Лабораторна робота №6. Шифр Playfair і шифр подвійного квадрата.

Ціль роботи: *Відпрацювати шифрування за допомогою біграм (шифри Playfair та подвійного квадрата).*

Загальні відомості

Найбільш відомий шифр біграмами називається Playfair. Він застосовувався Великобританією в Першу світову війну. Відкритий текст розбивався на пари букв (біграми) і текст шифровки будувався з нього по наступним двом дуже простим правилам (наводяться нижче).

Теоретичні відомості

Для шифрування ключ вписувався у таблицю, а потім усі останні літери вписувалися у цю таблицю за алфавітом. Наприклад:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| П | Р | И | К | Л | А | Д | Б |
| В | Г | Е | Є | Ж | З | І | Ї |
| Й | М | Н | О | С | Т | У | Ф |
| Х | Ц | Ч | Ш | Щ | Ь | Ю | Я |

Для шифрування використовуються наступні правила:

1. Якщо обидві букви біграми вихідного тексту належали одному стовпчикові таблиці, то буквами шифру вважалися букви, що лежали під ними. Так біграма ИН давала текст шифровки ЕЧ. Якщо буква відкритого тексту знаходилася в нижньому рядку, то для шифру бралася відповідна буква з верхнього рядка і біграма ЇЯ давала шифр ФБ. (Біграма з однієї букви чи пари однакових букв теж підкорялася цьому правилу і текст ЕЕ давав шифр НН).
2. Якщо обидві букви біграми вихідного тексту належали одному рядку таблиці, то буквами шифру вважалися букви, що лежали праворуч від них. Так біграма ВЄ давала текст шифровки ГЖ. Якщо буква відкритого тексту знаходилася в правому стовпчику, то для шифру бралася відповідна буква з лівого стовпчика і біграма ФТ давала шифр ЙУ.

Якщо обидві букви біграми відкритого тексту лежали в різних рядах і колонках, то замість них бралися такі дві букви, щоб уся четвірка їх представляла прямокутник. При цьому послідовність букв у шифрі була дзеркальною відносно вихідної пари. Наприклад, РШ шифрувалося як КЦ, а ЙБ шифрувалося як ФП.

Розберемо цей алгоритм на прикладі:

При шифруванні фрази НЕХАЙ КОНСУЛИ БУДУТЬ УВАЖНІ по біграмам виходить така шифровка:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| НЕ | ХА | ЙК | ОН | СУ | ЛИ | БУ | ДУ | ТЬ | УВ | АЖ | НІ |
| ЧН | ЬП | ОП | СО | ТФ | КА | ДФ | ІЮ | ЬА | ЙІ | ЛЗ | УЕ |

Шифрування біграмами різко підсилило стійкість, шифрів до розкриття.[2]

**Шифр подвійного квадрату.**

Даний шифр на перший погляд незначно відрізняється від шифру Playfair, для шифрування він використовує дві таблиці, однак, ці, здавалося б і не настільки значні зміни привели до появи на світ нової криптографічної системи ручного шифрування. Вона виявилася така надійна і зручна, що застосовувалася німцями навіть у роки Другої Світової війни. Шифрування методом подвійного квадрата дуже просте. Приведемо приклад використання шифру подвійний квадрат для російських текстів. Маються дві таблиці з випадково розташованими в них алфавітами:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ч |  | В | І | П |  | Е | Л | Ц | Й | П |
| О | К | Й | Д | У | . | Х | Ї | А | Н |
| Г | Ш | З | Є | Ф | Ш | Д | Є | К | С |
| Л | Ї | Х | А | , | І |  | Б | Ф | У |
| Ю | Р | Ж | Щ | Н | Я | Т | И | Ч | Г |
| Ц | Б | И | Т | Ь | М | О | , | Ж | Ь |
| . | С | Я | М | Е | В | Щ | З | Ю | Р |

Для шифрування повідомлення розбивають на біграми. Перша буква біграми знаходиться в лівій таблиці, а друга в правій. Потім, думкою в таблиці будується прямокутник так, щоб букви біграми лежали в його протилежних вершинах. Інші дві вершини цього прямокутника дають букви шифровки. Припустимо, що шифрується біграма тексту ОЖ. Буква О знаходиться в першій колонці другого рядка лівої таблиці. Буква Ж знаходиться в четвертій колонці шостого рядка правої таблиці. Виходить прямокутник утворений рядками 2 і 6, а також колонками 1 і 4 правої таблиці. Отже, шифровці відповідають букви, що лежать у першій колонці шостого рядка лівої таблиці Ц і в четвертій колонці другого рядка правої таблиці А – отримуємо біграму АЦ. Так парами букв шифрується все повідомлення:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Повідомлення: | ПР | ИЇ | ЗД | ЖА | Ю | ШО | СТ | ОГ | О |
| Шифровка: | ПЕ | ,Й | ЄШ | ЧЙ | ЛТ | ДБ | ЩР | НЮ | ХЛ |

Якщо обидві букви біграми повідомлення лежать в одному рядку, то і букви шифровки беруться з цього ж рядка. Перша буква біграми шифровки береться з лівої таблиці в стовпці, що відповідає другій букві біграми повідомлення. Друга буква біграми шифровки береться з правої таблиці в стовпці, що відповідає першій букві біграми повідомлення. Так, по приведеним вище таблицях біграма повідомлення ТО перетворюється в біграму шифровки ЖБ.

Безсумнівно, що шифрування біграмами дає дуже стійкий до розкриття і простий шифр, а це було в свій час великим успіхом. Злом шифровки подвійного квадрата вимагає великих зусиль і довжини повідомлення більш тридцяти рядків.[2]

Порядок виконання лабораторної роботи.

1. Вивчити схеми алгоритмів Playfair та подвійного квадрата.
2. В додатку №1 вибрати завдання відповідно до номеру студента в журналі.
3. Зашифрувати поданий текст алгоритмом Playfair.
4. Розшифрувати поданий шифротекст, який було зашифровано алгоритмом Playfair.
5. Зашифрувати поданий текст алгоритмом подвійного квадрата.
6. Розшифрувати поданий шифр текст, який було зашифровано алгоритмом подвійного квадрата.
7. Скласти звіт, у який включити початкові дані, опис послідовності дій шифрування, кінцевий результат і відповіді на контрольні запитання.

Контрольні питання.

1. Шифр Playfair, принцип шифрування.
2. Шифр подвійного квадрата, принцип шифрування.
3. Де знайшли застосування біграмні шифри?
4. Які недоліки біграмних шифрів?

### Лабораторна робота №2

**Шифр PLAYFAIR (зашифрувати)**

|  |  |  |
| --- | --- | --- |
| № | Ключ | Повідомлення |
| 1 | МІЦНИЙ | ПІДСИЛИТИ КОНТРОЛЬ |
| 2 | МОДЕЛЬ | ПРИЇДУ ЧЕРЕЗ ДОБУ |
| 3 | ПЕСТОЩІ | КОНТАКТ ВІДКЛАДЕНИЙ ДО ЗИМИ |
| 4 | ПИРІГ | НЕЗАМІННИХ КАДРІВ НЕМАЄ |
| 5 | ПОТРІБНИЙ | НЕПТУН ВИХОДИТЬ НА ОРБІТУ |
| 6 | ПОХІД | ПЕРЕЗДАЧІ ЛАБОРАТОРНИХ РОБІТ |
| 7 | РОКІТ | НА ПЕРШІЙ ПАРІ ПОБАЧИМО |
| 8 | РОМАНС | КРИТИЧНА МАСА ПЛУТОНІЮ НЕ ВИЗНАЧЕНА |
| 9 | РУЧКА | АЛЛАХ ЄДИНИЙ І МУХАМЕД ПРОРОК ЙОГО |
| 10 | УЖИТОК | КАРЛ У КЛАРИ ПОЦУПИВ КОРАЛИ |
| 11 | ЧЕРГОВИЙ | ЯКЩО ДРУГ ВИЯВИВСЯ РАПТОМ |
| 12 | ЮВЕЛІР | У ДАНИЙ ПЕРІОД ЕВАКУАЦІЯ НЕМОЖЛИВА |
| 13 | ЯЩІРКА | ПОРУШЕННЯ ДИСЦИПЛІНИ КАРАЄТЬСЯ |
| 14 | МАЙНОВИЙ | ЦЕ УЧБОВА ШИФРОГРАМА |
| 15 | АРМІЯ | У НАШІМ РАЇ НА ЗЕМЛІ |
| 16 | БІГАТИ | БІЛА БЕРЕЗА ПІД МОЇМ ВІКНОМ |
| 17 | БІЛИЙ | ЩОСЬ СТАЛО ХОЛОДНІТИ |
| 18 | БОРЩ | МЕНІ ТРИНАДЦЯТИЙ МИНАЛО |
| 19 | БРОНЯ | ПРИКЛАДНИЙ ЄКРАН |
| 20 | БУДІВЛЯ | ОТО ЯК БИ ВЗЯТИ ВСІ ГОРИ |
| 21 | ЮВЕЛІР | НЕПТУН ВИХОДИТЬ НА ОРБІТУ |
| 22 | ЯЩІРКА | ПІДСИЛИТИ КОНТРОЛЬ |
| 23 | ЯКИЙ | НА ПЕРШІЙ ПАРІ ПОБАЧИМО |
| 24 | АРМІЯ | ПРИЇДУ ЧЕРЕЗ ДОБУ |
| 25 | ГОРИ | ОТО ЯК БИ ВЗЯТИ ВСІ МОРЯ |
| 26 | БІЛИЙ | В ОДНЕ МОРЕ ОТО БУЛЬКНУЛО |
| 27 | БРОНЯ | ЯКЩО ДРУГ ВИЯВИВСЯ РАПТОМ |
| 28 | БІГАТИ | КАРЛ У КЛАРИ ПОЦУПИВ КОРАЛИ |
| 29 | БОРЩ | ОЙ НА ГОРІ ДВА ДУБКИ |
| 30 | БУДІВЛЯ | ВАЖКО ВСИДІТИ НА МІСЦІ |

**Шифр PLAYFAIR (розшифрувати)**

|  |  |  |
| --- | --- | --- |
| № | Ключ | Шифртекст |
| 1 | МОДЕЛЬ | РСВИБНЕЖПЛЄЛДМЯ |
| 2 | ЮВЕЛІР | МЙЕТЙГНІАРМЖЛЕТЮТБШЕЦУВНЧОЖАЕБ |
| 3 | БРОНЯ | РПЦАЕБЮИГЇАГЇГПАРВСУНЛ |
| 4 | БУДІВЛЯ | ПКБСЯГЗПСЙЯПБЖПСС |
| 5 | БІЛИЙ | ЦСТЩТУВИНЦПІНЕОБРА |
| 6 | РОКІТ | СІМЖІХРНСТОТЛТВАЯЕЛК |
| 7 | БУДІВЛЯ | ЛБГОПІЬСІВСЙТДОУНЬЖ |
| 8 | ПИРІГ | МЄЇГОИЧЧПЦЇВЄПГПМЄТИН |
| 9 | АРМІЯ | ЛЯЙИЙКХЖЕЛЇЕСІЮ |
| 10 | УЖИТОК | АБМСЖАСЖМКЩЄХЖМОЗУКПЖСД |
| 11 | БІГАТИ | ЗВФЇЮУЗДСТРПЮНСАКУПСДЗЙ |
| 12 | МІЦНИЙ | ЛНЖОІРАРМРПЦСУПОЙ |
| 13 | ЯКИЙ | РКНЖШАЖБРЙСЗРПВБЦЙНП |
| 14 | БІГАТИ | ІГЗДЕММЇПЗНАБФРЖСБВЄОПХ |
| 15 | ПОТРІБНИЙ | БЄОРЮЄЖТЦПЖІБЧОЕТІНБНК |
| 16 | ГОРИ | ГФЮДТЩРОАМАЙЖЮІЩ |
| 17 | РОМАНС | ИМЙУКХСНАНБНТПФУМСУБМЖРФЖСМШЖМЄ |
| 18 | ПЕСТОЩІ | МСЛЩСУЕДТЗМЛТЇЩЙЙКЄТБРЙН |
| 19 | ЮВЕЛІР | ЦЄИІПВЦЦДЬТЮЇВРЕЦЄТВН |
| 20 | ЯСНИЙ | НМОЮИТЯБЧЙЩККЄЩЗРН |
| 21 | БІЛИЙ | ЇБІУНХЄДПСОЦУПВНАЧДУПВЦ |
| 22 | МАЙНОВИЙ | ЦЕ УЧБОВА ШИФРОГРАМА |
| 23 | ГОРИ | БМДЦЇДАДКШПБАУЄСРИД |
| 24 | РУЧКА | УООУЦЕЕДТЖПДЛЧЩУЛЄІЙАЙАЙРНТАЩ |
| 25 | ПОХІД | ОГЛЗРЗХЬЕТБВДЛБСДЛТЖДМХВБН |
| 26 | ЯЩІРКА | СПЯЦХЗЦЦЩГЇТЮЄСМРМЖВБКРЗСЮЙБ |
| 27 | АРМІЯ | КОЯФЯІМРЄСЯДЄРОР |
| 28 | БОРЩ | КЖПЗМГЗТВБЧФЮТТЖПЩХЄ |
| 29 | БРОНЯ | КЯЕУСОЖБДУЕЛОВЖ |
| 30 | ЧЕРГОВИЙ | ФУОЖМДНЙИЙЬЙЙИУЬЧДСУРП |

**Шифр подвійного квадрата (зашифрувати)**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ч |  | В | І | П |  | Е | Л | Ц | Й | П |
| О | К | Й | Д | У |  | . | Х | Ї | А | Н |
| Г | Ш | З | Є | Ф |  | Ш | Д | Є | К | С |
| Л | Ї | Х | А | , |  | І |  | Б | Ф | У |
| Ю | Р | Ж | Щ | Н |  | Я | Т | И | Ч | Г |
| Ц | Б | И | Т | Ь |  | М | О | , | Ж | Ь |
| . | С | Я | М | Е |  | В | Щ | З | Ю | Р |

|  |  |
| --- | --- |
| № | Шифрограма |
| 1 | ПРИЇЖДЖАЮ ШОСТОГО |
| 2 | ОРБІТА МАРСА |
| 3 | НАРОДИВСЯ ХЛОПЧИК |
| 4 | СВІТЛО У ВІКНІ |
| 5 | ПРИЇДУ ЧЕРЕЗ ДОБУ |
| 6 | НЕЗАХИЩЕНІ ЗАСОБИ ЗВ'ЯЗКУ |
| 7 | ЩО ТАКЕ ДОБРЕ |
| 8 | ПЕРСПЕКТИВНІ РОЗРОБКИ |
| 9 | АТОМНА ЕНЕРГІЯ РЕАКТОРА |
| 10 | ПІДВОДНИЙ ФЛОТ СОЮЗНИКІВ |
| 11 | РУКОПИС ДОКУМЕНТА ДОДАЄТЬСЯ |
| 12 | СИЛА ТЕРОРИСТІВ У ЛІТАКАХ |
| 13 | ЕНЕРГОЗБЕРІГАЮЧІ УСТАНОВКИ |
| 14 | ОСЬ ТОБІ ВАРЕНИКИ |
| 15 | СЕКРЕТНІ РОЗРОБКИ |
| 16 | ЛОКАЛЬНА МЕРЕЖА |
| 17 | ВИПАДКОВІ ПОГРОЗИ |
| 18 | МАКРОЕКОНОМІЧНА СИТУАЦІЯ НЕСТАБІЛЬНА |
| 19 | ТРУБИ ДОСТАВЛЕНІ НА КУБУ |
| 20 | НЕОБХІДНА ГЛИБИНА ДОСЯГНУТА |
| 21 | БАЗІКА ЗНАХІДКА ДЛЯ ШПИГУНА |
| 22 | РІВНОВАГА В РЕГІОНІ ПОРУШЕНА |
| 23 | МЕТОДИКА РОЗРАХУНКУ ЧЕРВ'ЯЧНОЇ ПЕРЕДАЧІ |
| 24 | СТАН ЗДОРОВ'Я СТАБІЛЬНИЙ |
| 25 | ГРАФІЧНИЙ ІНТЕРФЕЙС ПРОРАМИ |
| 26 | СИСТЕМА ОБРОБКИ ДАНИХ |
| 27 | БАЗИ ДАНИХ МАЮТЬ ПОТРЕБУ В ОБНОВЛЕННІ |
| 28 | СИСТЕМА КРИПТОГРАФИЧНО СТІЙКА |
| 29 | ЗАХИСТ ПРИВАТНОЇ ВЛАСНОСТІ |
| 30 | ФАНАТ СВОЄЇ СПРАВИ |

**Шифр подвійного квадрата (розшифрувати)**

|  |  |
| --- | --- |
| № | Шифровка |
| 1 | ЗРФОЛРРЕН.ЬЗМАЛХХ,ІЛЖДАК Х |
| 2 | ЦЖЙУАЄ..ЛАЛЬС.Ї.ОХ |
| 3 | С.ФАЙЩИНХХПДМІЧЇЮПЩЇПЕН.ІТВТ |
| 4 | ЗРЩРВЬ АЇЛТБЖШОХАДИН Х |
| 5 | ГЇХБЦНЩЇХТНЇВІТН АХТАДДЩЬФЩХ |
| 6 | ЩРУДЦСХТТБЛИЩХЩРБАЛІЬУЖВ, |
| 7 | ЦАКУЦЧУЕБРЕЮЬ А |
| 8 | ЬМЇ,ОХХТЩРІМІЧЯ,ПК АНЇЬЇ |
| 9 | ВІОТЇЩАКПСЇ.ЧКУХЧФХ,ЕЧЯСЯРПОЇОП РЕЩФФЩЛА |
| 10 | ЖКШХАКЦСЧУІХАЄ АХІЩХС ЬЖНУ А |
| 11 | ЗРЩРВЬ АНСЬВОТС.ФАЖЖТЬПШМААЗ А |
| 12 | КЙБЖЩРП ИРЙЙЬДЇОЕСФОРКНГМА |
| 13 | НГО,ОТМЇЕСУМРУЖЗОХ |
| 14 | ЩРЧКМІШЛПО АЩРБАЛІЬУПЄЬТЩЛ |
| 15 | КУЧУОАВСЇГ ЇР ЧКЦЖ |
| 16 | ЖКЄЖЛШУДОЙЕБФМЬТП ХЮЯ ЬЇЕСЛБЬК..ІЧГУЛА |
| 17 | В НСЩНЯ,ПСЇ.ТБЖШОХ |
| 18 | ЮДНС.ЧХБТЬВАПО АЗРЬАБІЕЩПКРФЖДМЇУЦЧУ |
| 19 | ПЕ,ЙТЗЧЙТЛДБЩРНЮНЮ |
| 20 | ЯПКЙБЖЯІЯ,ЦСУЄЇЛОХШЯШЖКЗХ, |
| 21 | ЧУТБЇЩПЗЩХ ВНЧЦЮЇР |
| 22 | ПЕ,ЙНАЙРРЕЗЕЛШЇЛХ, |
| 23 | ЕПГШЕПХРМЯЯ,ПСЇ.ТБЖШОХ |
| 24 | Е,.МХГИНХХДПХЮПША.СЙЖЗЕМ |
| 25 | РУРЕДЦЄХРЕПЩФМЕЛПЇЩРУД..ЇР |
| 26 | ТТЛРФЄЩ,ХТЬСЩ, |
| 27 | Н.МЇЖДЕБУМЮКЩЇ |
| 28 | ЯПЇЛІХНД АДЧ,ХЬЙ АХТВРСОХН А |
| 29 | ЯЇПЙ..УЩ АЛХЯ ШЛНОЛАЛЬГЇШ ЧУ |
| 30 | ВСЛЩ ЦПЇЕСЙЄЯ, |