнями – "Лр 3\_ПЗ-18-2\_ч3\_ч4.docx".

Завдання обирати наступним чином: за порядковим номером.

До звіту за даним шифром включити закритий текст, знайдену послідовність символів, що повторювалась, відстані між ними та обчислену довжину ключа; обчислені індекси співпадіння для перевірки правильності знайденої довжини ключа; таблицю з частотами літер алфавіту в окремих фрагментах тексту (самі фрагменти окремо не наводити), що відповідають певним літерам ключа; знайдені зсуви зі взаємними індексами співпадіння, що їх підтверджують; знайдене ключове слово та відкритий текст.