

Міністерство аграрної політики та продовольства України

Вінницький національний аграрний університет

МЕТОДИЧНІ ВКАЗІВКИ

**для виконання лабораторних робіт з дисципліни
“Захист та кодування інформації”**

для студентів
усіх форм навчання
та спеціальностей

Вінниця 2012

Методичні вказівки для виконання лабораторних робіт з дисципліни “Захист та кодування інформації” для студентів усіх форм навчання та спеціальностей. /Укладач: В.О.Денисюк. - Вінниця: ВНАУ, 2012.- 53 с.

Укладач: В.О.Денисюк, доцент, к.т.н.

Рецензенти:

Рекомендовано науково-методичною радою Вінницького національного аграрного університету протокол № ____ від “ ____ ” _____ 2012 р.

НАУКОВО - МЕТОДИЧНЕ ВИДАННЯ

В методичних вказівках з дисципліни “Захист та кодування інформації” представлено 7 лабораторних робіт, які розраховані на загальний обсяг навчальної роботи у 28 годин. Завдання лабораторного практикуму спрямовані на оволодіння студентами сучасними технологіями захисту та кодування інформації: вивчення теоретичних основ створення та практичного використання алгоритмів криптології і теорії кодування інформації.

Укладач: доцент, к.т.н. Денисюк Валерій Олександрович

Підписано до

друку: _____ формат _____ папір _____

Друк № ____ друк офсетний.

Умовних друкованих аркушів _____

Обл. вид. аркушів _____

Тираж _____ примірників

Зам. № ____

Віддруковано в ВЦ ВНАУ, 21008, м.Вінниця, вул.Сонячна, 3.

ЗМІСТ

	Стор.
Вимоги до оформлення лабораторних робіт	4
<i>Лабораторна робота №1. Початкові відомості про криптологію</i>	5
<i>Лабораторна робота №2. Класичні методи шифрування</i>	11
<i>Лабораторна робота №3. Шифр “одноразовий блокнот”</i>	26
<i>Лабораторна робота №4. DES-шифр</i>	32
<i>Лабораторна робота №5. Афінні шифри</i>	37
<i>Лабораторна робота №6. Афінні шифри вищих порядків</i>	41
<i>Лабораторна робота №7. Криптосистеми з відкритим ключем.</i> Система Рабіна	45
Джерела інформації	47
Додаток. Абетки	53

ВИМОГИ ДО ОФОРМЛЕННЯ ЛАБОРАТОРНИХ РОБІТ

Виконувати лабораторні роботи слід за своїм варіантом, номер якого визначає викладач. Лабораторні роботи потрібно виконувати акуратно, на аркушах стандартного формату А4 з титульним аркушем, друкованим чи рукописним способом, чорнилом будь-якого кольору за винятком червоного та зеленого.

Звіт про виконання лабораторних робіт обов'язково повинен містити:

- тему роботи;
- мету та завдання для роботи;
- результати виконання;
- висновки по роботі.

Оформлені таким чином роботи повинні бути захищені у визначені викладачем терміни. При співбесіді студент повинен знати відповідний теоретичний матеріал і вміти розв'язувати задачі.

Лабораторна робота №1

Тема: Початкові відомості про криптологію.

Мета: Ознайомитися з основними визначеннями та принципами криптографії та криптоаналізу. Засвоїти найпростіші методи кодування та декодування інформації.

Теоретичні відомості

1. Початкові поняття та приклади. Класична задача криптографії постає тоді, коли двоє збираються обмінятися конфіденційною інформацією за присутності третьої недружньої особи, яка також намагається заволодіти цією інформацією.

Назвемо двох перших осіб *Алісою* та *Бобом*. Третій персонаж називатиметься *суперником*. Аліса та Боб є законними користувачами каналу зв'язку або легальними абонентами комунікаційної мережі. Суперник є несанкціонованим користувачем, який має нешляхетну мету перехопити чи підслухати Бобове повідомлення Алісі. Аби зберегти таємницю, Боб *шифрує* своє повідомлення, тобто перетворює його до незрозумілої для суперника форми, застосувавши *алгоритм шифрування*. В результаті з повідомлення, яке ще називають *відкритим текстом*, виходить *криптотекст*, який Боб і посилає Алісі. Отримавши криптотекст, Аліса *дешифрує* його за допомогою *алгоритму дешифрування* і отримує вихідне повідомлення. В наших криптологічних студіях ми виходимо із припущення, що суперникові завжди щастить перехопити криптотекст. Проте якщо алгоритм шифрування є *надійним*, то суперник не здатен дошукатися змісту повідомлення. Алгоритми шифрування та дешифрування разом складають *криптосистему* або, простіше, *шифр*.

Приклад 1. Поставивши себе на місце суперника, уявимо що нам вдалося підслухати зашифроване повідомлення:

осіла унофелет од шидохдін єн умоч

Спробуймо відновити повідомлення, відгадавши алгоритм шифрування. Поза сумнівом, успіх буде миттєвим.

Шифр, з яким ми щойно ознайомились, має дві типові риси, бажану і небажану. Перша полягає в тому, що цей шифр є *ефективним* — шифрування і дешифрування займають зовсім мало часу. Негативною рисою цього шифру є його *ненадійність*.

Найчастіше вимоги, які висуваються до криптосистеми, не вдається задовольнити одночасно — ідеального шифру не існує. Вибір шифру з тими чи іншими властивостями диктується конкретною ситуацією. Іноді інформація, скажімо біржова, перестає бути таємною через двадцять хвилин і

мусить бути зашифрована і передана за лічені секунди. А іноді інформація повинна зберігатись десятиліттями, зате нема потреби квапитись при шифруванні.

Приклад 2. Шифр Цезаря Давньоримський імператор Юлій Цезар (100-44 р. до н.е.) полюбляв зашифровувати свої таємні послання у спосіб, коли кожна буква заміщується деякою іншою, а саме тою, що знаходиться у алфавіті через три позиції. Стосовно української абетки це означає що, **а** міняється на **г**, **б** на **г**, **в** на **д** і т.д. Останні ж букви абетки **ь**, **ю**, та **я** зміщуються теж на три позиції **циклічно**, тобто переходять у **а**, **б** та **в**, відповідно. Для прикладу, слову **імперія** відповідає криптотекст **лппзулв**. Кажуть, що шифр Цезаря є *шифром зсуву* на 3 позиції.

Приклад 3. Шифр Частоколу. Алгоритм шифрування найліпше пояснити на прикладі. Щоб зашифрувати повідомлення криптографія, переписуємо його у вигляді "частоколу" **к^ри^пт^ог^ра^фі^я** і зчитуємо текст рядками, почавши з верхнього. В результаті отримуємо криптотекст **рппорфякитгаі**. "Висоту" частоколу можна вибирати. Щойно вона була 2.

Довжина зсуву і висота частоколу у розглянутих шифрах є секретним *ключем*, який використовується як алгоритмом шифрування для перетворення відкритого тексту у криптотекст, так і алгоритмом дешифрування для зворотнього перетворення. У прикладі описана найпростіша криптографічна ситуація. Схематично вона зображена на рис. 1.

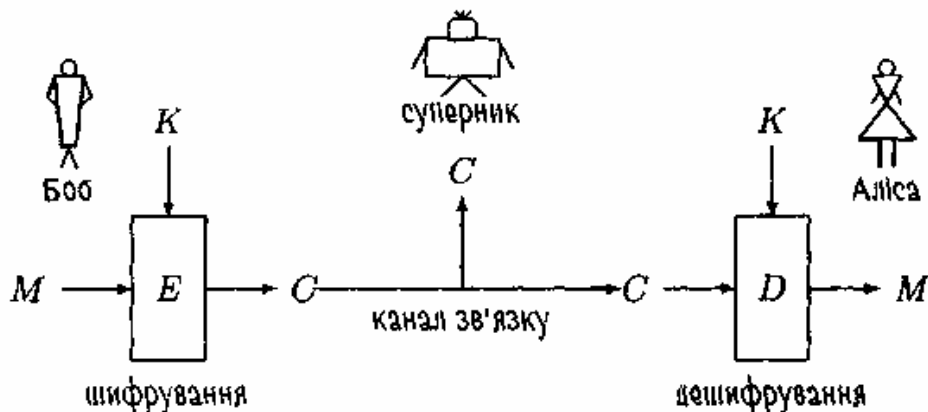


Рис.1. Класична криптографічна схема

Літерами M та C на малюнку позначено відкритий текст та криптотекст, а літерою K — ключ. Літерами E та D позначені алгоритми шифрування та дешифрування відповідно.

Те, що криптотекст C є результатом застосування алгоритму E до відкритого тексту M та ключа K , записуватимемо як $C = E_K(M)$. Подібним чином, запис $M = D_K(C)$ означає, що M отримується із C та K за допомогою алгоритму D .

Аналізуючи надійність шифру, ми зобов'язані виходити із припущення, що суперник не лише здатен підслухати C , але й знає алгоритми E і D , і тільки ключ K йому невідомий.

Для знаходження M суперник може скористатися методом *повного перебору*. Тобто, суперник може перебирати всі можливі ключі K і обчислювати $D_K(C)$ доти, доки не натрапить на осмислений текст, який вірогідно і буде шуканим. Тому у надійної криптосистеми кількість можливих ключів мусить бути досить великою, щоб повний перебір не можна було зробити ні за який розумний час навіть з використанням швидкодіючої обчислювальної техніки.

Якщо суперникові пощастило віднайти спосіб знаходження повідомлення за криптотекстом, то кажуть, що він *розкрив* шифр. *Криптографія* є мистецтвом створення шифрів, а *криптоаналіз* — їх розкриття. Тож респектабельніше називати суперника *криптоаналітиком*. Криптографія та криптоаналіз — дві складові *криптології*. Зрозуміло, що поділ дещо умовний, адже криптограф не може бути впевненим у надійності шифру без проведення його криптоаналізу. У ширшому трактуванні, завдання криптоаналізу не лише ламати шифри, тобто доводити їх ненадійність, але й навпаки, доводити у вигляді математичної теореми надійність шифру, попередньо означивши, який саме шифр слід вважати надійним.

Отже, перед криптоаналітиком стоїть завдання відновити повідомлення M . Згідно із традиційною термінологією, він проводить *атаку* на шифр. Так, метод повного перебору ключів ми будемо називати також *брутальною атакою*. Для розв'язування свого завдання криптоаналітик може мати різні передумови. Для останніх прийнята така класифікація.

Атака лише із криптотекстом. Суперник знає лише криптотекст $E_K(M)$. Досі саме така ситуація і малася на увазі. У гіршому випадку (кращому з погляду суперника), крім $E_K(M)$ відома ще певна кількість криптотекстів $E_K(M_1), \dots, E_K(M_l)$, зашифрованих з використанням одного й того ж ключа.

Атака з відомим відкритим текстом. Крім $E_K(M)$ суперник знає як додаткові криптотексти $E_K(M_1), \dots, E_K(M_l)$, так і відповідні їм відкриті тексти M_1, \dots, M_l (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 $E_K(M_1), \dots, E_K(M_l)$ для вибраних на власний розсуд відкритих текстів M_1, \dots, M_l (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 $D_K(M_1), \dots, D_K(M_l)$ для вибраних на власний розсуд криптотекстів C_1, \dots, C_l

(однак, як і у випадку попередньої атаки, неспроможний отримати безпосередньо таємний ключ).

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.

Тайнопис також є ширшим поняттям. Крім криптографічних, він допускає й такі способи збереження таємниці, при яких повідомлення ніяк не перетворюється, а приховується сам факт його існування чи пересилання. Прикладом може служити використання невидимого чорнила.

Вживання термінів *код* та *кодування* як синонімів до *шифру* та *шифрування* є не лише архаїчним, а часто й помилковим. Код — це стало правило для заміни одиниць інформації (букв, слів, цілих фраз) певними символами. Наприклад, SOS є кодом прохання про допомогу, а згідно із ASCII кодом літера *a* кодується двійковою послідовністю 1100001. Коди, які вивчає математична *теорія кодування*, застосовуються з метою дещо протилежною до криптографічної. Повідомлення *шифрується* для того, щоб воно стало незрозумілим, а *кодується* для того, щоб бути зрозумілим навіть після часткового спотворення із-за природних перешкод у каналі зв'язку. Ці два терміни слід чітко розмежовувати тому, що на практиці одна й та ж інформація може підлягати обом діям — у типовій ситуації текст закодовують у двійкову послідовність, її шифрують, а отриманий криптотекст перед відправленням кодують за допомогою коду, який дозволить виправити помилки після передачі.

Історична довідка. Першим шифром, про який збереглася згадка, вважається шифр *Скитала*, який використовувався спартанцями для військових донесень у V ст. до н.е. Скиталою називався дерев'яний валик, на який щільно намотувалась стрічка пергаменту або шкіри. Повідомлення писалося рядками поздовж поверхні так, щоб у рядку на один звій припадала лише одна буква. Знята з валика стрічка містила незрозумілу послідовність букв, яку можна було прочитати лише знову намотавши стрічку на валик такого ж діаметру. Таким чином, ключем у цьому шифрі слугував діаметр валика.

Криптоаналіз відкрили араби. Опис частотного методу є у їхніх писемних джерелах початку XV століття.

Шифри, які використовувались починаючи від античних часів і аж до середини XX століття, можна класифікувати як шифри *перестановки* або *заміни*. *Скитала* і *шифр частоколу* є прикладами шифрів перестановки — при шифруванні всі букви повідомлення зберігаються, лише розміщуються в іншому порядку. *Шифр Цезаря* є прикладом шифру заміни — кожна буква повідомлення замінюється деякою іншою.

З сьогоднішніх позицій можна вважати, що аж до середини нашого століття у криптографії активно розвивались класичні методи. Так, знаменитий шифр часу II-ї світової війни *Enigma* можна трактувати як вдалу на тоді технічну реалізацію шифру Блеза де Віженера, французького криптографа XVI сторіччя. Все ж винахід телеграфу та радіо дав потужний поштовх дослідженням у царині криптології, адже при наявності у суперника відповідного обладнання підслуховування стало для нього зовсім необтяжливою справою. Шифр *одноразового блокноту* був винайдений у 1917 році інженером Гілбертом Вернамом з AT&T для застосування у телетайпній мережі. Цей шифр є *абсолютно надійним*, лише деякі обставини звужують сферу його застосування, як от необхідність мати безпечний канал для обміну довгим ключем.

Перша електронно-обчислювальна машина була сконструйована задля зламу шифру *Enigma* за участю видатного англійського математика Алана Тьюрінга. Поява обчислювальної техніки докорінно змінила критерії ефективності та надійності шифру. Шифр вважається *надійним в обчислювальному сенсі*, якщо його розкриття хоча в принципі й можливе, але навіть на найшвидшому комп'ютері вимагатиме нереального часу (роки, століття і т.д.), після завершення якого будь-яка таємниця стане неактуальною. Популярною криптосистемою, надійною саме в такому сенсі, є DES — стандарт шифрування даних прийнятий у Сполучених Штатах. Шифр одноразового блокноту та DES.

Початком сучасного етапу розвитку криптографії є 1976 рік. З'являються принципово нові криптографічні засоби, що дозволяє називати цей етап революційним. Давня задача збереження конфіденційності повідомлення знайшла нове елегантне розв'язання у концепції відкритого ключа. Кардинальна відмінність криптосистеми із відкритим ключем (за іншою термінологією, асиметричної системи) від системи "дореволюційного зразка" (симетричної системи) полягає в тому, що у криптосистемах з відкритим ключем процедура шифрування стає загальнодоступною, але це не означає як у традиційних криптосистемах, що загальнодоступним є також дешифрування. Поняття ключа розбивається на дві частини: ключ відкритий, та ключ таємний. Загальновідомий відкритий ключ використовується для шифрування, але дешифрування може здійснити лише той, хто володіє таємним ключем. Озброєна новою концепцією, криптографія почала розв'язувати і нетрадиційні доволі софістичні завдання, як от підписування документів у електронній формі, жеребкування телефоном, поділ секрету між кількома особами тощо.

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 (Додаток).

1.3. Розшифрувати криптотекст, отриманий за допомогою шифру зсуву із невідомим ключем:

- a) бвсблбебвсб;
- b) мдодпдбдпчдмд;
- c) фхлфлтлнл;
- d) тсжсусіьгос.

1.4. Зашифрувати повідомлення **переховуватися** за допомогою шифру частоколу висоти

- a) 2;
- b) 3.

1.5. Розшифрувати криптотекст **нйеаінндо**, якщо відомо, що застосовано шифр частоколу невеликої висоти.

1.6. Зашифрувати повідомлення **передача шифрованих повідомлень** за допомогою шифру зсуву на позицію що дорівнює вашому номеру в журналі.

Контрольні питання

1. Що таке криптографія?
2. Що таке криптоаналіз?
3. Що таке криптологія?
4. Принцип шифру Цезаря.
5. Принцип шифру частоколу.
6. Принцип шифру перестановки.
7. В чому різниця або тотожність понять кодування та шифрування.

Лабораторна робота №2

Тема: Класичні методи шифрування.

Мета: Ознайомитись з основними класичними методами шифрування.

Теоретичні відомості

2.1. Шифри простої заміни перетворюють відкритий текст таким чином, що кожен символ замінюється на якийсь Інший. При цьому однаковим символам у відкритому тексті відповідають однакові символи у криптотексті, а різним — різні. Ключем є таблицка, що вказує в який саме символ переходить кожен символ відкритого тексту. Для прикладу, шифр Цезаря в українському алфавіті задається таким ключем:

**абвггдевжзийійклмнопрстуфхцщщюя
ггдевжзийійклмнопрстуфхцщщюяабв**

При шифруванні кожна буква, яка зустрічається у повідомленні, шукається у верхньому рядку і замінюється відповідною буквою із нижнього рядка (пропуски між словами та розділові знаки ігноруються). Алгоритм шифру Цезаря підставляє замість кожної букви алфавіту деяку букву того ж алфавіту. Могла б здійснюватись підстановка будь-яких інших символів, скажімо, ієрогліфів.

Зробивши це припущення, ми можемо підрахувати кількість всіх можливих ключів. Зробимо це для української абетки. Ключ — це таблицка, верхній рядок якої містить всі букви у алфавітному порядку, а нижній — теж всі букви, але довільним чином перемішані. Отже питання полягає в тому, скількома способами можна розмістити всі букви абетки у нижньому рядку. Міркуємо так. Для першої позиції букву можна вибрати 33-ма способами. Після того як вона вибрана, для другої позиції букву можна вибрати вже 32-ма способами, для третьої — 31-м способом і т.д. Для передостанньої позиції вибір здійснюється 2-ма способами, остання ж буква визначена однозначно. Загальна кількість можливостей розмістити букви у всіх 33 позиціях дорівнює добутку $33 * 32 * 31 * \dots * 2$. Таким чином, загальна кількість ключів є $33!$.

В загальному випадку, коли алфавіт налічує n символів, результатом такого ж підрахунку числа всіх ключів буде $n!$. Зауважимо, що серед цієї загальної кількості деякі ключі є непридатними для вжитку, як от тривіальний ключ, у якому нижній рядок збігається з верхнім.

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.

2.2. Частотний аналіз. Як нам відомо з попереднього пункту, шифр заміни над n -символьним алфавітом має $n!$ ключів. Для значень $n = 26,33$ (латинський та український алфавіти) це число є дуже великим. Для його оцінки можна скористатися варіантом формули Стірлінга, звідки для $n=26$ отримуємо $n > 10^{26}$. Число справді велике — нагадаємо, що наша планета існує лише 10^9 років, а наступний льодовиковий період очікується через 14000 років, тобто $4,41504 \cdot 10^{11}$ секунд. Це співставлення переконливо засвідчує безперспективність брутальної атаки на шифр заміни, однак цього недостатньо аби стверджувати, що він є надійним. Виявляється, успішний криптоаналіз можливий за допомогою *частотного методу*.

Частота символу у тексті дорівнює кількості його входжень у цей текст, поділений на загальну кількість букв у тексті. Наприклад, частота букви *а* у тексті **купила мама коника** дорівнює $4/18 = 2/9$, а частота пропуску між словами у цьому ж тексті дорівнює $2/18 = 1/9$. Для кожної мови справджується такий емпіричний факт:

У досить довгих текстах кожна буква зустрічається із приблизно однаковою частотою, залежною від самої букви та незалежною від конкретного тексту.

Частотним методом можна здійснити дешифрування, навіть не знаючи ключа. Для цього обчислюють частоти кожного символу в криптотексті і порівнюють отримані результати з табличкою частот для мови, якою написане повідомлення. Не слід сподіватися, що таким чином можна буде однозначно встановити ключ, але перебір це дозволить скоротити радикально. Наприклад, якщо при шифруванні не ігноруються пропуски між словами, то найпоширеніший символ у криптотексті поза сумнівом відповідає саме пропуску. А відтак стає відомою сукупність символів, що відповідають словам з одної букви (в українській мові це *а,б,в,є,ж,з,і,й,о,у,я*) та словам з двох букв (*це,не,на,до* та інші), що дозволяє ці символи розпізнати ціною справді невеликого перебору. Свою роль при частотному аналізі відіграє та обставина, що кожна мова володіє властивістю *надлишковості*, тобто текст можна поновити навіть коли частина його букв невідома.

Миттєвою є користь від частотного аналізу при розкритті шифру зсуву. Проілюструємо загальну ідею таким прикладом. Нехай нам належить розшифрувати криптотекст ***пццспофнпмлпнбгнефрптмбвмєоп***, який був отриманий шифром зсуву, причому пропуски та розділові знаки ігнорувались. Підраховуємо частоти і зауважуємо, що найбільша, а саме $9/29$, припадає на літеру *п*. Природньо припустити, що у відкритому тексті їй відповідає найпоширеніша в українській мові літера *о*. Це означало б, що

довжина зсуву дорівнює 1. Виконуємо обернений зсув, тобто на одну позицію вліво, і справді отримуємо змістовне повідомлення, що *охоронумолокозаводупослаблено*.

Гомофонний шифр заміни був винайдений великим німецьким математиком Карлом Фрідріхом Гаусом. Цей шифр ґрунтується на ідеї, яка робить підрахунок частот символів безперспективним. Кожна буква відкритого тексту замінюється не єдиним символом як у шифрі простої заміни, а будь-яким символом із декількох можливих. Наприклад, замість а може здійснюватись підстановка будь-якого із чисел 10,17,23,46,55, а замість б — будь-якого із 12,71. Головне, щоб замість різних букв завжди підставлялись різні символи — ця вимога забезпечує можливість дешифрування. Вибір одного з можливих варіантів щоразу робиться випадково. Якщо кількість варіантів для кожної букви пропорційна її частоті в мові, то всі символи у досить довгому криптотексті зустрічатимуться з приблизно однаковою частотою, що не дозволить пов'язати їх з якимись буквами відкритого тексту. Однак 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.

Частотний аналіз може бути корисним і в інших ситуаціях. Наприклад, він дозволяє комп'ютерові без участі людини відрізнити осмислений текст від хаотичного набору символів. Завдяки цьому на машину можна перекласти здійснення брутальної атаки, тобто повного перебору ключів.

2.3. Поліграмні шифри. Послідовність кількох букв тексту називається *поліграмою*. Послідовність із двох букв називається *біграмою* (іноді *диграфом*), а із l букв — *l-грамою*. 3- і 4-грами називають відповідно три- і тетраграмами. *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 довільним наперед обумовленим способом.

Як приклад розглянемо *біграмний* (часом кажуть *диграфний*) шифр, який назвемо *шифром чотирьох квадратів*, хоча насправді він є відміною відомого шифру *Playfair* (початок XVI століття). Цей шифр застосовується до текстів латинкою. Точніше, ми нехтуємо літерою *j*, яка найрідше зустрічається в англomовних текстах, і працюємо з 25-літерним алфавітом. Ключем є чотири квадрати розміру 5 на 5, кожен з яких сформований із всіх 25 букв, розташованих у довільному порядку. Зручно розмістити ці чотири

квадрати так, щоб вони утворювали один великий квадрат як у прикладі на рис.2.1.

k	i	n	g	d	v	q	e	o	k
o	m	a	b	c	w	r	f	m	i
e	f	h	l	p	x	s	h	a	n
q	r	s	t	u	y	t	l	b	g
v	w	x	y	z	z	u	p	c	d

z	y	x	w	v	d	c	p	u	z
u	t	s	r	q	g	b	l	t	y
p	l	h	f	e	n	a	h	s	x
c	b	a	m	o	i	m	f	r	w
d	g	n	i	k	k	o	e	q	v

Рис. 2.1. Приклад ключа для біграмного шифру чотирьох квадратів.

Перед шифруванням із повідомлення вилючаються всі розділові знаки, пропуски між словами, а також літера *j*, після чого повідомлення розбивається на біграми. Кожна біграма заміщується деякою іншою, яка визначається за таким правилом. Перша буква біграми, що підлягає заміщенню, відзначається у верхньому лівому квадраті, а нижня друга— у нижньому правому. Далі беруться дві букви, одна у верхньому правому, а друга у нижньому лівому квадратах, так, щоб разом з двома відзначеними буквами вони утворювали вершини прямокутника. Саме ці дві букви є біграмою, яка з'являється у криптотексті.

Наприклад, при використанні ключа, зображеного на малюнку 2.1, біграма **cr** замінюється біграмою **mo**, а слово **cryptography** перетворюється у **mo pw ti om fx ns**.

Зрозуміло, що для поліграмних шифрів при $l > 1$ підрахунок частот окремих букв алфавіту нічого не дає. Однак для $l = 2$ з успіхом застосовується аналіз частот біграм. У додатку А наведено найпоширені в українській мові біграми.

2.4. Поліалфавітні шифри можна потрактувати як такі шифри заміни, в яких позиція букви у відкритому тексті впливає на те, за яким саме правилом ця буква буде змінена. Ми розглянемо два класичні приклади.

Шифр Віженера. Відкритий текст і криптотекст записуються в одному й тому ж алфавіті. 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. При цьому дотримуємося такої домовленості: *нумерація букв алфавіту починається з нуля*.

Наприклад, для української абетки маємо $a + a = a$, $b + a = b$, $v + b = g$, $y + v = b$. Ця операція природним чином задається так званою таблицею Віженера, яка зображена на рис.2.2.

	а	б	в	г	д	е	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ью
а	а	б	в	г	д	е	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ью
б	б	а	в	г	д	е	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ью
в	в	б	а	г	д	е	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ью
г	г	б	в	а	д	е	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ью
д	д	б	в	г	а	е	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ью
е	е	б	в	г	д	а	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ью
є	є	б	в	г	д	е	а	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ью
ж	ж	б	в	г	д	е	є	а	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ью
з	з	б	в	г	д	е	є	ж	а	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ью
и	и	б	в	г	д	е	є	ж	з	а	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ью
і	і	б	в	г	д	е	є	ж	з	и	а	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ью
й	й	б	в	г	д	е	є	ж	з	и	і	а	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ью
к	к	б	в	г	д	е	є	ж	з	и	і	й	а	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ью
л	л	б	в	г	д	е	є	ж	з	и	і	й	к	а	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ью
м	м	б	в	г	д	е	є	ж	з	и	і	й	к	л	а	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ью
н	н	б	в	г	д	е	є	ж	з	и	і	й	к	л	м	а	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ью
о	о	б	в	г	д	е	є	ж	з	и	і	й	к	л	м	н	а	п	р	с	т	у	ф	х	ц	ч	ш	щ	ью
п	п	б	в	г	д	е	є	ж	з	и	і	й	к	л	м	н	о	а	р	с	т	у	ф	х	ц	ч	ш	щ	ью
р	р	б	в	г	д	е	є	ж	з	и	і	й	к	л	м	н	о	п	а	с	т	у	ф	х	ц	ч	ш	щ	ью
с	с	б	в	г	д	е	є	ж	з	и	і	й	к	л	м	н	о	п	р	а	т	у	ф	х	ц	ч	ш	щ	ью
т	т	б	в	г	д	е	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	а	у	ф	х	ц	ч	ш	щ	ью
у	у	б	в	г	д	е	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	а	ф	х	ц	ч	ш	щ	ью
ф	ф	б	в	г	д	е	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	а	х	ц	ч	ш	щ	ью
х	х	б	в	г	д	е	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	а	ц	ч	ш	щ	ью
ц	ц	б	в	г	д	е	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	а	ч	ш	щ	ью
ч	ч	б	в	г	д	е	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	а	ш	щ	ью
ш	ш	б	в	г	д	е	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	а	щ	ью
щ	щ	б	в	г	д	е	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	а	ью
ью	ью	б	в	г	д	е	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	а
я	я	б	в	г	д	е	є	ж	з	и	і	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ью

Рис.2.2. Таблиця Віженера. Буква $x + y$ знаходиться на перехресті рядка, що відповідає букві x , і стовпчика, що відповідає букві y .

Шифр Віженера застосовують до повідомлення, записаного в рядок без пропусків між словами та розділових знаків. Ключем є слово у тому ж алфавіті. Якщо ключ коротший за повідомлення, то його записують багато разів підряд доки не вийде рядок такої ж довжини. Рядок з розмноженим ключем розміщують під рядком з повідомленням, і букви, що опинилися одна над другою, додають. В результаті отримують ще один рядок тої ж довжини, який і є криптотекстом. Наприклад, шифрування наказу "бороніть королівну від ворогів" з ключем "ключ" відбувається так:

БОРОНІТЬКОРОЛІВНУВІДВОРОГІВ
КЛЮЧКЛЮЧКЛЮЧКЛЮЧКЛЮЧКЛЮЧКЛЮ
ЛАОЇЮЦРФШАОЇЩЦАІГНЗЯМАОЇНЦА

Результатом шифрування є нижній рядок.

Як бачимо, на відміну від шифру простої заміни при використанні шифру Віженера однаковим буквам у відкритому тексті можуть відповідати різні букви у криптотексті. Ця обставина безперечно ускладнює частотний криптоаналіз. Шифр Віженера кілька століть вважався надійним, поки у 60-их роках минулого століття офіцер пруського війська Касискі не виявив, що цей шифр все ж піддається частотному методу. Скористаємось попереднім прикладом для пояснення основної ідеї. Шифр Віженера влаштований так, що при довжині ключа 4 кожна з чотирьох підпоследовностей відкритого тексту перетворюється відповідно до деякого шифру зсуву (на 14, 15, 31 і 27 позицій). За умови, що текст досить довгий, всі чотири довжини зсувів знаходяться стандартним підрахунком частот букв у відповідних підпоследовностях криптотексту. Однак як визначити із криптотексту, що застосовано ключ довжини саме 4? При прискіпливішому погляді на криптотекст зауважуємо у ньому однакові шматки — триграма аої зустрічається тричі, а біграма ца двічі. Природньо припустити, що це зумовлене не випадковістю, а тим, що у відкритий текст у відповідних місцях входить одна й та ж триграма та біграма (справді, у нашому випадку це оро та ів). Те, що дві однакові поліграми відкритого тексту проявились у криптотексті, означає, що відстань між ними є кратною довжині ключа. 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, — і нам лишається випробувати лише три можливості, щоб знайти, яка з них в дійсності має місце.

Зрозуміло, що описана метода може розраховувати на успіх завжди, коли довжина тексту співвідносно із довжиною ключа є великою. За цієї умови слід сподіватись, що текст міститиме чимало однакових біграм та триграм, і частині з них відповідатимуть однакові біграми та триграми у

криптотексті з тої причини, що відстань між ними пропорційна до довжини ключа.

Шифр з автоключем ґрунтується на ідеях Віженера і Кардано. Подібно до шифру Віженера, 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. Якщо розглянути той же приклад, то шифрування відбуватиметься так:

БОРОНІТЬКОРОЛІВНУВІДВОРОГІВ
КЛЮЧБОРОНІТЬКОРОЛІВНУВІДВОР
ЛАОЇОЩЗЛЮЩЗЛЩЦТВДІЙТХРЮДЩТ

2.5. Шифрування блоками. Часто алгоритм шифрування буває призначений для перетворення послідовностей символів лише фіксованої довжини l . Коли ж потрібно застосувати його до більшого тексту, цей текст розбивають на *блоки* — групи по l символів, і кожен блок перетворюють окремо. Такі шифри називаються *блоковими з періодом l* . Якщо загальна кількість символів у тексті не ділиться націло на l , то остання група символів доповнюється до повного блоку довільним наперед обумовленим способом.

Прикладом блокового шифру з періодом l може слугувати будь-який поліграмний шифр, що здійснює заміну l -грам. Стосовно термінології зазначимо, що під поліграмою розуміють послідовність літер деякої природної мови, в той час як блок може складатися із довільних символів, скажімо, цифр.

Шифр Віженера з фіксованою довжиною ключа l теж можна розглядати як блоковий шифр з періодом l .

2.6. Шифри перестановки зберігають всі букви відкритого тексту, але розміщують їх у криптотексті в іншому порядку. Прикладами шифрів перестановки, які нам вже зустрічалися, є шифр частоколу і Ски-тала. Це представники широкого підкласу шифрів перестановки, які називаються шифрами *обходу*. У якості ще одного типового прикладу розглянемо *матричний шифр обходу*. Повідомлення записується рядками у вигляді прямокутної матриці. Криптотекст формується зчитуванням букв із матриці у зміненому порядку, а саме, стовпчиками. При цьому послідовність, у якій зчитуються стовпчики, визначається ключем. Було поширеним задання ключа у вигляді ключового слова, що легко запам'ятовувалось. Порядок зчитування стовпчиків збігався з алфавітним порядком букв ключового слова. Приклад наведено на рис.2.3.

GARDEN	Повідомлення:
<u>416235</u>	DON'T PUT IT OFF TILL
TOMORROW	
DONTPU	Ключове слово:
TITOFF	GARDEN
TILLTO	Криптекст:
MORROW	OTIOTOLRPFTODTTMUFWNTLR

Рис.2.3. Матричний шифр обходу

Дещо відхиляючись від теми, необхідно зазначити, що в наш час вживання в якості ключа для будь-якого шифру зручних для запам'ятовування ключових слів, є досить ризикованим із-за *словникової атаки*. Найпростіший варіант цього методу криптоаналізу полягає в укладанні списку із, скажімо, 100000 найвживаніших ключових слів, включно із географічними назвами та екзотичними термінами. Рафінованіші версії включають лексику із вузько-фахових публікацій автора повідомлення, послідовності із двох-трьох складів китайської мови тощо.

У якості ще одного прикладу шифру перестановки наведемо доволі відомий у популярній математиці *шифр Кардана*. Це блоковий шифр з періодом $l = k^2$, де k парне число. Ключем є вирізаний з паперу в клітинку квадрат розміру k на k , що складається з k^2 клітинок, четверту частину яких, цебто $k^2/4$, прорізають. На малюнку 5 подано приклад для $k = 4$, причому квадрат розліновано пунктиром, а контури чотирьох прорізаних клітинок виділено суцільною лінією.

Нехай потрібно зашифрувати блок повідомлення, у якому k^2 літер. Криптекст записують на клітчастому папері у квадраті k на k . Процедура займає чотири кроки. На першому кроці на аркуш, на якому буде писатись Криптекст, накладають ключ і вписують перші $k^2/4$ літер повідомлення у прорізані клітинки, починаючи з верхнього рядка. На другому кроці ключ повертають на 90 градусів за годинниковою стрілкою відносно центру квадрату і у прорізані клітинки вписують наступні $k^2/4$ літер повідомлення. Подібним чином виконують третій і четвертий кроки — щоразу ключ повертають на 90 градусів і у нові позиції прорізаних клітинок вписують чергові $k^2/4$ літер повідомлення.

Ключ має бути виготовлений у такий спосіб, щоб при повороті прорізані у ключі клітинки попали на вільні клітинки аркуша, і в жодному разі не накладися на клітинки вже заповнені на попередніх кроках. В результаті після четвертого кроку всі k^2 літер блоку повідомлення виявляються розміщеними в деякому порядку у квадраті k на k . Зчитавши їх рядками, отримують криптекст.

На малюнку 2.4. показано процедуру перетворення повідомлення мамамиларамурано у криптотекст *рмрмиаааммлнуаоа*.

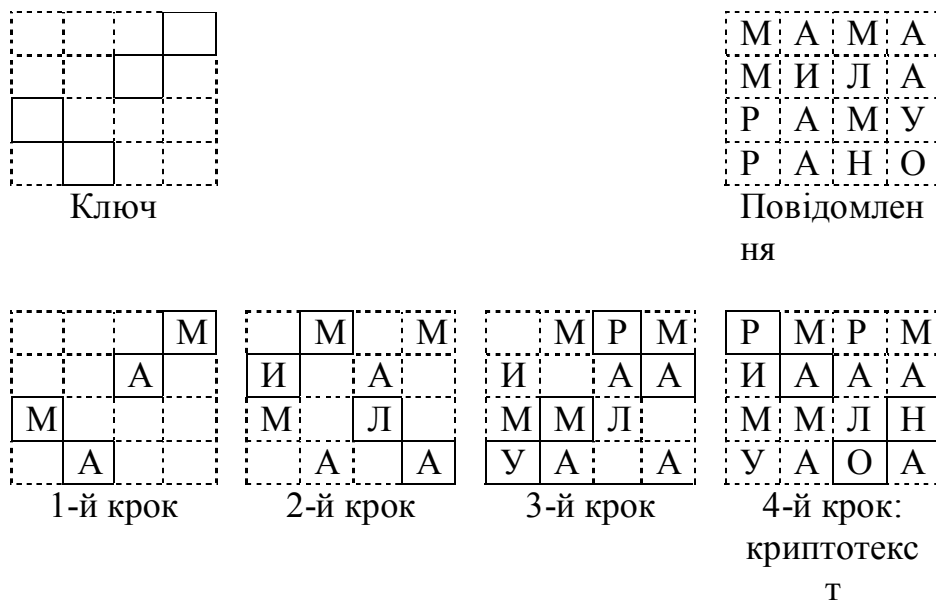


Рис.2.4. Шифр Кардано

Шифр Кардано є шифром перестановки спеціального виду, у якому правило переставлення букв у блоці зручне для реалізації на папері за допомогою ножиць та олівця. Загальний шифр перестановки з періодом l переставляє l букв у довільному порядку, який визначається ключем. Ключ зручно задавати табличкою

$$\begin{bmatrix} 1 & 2 & \dots & l \\ i_1 & i_2 & \dots & i_l \end{bmatrix}$$

яка показує, що перша буква блоку відкритого тексту займає позицію i_1 у відповідному блоці криптотексту, друга буква переміщується на позицію i_2 , і т.д. Наприклад, при $l = 4$ шифр перестановки з ключем

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix}$$

перетворює відкритий текст *мамимиларамурано* у криптотекст *амамалимумаронар*. А зображений на рис.2.4. ключ для шифру Кардано можна задати табличкою

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 4 & 7 & 9 & 14 & 2 & 5 & 11 & 16 & 3 & 8 & 10 & 13 & 1 & 6 & 12 & 15 \end{bmatrix}$$

Міркуваннями, подібними до викладених у пункті 2.1, легко довести, що шифр перестановки з періодом l має $l!$ різних ключів. Якщо l є невеликим у порівнянні з довжиною тексту, шифр перестановки розкривається спеціальним чином організованим аналізом частот біграм. Як саме це відбувається, ми пояснимо на такому прикладі. Нехай маємо криптотекст

ІЦКАЗИВИМЯІЛКИНОЙРЕСПІНЗМЕЛБОПІРПІИТИНИІВІСВИТАЛП

і відомо, що він отриманий шифром перестановки з періодом 5. Розіб'ємо криптотекст на блоки по 5 букв і запишемо їх один під другим, розташувавши текст у десяти рядках та п'яти колонках як показано на малюнку 2.5.

ІЦКАЗ		ЗАКЦІ
ИВИМЯ	<- криптотекст	ЯМИВИ
ИЛКИН	відкритий текст ->	НИКЛИ
ОЙРЕС		СЕРЙО
РПІНЗ		ЗНІПР
МЕЛБО		ОВЛЕМ
ПІРПІ		ИПРИП
ИТИНИ		ИНИТИ
ИВІСВ		ВСІВИ
ИТАЛП		ПЛАТИ
12345	<- Номери СТОВПЧИКІВ ->	54321

Рис.2.5. Криптоаналіз шифру перестановки

Зауважимо тепер, що дешифрування полягає у переставленні стовпчиків у належному порядку. Порядок цей, не знаючи ключа, можна встановити такими міркуваннями. На першій і третій позиціях другого рядка стоїть літера й. Це означає, що перший і третій стовпчики не можуть стояти поруч, інакше ми мали б у відкритому тексті біграму ии, яка ніколи в українській мові не зустрічається, навіть якщо з тексту вилучено пропуски між словами. Зауважуємо також подвійні входження літери и у третьому та сьомому рядках і потрійне входження у восьмому рядку. Беручи до уваги позиції букви и у цих рядках, приходимо до висновку, що не можуть знаходитись поруч 1-й і 4-й, 2-й і 5-й стовпчики, а також будь-які два із 1-го, 3-го та 5-го стовпчиків. Неважко пересвідчитись, що ці вимоги задовольняють лише два розташування стовпчиків — (1,2,3,4,5) та (5,4,3,2,1). Оскільки перше розташування відповідає нашому криптотекстові, то для розташування стовпчиків у відкритому тексті залишається єдина можливість — (5,4,3,2,1), що відповідає ключеві

[1	2	3	4	5]
[5	4	3	2	1]

Здійснивши обернену перестановку, прочитуємо розшифроване повідомлення по рядках:

З АКЦІЯМИ ВИНІКЛИ СЕРЙОЗНІ ПРОБЛЕМИ. ПРИПІНИТИ ВСІ ВИПЛАТИ!

У нашому криптоаналізі ми виходили з апріорно заданої інформації, що шифрування здійснювалось блоками довжини $l = 5$. Якби цього не було відомо, належало б подібний аналіз проводити по чергово для значень $l = 2, 3, 4, \dots$ аж поки б не було досягнуто успіху.

Для максимально наочної ілюстрації загального принципу приклад був підібраний так, що ключ було визначено однозначно на підставі єдиного факту — біграма *ии* зустрічається в українській мові з малою частотою (насправді нульовою). В загальному випадку беруть до уваги й інші малоймовірні буквосполучення, і в результаті отримують систему обмежень на ключ, яка як правило дозволяє суттєво скоротити перебір.

На завершення зробимо ще одне просте зауваження, корисне при атаці з відомим відкритим текстом. У цьому випадку легко визначити, що використовується шифр саме перестановки — досить пересвідчитись, що кожна буква зустрічається в повідомленні та криптотексті з однаковою частотою.

Завдання

2.1. а) Зашифрувати слово *cryptography* за допомогою шифру заміни з ключем

**abcdefghijklm nopqrstuvwxyz
badcfeghijkln mporqtsvuxwzy**

б) Дешифрувати криптотекст *vnjufqtjsz*, отриманий за використанням того ж ключа.

2.2. Порахувати частоти всіх символів у тексті *мама_имила_ираму*.

2.3. В потоці зашифрованих донесень від інформатора з Марийського палацу домінує буква *н*. Припустивши, що використовується шифр зсуву і пропуски між словами ігноруються, знайти за допомогою частотного аналізу ключ і розшифрувати повідомлення

опдрснкнмярстомзйнлопнвнкчдмннкджкшйяспдсшнвн.

2.4. а) Використовуючи шифр чотирьох квадратів із пункту 2.3 з ключем як на малюнку 2.4, зашифрувати слово *university*.

б) Дешифрувати криптотекст *sknqomra*, отриманий за допомогою того ж шифру з тим же ключем.

2.5. а) Зашифрувати повідомлення *білі мухи налетіли*, використавши шифр Віженера з ключем *зима*.

б) Розшифрувати криптотекст *ьччжпчьишисаеяйпявааььч*, отриманий за допомогою шифру Віженера з тим же ключем.

2.6. Показати, що шифр зсуву є частковим випадком шифру Віженера. Який ключ у шифрі Віженера над українським алфавітом слід взяти, щоб отримати шифр Цезаря?

2.7. Вибрати для шифру Віженера довільний ключ довжини а) 3, б) 6 і зашифрувати повідомлення *боронить королівну від ворогів*. У отриманому криптотексті знайти однакові триграми або біграми і порахувати, на якій відстані одна від одної вони знаходяться.

2.8. (Beaufort) Для букви x алфавіту через $\text{---}x$ позначимо *протилежну* їй букву алфавіту, а саме таку, що сума номерів обох букв дорівнює кількості букв у алфавіті. Нагадаємо, що нумерація в алфавіті починається з 0. Покладемо також, що перша буква є протилежною сама до себе. При криптуванні за допомогою шифру Віженера кожна буква c криптотексту отримується із відповідних букв m і k повідомлення і ключа за формулою $c = m + k$, де операція додавання описана у пункті 2.4. Розглянемо модифікацію шифру, при якій криптування здійснюється за формулою $c = (\text{---}m) + k$.

а) Зашифрувати повідомлення білі **мухи** налетіли за допомогою ключа зима.

б) Розшифрувати криптотекст **етишфжвлчишізшюняюшен**, отриманий за допомогою того ж ключа.

с) Довести, що у якості алгоритму дешифрування для цієї модифікації шифру Віженера можна взяти просто алгоритм шифрування. Шифр з такою властивістю називається *інволютивним*.

2.9. а) Зашифрувати повідомлення **білі мухи налетіли**, за допомогою шифру з автоключем, взявши як ключ слово зима.

б) Розшифрувати криптотекст **ьччхюбхоцнпнтвсккпїкш**, отриманий за допомогою того ж шифру з тим же ключем.

2.10. а) Зашифрувати за допомогою матричного шифру обходу з ключем, зображеним на рис.2.3, повідомлення **you must strike while the iron is hot.**

б) Дешифрувати криптотекст **niuhngdsoneuahwtterndrme**, отриманий за допомогою того ж шифру з тим же ключем.

2.11. а) Зашифрувати за допомогою шифру Кардано з ключем, зображеним на малюнку 2.4., слово **недопереповнення.**

б) Дешифрувати криптотекст **ьетуркнейтсисвйи**, отриманий тим же шифром з тим же ключем.

2.12. Виготовити ключ 6 на 6 для шифру Кардано і зашифрувати з його допомогою довільний текст із 36 букв.

2.13. а) Зашифрувати за допомогою загального шифру перестановки з періодом 6 і ключем

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 3 & 4 & 1 \end{bmatrix}$$

СЛОВО *криптоаналіз*.

б) Розшифрувати криптотекст *оеекпреиолтп*, отриманий з допомогою того ж шифру з тим же ключем.

2.14. Перехоплено три криптотексти: **саннаа**, **бббаао** і **укаадк**. Як стало відомо, перші два відповідають повідомленням **ананас** і **баобаб**. Розшифрувати третій криптотекст.

2.15. Використовується шифр перестановки з періодом 5. Визначити ключ і розшифрувати криптотекст

ничаз ніюон курте сюєіц терке ивийн рпбір иниви нненк ьдубі зіюкя зорга щинзи сьтеу рохоя мецно.

2.16. а) Довести, що послідовне застосування шифру простої заміни двічі, один раз з ключем K_1 , а другий раз з ключем K_2 , еквівалентне одноразовому застосуванню шифру заміни з деяким ключем K_3 .

б) Довести, що текст, отриманий за допомогою шифру заміни з ключем K , можна дешифрувати, застосувавши шифр заміни з деяким ключем K' .

с) Нехай в позначеннях попереднього пункту $K' = K$, тобто дешифрування можна здійснити, застосувавши шифр з тим же ключем ще раз. Припустимо також, що при шифруванні з ключем K жоден символ алфавіту не залишається незмінним. Скільки ключів K для шифру заміни у 26-символьному алфавіті мають такі дві властивості?

2.17. Для букви a у n -символьному алфавіті та цілого числа s , означимо їх суму $a + s$ як результат циклічного зсуву букви a на s позицій у алфавіті, вправо якщо $s > 0$ і вліво інакше.

Наприклад, для латинського алфавіту $a + 3 = d$, $b + (-3) = y$.

Довести співвідношення:

а) $a + (я + п) = a + 3$;

б) $(a + s_1) + s_2 = a + (s_1 + s_2)$;

с) $(a + s_1) + s_2 = (a + s_2) + s_1$ для будь-якої букви a та чисел s_1 та s_2 .

2.18. а) Довести, що послідовне застосування шифру зсуву двічі, один раз з ключем s_i , а другий раз з ключем s_r , еквівалентне одноразовому застосуванню шифру зсуву з ключем $(i + r)$;

б) Довести, що криптотекст, отриманий за допомогою шифру зсуву з ключем s , $0 < s < n$, можна дешифрувати, застосувавши шифр зсуву з ключем $(n-s)$.

2.19. а) Скільки різних k -грам є у n -символьному алфавіті?

б) Скільки різних біграм є у алфавіті з 25 букв?

2.20. а) Скільки різних ключів має шифр чотирьох квадратів, описаний у пункті 2.3?

б) Вказати два різні ключі для шифру чотирьох квадратів, шифрування з якими завжди дає однакові результати.

с) Скільки різних ключів має загальний біграмний шифр для 25-символьного алфавіту, який кожен біграму відкритого тексту переводить у біграму криптотексту в тому ж алфавіті (що різні біграми переводяться у різні криптотексти)?

d) Скільки з них можуть бути реалізовані як ключі для шифру чотирьох квадратів?

2.21. а) Розглянувши операцію додавання букв алфавіту, введену в пункті 2.18, довести, що для будь-яких букв x, y , та z виконуються рівності

$$(x + y) + z = x + (y + z) \text{ (асоціативність) та}$$

$$x + y = y + x \text{ (комутативність).}$$

б) Позначимо через X та Y довільні два слова однакової довжини. Довести, що шифрування слова X за допомогою шифру Віженера з ключем Y дає той же результат, що й шифрування слова Y з ключем X .

2.22. а) Довести, що послідовне застосування шифру Віженера двічі, один раз з ключем K_1 і другий раз з ключем K_2 тої ж довжини, еквівалентне одноразовому застосуванню шифру з ключем K_3 , де K_3 можна отримати шифруванням слова K_1 з ключем K_2 .

б) Довести, що послідовне застосування шифру Віженера двічі, один раз з ключем K_1 довжини l_1 і другий раз з ключем K_2 довжини l_2 , еквівалентне одноразовому застосуванню шифру з деяким ключем K_3 довжини l_3 , де l_3 є найменшим спільним кратним чисел l_1 та l_2 .

2.23. Зламати таку версію шифру з автоключем. Якщо ключ має довжину l , то відкритий текст розбивають на блоки довжини l кожен, які послідовно перетворюють у блоки криптотексту наступним чином. Перший блок криптотексту є сумою першого блоку відкритого тексту і ключа. Кожен наступний блок криптотексту отримують сумуванням відповідного блоку відкритого тексту із попереднім блоком криптотексту. (Не знаючи ключа, за криптотекстом можна відновити відкритий текст за винятком перших l літер).

2.24. Довести, що послідовне застосування до досить довгого тексту двох блокових шифрів, одного з періодом l_1 , а другого з періодом l_2 , призводить до шифрування блоками довжини l , де l є найменшим спільним кратним чисел l_1 та l_2 .

2.25. Скільки є для шифру Кардано ключів розміру а) 4 на 4; б) 6 на 6; в) k на k , для парного fc?

2.26. а) Довести, що послідовне застосування шифру перестановки двічі, один раз з ключем K_1 та другий раз з ключем K_2 , еквівалентне одноразовому застосуванню шифру з деяким ключем K_2 (період фіксований).

б) Довести, що криптотекст, отриманий за допомогою шифру перестановки з ключем K , можна дешифрувати, застосувавши той же шифр з деяким ключем K' .

в) Нехай у позначеннях попереднього пункту $A'' = K$, тобто дешифрування можна здійснити, застосувавши шифр з тим же ключем ще раз. Припустимо також, що при шифруванні з ключем K кожна буква переходить на нове

місце. Скільки ключів K для шифру перестановки з періодом I мають такі дві властивості?

2.27. а) Нехай A — шифр перестановки, а B — шифр заміни. Довести, що застосування спочатку шифру A , а потім B , еквівалентне застосуванню спочатку шифру B , а потім A з тими ж ключами. (В такому випадку кажуть, що шифри A і B комутують.)

б) Навести приклад двох шифрів перестановки, які не комутують.

с) Навести приклад двох шифрів заміни, які не комутують.

2.28. Довести, що послідовне застосування до досить довгого повідомлення двох шифрів перестановки з періодами l_1 та l_2 , першого з ключем K_1 а другого з ключем K_2 , еквівалентне одноразовому застосуванню шифру перестановки з деяким ключем K_3 та періодом l_3 , що є найменшим спільним кратним чисел l_1 та l_2 .

Лабораторна робота №3

Тема: Шифр “одноразовий блокнот”.

Мета: Ознайомитися з шифром одноразового блокноту та пов'язаними з ним концепціями.

Теоретичні відомості

Важливо зазначити, що ці два шифри ілюструють два різні поняття надійності. Шифр одноразового блокноту є надійним у *теоретико-інформаційному сенсі*, а DES ось уже двадцять років вважається надійним в *обчислювальному сенсі*.

3.1. Подання тексту у цифровій формі. У період класичної криптографії як правило не виникали потреби записувати відкритий текст та криптотекст якимось інакше, ніж у звичайній абетці. Завдяки цьому криптограф-практик не потребував для роботи нічого, крім письмового приладдя свого часу, чого було достатньо і для шифрування, і для пересилання повідомлення. Але як тільки ми забажаємо скористатися модерними засобами зв'язку для передачі повідомлення, або доручити шифрування комп'ютерові, то виявимо, що у технічному відношенні традиційний текст не є найзручнішою формою для перетворення та передачі інформації.

З цього погляду вигіднішим є подання інформації у *цифровій формі*. Ідея є зовсім простою — кожен символ тексту замінюємо його номером у алфавіті. Нагадаємо, що нумерацію ми домовились починати з 0. Для прикладу, слово банан буде подане як 01 00 17 00 17. Кожна літера представлена своїм номером, записаним двома цифрами, перша з яких може бути нулем. При потребі в алфавіт можна включити окрім букв також знаки пунктуації, пропуск, цифри тощо.

Номери букв ми можемо записувати не в десятковій системі числення, а у двійковій. Для того ж слова банан матимемо запис 000001000000010001000000010001, де кожен блок із шести цифр є номером відповідної букви у двійковому записі. Таку форму подання тексту називатимемо *двійковою*. **Ми потребуємо не менше шести цифр, бо п'ятьма можна записати щонайбільше 32 числа, в той час як українська абетка налічує 33 літери.**

Таким чином, довільний текст можна записати у двійковій формі, використовуючи всього лише два символи — 0 та 1 (один біт). Будь-яку послідовність бітів називають *двійковим словом*.

3.2. Шифр одноразового блокноту був винайдений у 1917 році Гілбертом Вернамом. Він використовує операцію додавання бітів за модулем

2, яку ми розглянемо перед тим як описати сам шифр. Операція позначається символом \oplus і задається так:

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1, \quad 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0.$$

Поширимо цю операцію на двійкові слова однакової довжина домовившись, що додавання таких слів відбувається побітово (не слід плутати цю операцію із звичайним додаванням чисел у двійковій системі. Зокрема, при побітовому додаванні не виникає ніяких переносів у наступний розряд). Наприклад,

$$\begin{array}{r} 000001000000010001000000010001 \\ 001100110101110011011000101011 \\ \hline \end{array}$$

Для двійкових слів X і Y однакової довжини результат їх побітового додавання позначатимемо як $X \oplus Y$. Легко перевірити рівності $X \oplus Y = Y \oplus X$ та $(X \oplus Y) \oplus Z = X \oplus (Y \oplus Z)$, що справджуються для будь-яких двійкових слів X , Y і Z однакової довжини. Для фіксованого k позначимо через 0 двійкове слово $000\dots 00$, що складається із k нулів. Очевидно, що для будь-якого двійкового слова X довжини k виконуються рівності $X \oplus 0 = X$ і $X \oplus X = 0$.

Перейдемо тепер до опису шифру. Перед шифруванням повідомлення M записують у двійковій формі. Ключем K служить довільне двійкове слово однакової з M довжини. Криптотекст C отримують побітовим додаванням повідомлення і ключа, тобто $C = M \oplus K$.

Для прикладу, нехай ми хочемо зашифрувати слово банан. У попередньому пункті ми подали його у двійковій формі:

M - 000001000000010001000000010001. В якості ключа оберемо

K = 001101110101100010011000111010.

Сумування цих двох двійкових послідовностей вже проведене нами вище. Отож маємо криптотекст

C = 001100110101110011011000101011.

Дешифрування у шифрі одноразового блокноту збігається із шифруванням — щоб отримати вихідне повідомлення M , слід додати до криптотексту C той же ключ K . Це легко обгрунтувати: оскільки $C = M \oplus K$, то

$$C \oplus K = (M \oplus K) \oplus K = M \oplus (K \oplus K) = M \oplus 0 = M.$$

Шифр одноразового блокноту є *абсолютно надійним* або, як ще кажуть, *надійним у теоретико-інформаційному сенсі*. Якщо суперник не знає ключа K , то з підслуханого криптотексту C він *зовсім нічого* не може довідатись про повідомлення M . Справді, двійкове слово C могло би бути криптотекстом для *будь-якого* повідомлення M' , якби шифрування здійснювалось з деяким іншим ключем K' , а саме $K' = M' \oplus C$, в той час як

для суперника всі ключі однаково вірогідні. Наприклад, за допомогою деякого ключа K ми щойно перетворили повідомлення банан у криптотекст

$C = 001100110101110011011000101011$.

Але такий же криптотекст ми отримали б, якби зашифрували повідомлення **груша** з ключем

$K' = 001111100001100100000100101011$.

Назва шифру походить від того, що агент, який здійснював шифрування вручну, отримував свої копії ключів записаними у блокноті. Як тільки ключ використовувався, сторінка з ним знищувалась. Зрозуміло, що шифр просто реалізується і технічними засобами. Кажуть, що саме шифр одноразового блокноту використовувався для захисту від підслуховування встановленої під час холодної війни гарячої лінії зв'язку між Москвою і Вашингтоном.

Однак обмеженість сфери застосувань шифру очевидна, оскільки він вимагає ключа такої ж довжини як саме повідомлення. З цією обставиною пов'язані дві проблеми. Перша полягає в генеруванні довгої послідовності випадкових бітів. Другою проблемою є необхідність у надійному каналі для регулярного обміну довгим ключем (на зразок дипломатичної пошти). У більшості ситуацій такого каналу або взагалі нема, або ж він не є достатньо швидким.

На завершення зауважимо, що достеменно такими ж перевагами та недоліками володітиме шифр Віженера, якщо у ньому брати ключ тої ж довжини, що й повідомлення.

3.3. Кількаразове шифрування. Алгоритм, який полягає у шифруванні повідомлення за допомогою одного шифру, а потім застосуванні до отриманого криптотексту ще одного шифру називається *композицією* або *добутком* цих двох шифрів.

Компонування шифрів (утворення їх композиції) часто використовувалось у ранній криптографії. Корисним є також спостереження, що в результаті компонування двох блокових шифрів із взаємно простими періодами період збільшується.

У роки 1-ої світової війни з'явилися *подрібнюючі системи*, чи не найвідомішим представником яких є шифр **ADFGVX**, що застосовувався німецькою армією. ADFGVX є композицією двох шифрів — підстановки і перестановки. Спочатку кожен символ повідомлення, який може бути латинською літерою або десятковою цифрою, замінюється парою символів A, D, F, G, V, або X, згідно із табличкою розміру 6 на 6, як це показано на рис.3.1. Отриманий проміжний криптотекст знову зашифровується, цього разу за допомогою матричного шифру обходу.

У 20-х роках нашого сторіччя були винайдені *роторні* шифрувальні пристрої, які вдосконалювались упродовж наступних десятиліть і інтенсивно

використовувались під час другої світової війни. Прикладом може служити відомий німецький шифр Enigma. Роторні системи реалізовували багатократну композицію шифрів Віженера, що давало шифр з дуже великим періодом.

ADFGVX

A	C08XF4
D	MK3AZ9
F	NWLOJD
G	5SIYHU
V	P1VB6R
X	EQ7T2G

Таблиця білітеральної підстановки-подрібнення.

Повідомлення:

D O N'T PUT IT OFF TILL TOMORROW

Проміжний криптотекст:

FXADFA XGVAGXXGGFXGADAVAVXGGFFFFFXGADDAADVXVX
ADFD

GARDEN	Матриця перестановки. Запис
416235	проміжного криптотексту рядками
FXADFA	і зчитування колонками в порядку
XGVAGX	визначеному ключовим словом
XGGFXG	GARDEN.
ADAVAV	
XGGFFF	Криптотекст:
FFXGAD	XGGDG FAXDA FVFGD DFGXA
DAADVX	FAVFF XXAXF DVAXG VFDXD
VXADFD	AVGAG XAA

Рис.3.1. Шифр ADFGVX.

Частковим випадком композиції двох шифрів є послідовне застосування двічі одного й того ж шифру. Інтуїтивно правдоподібним виглядає припущення, що подвійне шифрування збільшує надійність. Втім, наведемо кілька прикладів, що мають застерегти від покvapливих висновків з цього приводу — питання потребує акуратного розгляду у кожному конкретному випадку.

Спершу припустимо, що обидва рази шифрування здійснюється з одним і тим же ключем. Зрозуміло, що такий спосіб зовсім не ускладнює

брутальну атаку — потрібно перебрати ту ж кількість ключів. Більше того, є так звані *інволютивні* криптосистеми, як от шифр одноразового блокноту, у яких процедура шифрування збігається з процедурою дешифрування. Для таких систем подвійне шифрування залишає повідомлення незмінним!

Перспективнішим видається подвійне шифрування з незалежним вибором ключа кожного разу. Тобто, за допомогою алгоритму шифрування E повідомлення M перетворюється у криптотекст $C = E_{K_2}(E_{K_1}(M))$, де два ключі K_1 та K_2 вибираються незалежно один від одного. Дешифрування не складає труднощів: $M = D_{K_1}(D_{K_2}(C))$ (належить звернути увагу на зміну порядку, в якому застосовуються ключі).

Припустимо, що ключем служить двійкове слово довжини n . В цьому разі всіх можливих ключів є 2^n , а всеможливих пар ключів є 2^{2n} . Однак це не означає, що ламання двократного шифру перебором займе 2^{2n} кроків замість 2^n . Є спосіб оптимізації перевіркою процедури, так звана *зустрічна атака*, що займає кількість кроків пропорційну до 2^n , але взамін вимагає машинної пам'яті такого ж порядку. Це атака з відомим відкритим текстом, для проведення якої потрібно знати якусь пару з повідомлення M та відповідного йому криптотексту C . Зустрічна атака проходить таким чином. Маючи M і C , укладають дві таблиці. В першу поміщають значення $E_K(M)$ для всіх можливих ключів K , а у другу — значення $D_K(C)$ теж для всіх можливих ключів K . Обидві таблички впорядковують згідно з алфавітом, що використовується, і шукають в них однакові пари $E_{K_1}(M) = D_{K_2}(C)$ — слід сподіватися таких виявиться не надто багато. Серед знайдених пар ключів (K_1, K_2) виявиться та, яка справді була використана при подвійному шифруванні.

Для деяких шифрів їх кількарразове застосування не збільшує надійності з тої причини, що для таких шифрів подвійне шифрування з двома ключами K_1 і K_2 дає той же результат, що й одноразове шифрування з деяким ключем K_3 , тобто, для будь-якого повідомлення M виконується рівність $E_{K_2}(E_{K_1}(M)) = E_{K_3}(M)$. Кажуть, що такі шифри *утворюють групу*. Прикладом є шифр одноразового блокноту — легко перевірити, що для нього $K_3 = K_1 \oplus K_2$. Іншими прикладами можуть служити шифр простої заміни, шифри зсуву, Віженера та перестановки.

Розробники шифрів намагаються проектувати шифр так, щоб він не утворював групи. З успішним прикладом є шифр описаний у наступному пункті, присвяченому алгоритмові DES, який здійснює 16-кратне повторення одного й того ж циклу перетворення інформації.

Завдання

3.1. а) Подати у двійковій формі слова **ананас** та **яблуко**.
б) Зашифрувати повідомлення ананас, використавши шифр одноразового блокноту з ключем
110000 011110 010100 110010 010110 011110.

с) З яким ключем той же результат дало б шифрування повідомлення **яблуко**?

3.2 Із скількома різними ключами можна зашифрувати двійкове повідомлення довжини n шифром одноразового блокноту?

3.3. а) Зашифрувати за допомогою шифру **ADFGVX** з ключем, зображеним на рис.3.1, повідомлення
you must strike while the iron is hot.

б) Дешифрувати криптотекст
avxdx gddfa xavxx fxfvx ffgxf fxgga aaxaa agf gx gg,
отриманий з допомогою того ж шифру з тим же ключем.

3.4. Нехай (E, D) — алгоритми шифрування і дешифрування деякої криптосистеми. Криптотекст C отримано із повідомлення M за допомогою ключів K_1, K_2 і K_3 так:

$C = E_{K_3}(D_{K_2}(E_{K_1}(M)))$. Яким чином можна зробити зворотнє перетворення, тобто за C отримати M ?

3.5. Чи утворюють групу шифри:

- а) частоколу;
- б) Скитала;
- с) матричний шифр обходу;
- д) Кардано?

Лабораторна робота №4

Тема: DES-шифр

Мета: Ознайомитись з шифром *DES*, та пов'язаним із ним концепціями.

Теоретичні відомості

Шифр одноразового блокноту є надійним у *теоретико-інформаційному сенсі*, а DES ось уже двадцять років вважається надійним в *обчислювальному сенсі*. Важливо зазначити, що ці два шифри ілюструють два різні поняття надійності.

3.4. DES. *Стандарт шифрування даних* (англійською **Data Encryption Standard — DES**) був розроблений у 70-х роках фахівцями з IBM і у 1976 році був прийнятий через NBS та ANSI у якості федерального стандарту Сполучених Штатів для захисту комерційної та урядової інформації, не пов'язаної з національною безпекою. Цим актом увінчався цілий етап у розвитку криптографії — майже одночасно з'явилися принципово нові криптосистеми з відкритим ключем.

Простежимо уявний шлях від шифру одноразового блокноту до криптосистеми DES. Згадаємо дві основні характеристики першого. З одного боку, шифр одноразового блокноту є абсолютно надійним, а з іншого, він далеко не завжди є практичним через велику довжину ключа. Тому перший крок є таким — довжина ключа має бути фіксованою, а шифрування має відбуватися блоками. Як і шифр одноразового блокноту, DES оперує з інформацією поданою у двійковій формі, а довжина блоку і довжина ключа вибрані рівними 64. Іншими словами, двійкове повідомлення M розбивають на блоки по 64 біти і шифрують кожен блок окремо, використовуючи один і той же двійковий ключ K довжини 64. Таким чином, повідомлення $M = M_1M_2M_3\dots$ перетворюється у криптотекст $C = C_1C_2C_3\dots$, де $C_i = E_K(M_i)$. У стандарті DES кожен блок криптотексту C_i також є двійковою послідовністю довжини 64.

Звернемося до питання вибору алгоритму E . Априорно він повинен задовільняти три умови:

можливість дешифрування, для будь-якого ключа K різним блокам повідомлення M' і M'' відповідають різні блоки криптотексту $E_K(M')$ і $E_K(M'')$, інакше кажучи, алгоритм E_K з будь-яким ключем здійснює перестановку двійкових послідовностей довжини 64;

ефективність, і шифрування, і дешифрування відбуваються швидко;

надійність, якщо ключ невідомий, то немає способу розкриття шифру.

Останній пункт потребує принципового уточнення. Зрозуміло, що як би вдало алгоритм E не був спроектований, надійність, що давалася шифром

одноразового блокноту, вже буде недосяжною. Недосяжною з тої причини, що будь-який блоковий шифр можна зламати за допомогою брутальної атаки, яка у нашому випадку полягає в переборі всіх двійкових ключів K довжини 64. Про яку ж надійність йдеться? Зауважимо, що всього двійкових ключів довжини 64 є 2^{64} . Елементарні обчислення показують, що комп'ютер із тактовою частотою 100 MHz перебиратиме всі можливі ключі $2^{64}/10^8$ секунд, тобто довше ніж 5800 років. Звичайно, повний перебір необхідний лише у найгіршому випадку. У середньому, потрібний ключ буде знайдено вдвічі швидше — приблизно за 2900 років — час, за який таємниця втратить актуальність. Якщо для шифру невідомо методу його ламання упродовж більш реалістичного терміну, то такий шифр вважають *надійним в обчислювальному сенсі*.

Якщо ми хочемо отримати криптосистему надійну у такому новому розумінні, зразу відмовимось від наївної спроби вдосконалити шифр одноразового блокноту і покласти $M_K(M) = M \oplus K$. Таке шифрування є, що приємно, дуже швидке, але, що неприйнятне, вкрай ненадійне. Для розкриття досить просумувати за модулем 2 криптотекст із самим собою, але зсунутим на 64 позиції. Із рівності $K \oplus K = 0$ випливає, що результат буде тим же, що й при сумуванні повідомлення із самим собою зсунутим на ту ж кількість позицій. Із цієї інформації, яка вже ніяк не залежить від ключа, неважко отримати саме повідомлення, запорукою чого є феномен надлишковості будь-якої природної мови.

Розробники стандарту DES пропонують наступну конструкцію (по-дальший опис алгоритму спрощено задля акцентування найважливіших фаз його роботи).

Алгоритм E приймає на вхід двійковий блок M довжини 64 та використовує ключ K , з якого виділяються 16 частин K_1, \dots, K_{16} по 48 бітів кожна. Це так звані *циклові ключі*. Блок M розбивається на дві рівні частини по 32 біти: ліву L_0 та праву R_0 . Відбувається 16 циклів перетворення повідомлення $M = L_0 R_0$. У i -му циклі (L_{i-1}, R_{i-1}) за допомогою K_i перетворюється у (L_i, R_i) наступним чином:

$$\begin{aligned} L_{i-1} &= R_{i-1} \\ R &= L_{i-1} \oplus f(R_{i-1}, K_i), \end{aligned}$$

де f — деяка функція, що перетворює двійкові послідовності довжини 80 у двійкові послідовності довжини 32. Насамкінець ліва та права частини міняються місцями, що і є результатом роботи алгоритму: $E_K(M) = R_{16}L_{16}$.

Неважко перевірити (вправа 3.6), що описана процедура різні блоки M' і M'' перетворює у різні блоки $E_K(M')$ і $E_K(M'')$, незалежно від вибору функції f . Більше того, якщо $E_{K1}, \dots, E_{K16}(M) = C$, то $M = E_{K16}, \dots, E_{K1}(C)$, тобто дешифруючий алгоритм ідентичний із шифруючим, варто лише взяти послідовність ключів у зворотньому порядку.

Функцію f стандарт DES пропонує такої форми: $f(R, K_i) = s(e(R) \oplus K_i)$. Функція e розширює R із 32 бітів до 48, вставляючи копії деяких 16 позицій. Функція s перетворює двійкові послідовності довжини 48 у двійкові послідовності довжини 32. Вона реалізується так. Двійковий вхід A довжини 48 розбивається на 8 блоків $A_1 \dots A_8$ по 6 бітів і кожен блок A_i замінюється на деякий блок із 4 бітів шляхом застосування деякої функції s_i . Кожна із цих 8-ми функцій реалізована незалежно від інших. Реалізації цих функцій називаються *S-блоками*. Після цього отримані 32 біти перемішуються згідно із деякою перестановкою p . Таким чином, $s(A) = p(s_1(A_1) \dots s_8(A_8))$, що й завершує опис алгоритму DES.

Деякі моменти були пропущені. Згідно із стандартом, описана нами процедура починається із переставлення бітів блоку M відповідно до фіксованої перестановки IP і завершується застосуванням до отриманого результату оберненої перестановки IP^{-1} .

Із 64 бітів ключа K алгоритм DES насправді використовує лише 56. Решта бітів можуть служити для перевірки неушкодженості даних при пересиланні ключа — з цією метою кожен восьмий біт покладають рівним сумі за модулем 2 попередніх семи. Кожен із циклових ключів K_1, \dots, K_{16} отримується проектуванням K на деякі 48 координат, які окрім того переставляються місцями.

Кількість циклів у алгоритмі DES дорівнює 16. Чим це краще від, скажімо, двох циклів? Справа в тому, що у випадку двох циклів незначна зміна ключа (наприклад, у кількох бітах) спричиняє таку ж незначну зміну у криптотексті. Ця обставина звужує множину ключів, які досить перебрати для реконструкції початкового тексту. Кількість циклів збільшується для того, щоб кожен біт криптотексту залежав від всіх бітів ключа та від всіх бітів відкритого тексту.

3.5. Рецепти використання блокових шифрів. Шифрування блоками по 64, про яке йшлося у попередньому пункті, називається *режимом простого заміщення* або *режимом електронної кодової книжки*. Певні недоліки такого способу шифрування лежать на поверхні. Зрозуміло, що однакові блоки у відкритому тексті перейдуть у однакові блоки криптотексту — отже деяка інформація про структуру повідомлення все ж буде доступною для суперника. Додатковим внеском у криптоаналіз може бути те, що суперник може знати кілька перших чи останніх блоків відкритого тексту (наприклад, "Вельмишановний Іване Івановичу" чи "Щиро Ваш, Петро Петрович").

Нема гарантій ще й від таких неприємностей. Суперник може перехопити повідомлення і частково його сфальшувати шляхом заміни деяких блоків іншими. Наприклад, у банківському розпорядженні перерахувати значні кошти на певний рахунок зловмисник може змінити номер рахунку на власний. Для цього йому слід раніше переказати самому

собі цілком легально невелику суму грошей, і перехопивши відповідний фінансовий документ, дізнатися з нього номер свого рахунку, зашифрований ключем, що використовується банком того дня.

Всіх цих небезпек можна уникнути, здійснюючи шифрування в інших режимах. Ці режими передбачені стандартом для алгоритму DES, але вони однаково придатні й для інших блокових шифрів.

Зчеплення зашифрованих блоків. До кожного блоку M_i , перед подачею його на вхід алгоритму E , додається за модулем 2 зашифрований попередній блок C_{i-1} . Таким чином, однаковим блокам у відкритому тексті будуть відповідати різні блоки криптотексту. Кожен блок криптотексту у цьому режимі залежить від всіх попередніх, тому підміна якогось блоку повідомлення неминуче буде виявлена адресатом.

Але, якщо два різні повідомлення починаються однаковим блоком, відповідні криптотексти теж будуть мати перший блок однаковий. У певних ситуаціях, це може дати небажану інформацію суперникові. Щоб позбутися цього недоліку, перед шифруванням до повідомлення приписують якийсь випадковий блок — так званий *ініційний вектор*.

Зворотній зв'язок за виходом. У цьому режимі блоковий алгоритм E служить для породження блоків *псевдовипадкових бітів* V_i довжини 64: $V_i = E_k(I_i)$, де I_1 — довільний ініційний вектор, а I_i отримується з I_{i-1} відкиданням перших k бітів і приписуванням справа перших k бітів блоку V_{i-1} . Тут k є фіксованим натуральним числом, меншим від 64. Блок повідомлення M , передається у вигляді криптотексту $C_i = M_i \oplus V_i$.

Зворотній зв'язок за криптотекстом. Цей режим схожий з попереднім, лише для поновлення I_i використовується C_{i-1} замість V_{i-1} .

Завдання

4.1. Нехай (E, D) — алгоритми шифрування і дешифрування деякої криптосистеми. Криптотекст C отримано з повідомлення M за допомогою ключів K_1, K_2 і K_3 так:

$C = E_{K_3}(D_{K_2}(E_{K_1}(M)))$. Яким чином можна зробити зворотнє перетворення, тобто за C отримати M ?

4.2. Чи утворюють групу шифри:

- a) частоколу;
- b) Скитала;
- c) матричний шифр обходу;
- d) Кардано?

4.3. Для двійкового слова X через \bar{X} будемо позначати результат заміни кожного біта у слові на протилежний. Наприклад, $101 = 010$. Нехай E -

алгоритм шифрування стандарту DES. Довести, що $E_K(M) = E_K(M)$ для довільних повідомлення M та ключа K .

4.4. Скількома способами можна було б вибрати функцію s , що фігурує у нашому описі алгоритму DES? (Стандарт задає її явним чином.)

4.5. а) Довести, що якби S-блоки s_i , де $i \leq 8$, були вибрані лінійними функціями з $(\mathbb{Z}_2)^6$ в $(\mathbb{Z}_2)^4$, то DES утворював би групу, яка була б підгрупою групи невироджених лінійних операторів над $(\mathbb{Z}_2)^{64}$.

б) Знайти порядок згаданої групи невироджених лінійних операторів над $(\mathbb{Z}_2)^{64}$.

4.6. Вказати порядок дешифрування повідомлення із m блоків для різних режимів застосування блокових шифрів.

Лабораторна робота №5

Тема: Афінні шифри

Мета: Ознайомитись з афінними шифрами — підклас шифрів заміни, що включає як частковий випадок шифр Віженера і навіть шифр перестановки з фіксованим періодом

Теоретичні відомості

5.1. Шифри простої заміни II. В рамках формалізації моноалфавітні k -грамні шифри заміни можна означити як блокові шифри з періодом k . Відповідно, шифри простої заміни можна трактувати як блокові шифри з періодом 1.

Давайте повернемося ще раз до шифру зсуву, нашого першого прикладу шифру простої заміни (лабораторна робота 1, пункти 1.1.1 та 1.2.1). Подивимось, як можна описати цей шифр із застосуванням арифметичного апарату, розвиненого у попередньому параграфі. Користь такого підходу зрозуміла — обчислювальну техніку майже завжди простіше навчити оперувати із числовою інформацією, аніж із символічною. Основна домовленість, якої ми будемо дотримуватись у цій практичній роботі, така:

n -символьний алфавіт утотожнюємо з кільцем Z_n . А саме, кожна буква замінюється своїм номером у алфавіті, причому нумерація починається з нуля.

Наприклад, латинська абетка утотожнюється із Z_{26} , а українська із Z_{33} - Літера *а* української абетки трактується як **0**, літера *б* як **1**, *в* як **2** і т.д. Тепер до букв відкритого тексту ми можемо вільно застосовувати операції додавання та множення за відповідним модулем.

До кінця практичної роботи **n** буде служити позначенням для кількості букв у алфавіті відкритого тексту. Отже,

Шифр зсуву.

Ключ: s таке, що $0 \leq s < n$.

Шифрування. У повідомленні кожна буква x замінюється буквою $E(x) = (x + s) \bmod n$.

Дешифрування. У криптотексті кожна буква x' замінюється буквою $D(x') = (x' + s') \bmod n$, де $s' = n - s$. Величину зворотнього зсуву s' будемо називати дешифруючим ключем.

За аналогією введемо у розгляд лінійний шифр.

Лінійний шифр.

Ключ: a таке, що $0 < a < n$ і $\text{НСД}(a, n) = 1$.

Шифрування: У повідомленні кожна буква x заміщується буквою $E(x) = (ax) \bmod n$.

Дешифрування: У криптотексті кожна буква x' заміщується буквою $D(x') = (a'x') \bmod n$, де $a' = a^{-1} \bmod n$ — дешифруючий ключ.

Приклад 5.1. Припустимо, повідомлення записуються українською абеткою без пропусків між словами та розділових знаків, тобто $n = 33$. Нехай для шифрування використовується ключ $a = 2$. За допомогою розширеного алгоритму Евкліда знаходимо, що $a' = 17$ (див. приклад 2.9). Розглянемо процедуру шифрування повідомлення **завтра**. У цифровій формі воно представляється послідовністю чисел **9, 0, 2, 22, 20, 0**. Множення на 2 за модулем 33 дає послідовність **18, 0, 4, 11, 7, 0**, яка відповідає криптотекстові **оагіеа**.

Дешифрування відбувається так само, лише із використанням дешифруючого ключа $a' = 17$. Наприклад, якщо ми маємо криптотекст **хдхт = 25, 5, 25, 22**, то множення на 2 за модулем 33 приводить до **17, 10, 17, 11 = нині**.

Співвідношення $D(E(x)) = x$ для будь-якого $x \in Z_n$ доводиться просто: $a'(ax) = (a'a)x = 1x = x$ (операції виконуються в Z_n). Існування a' для a гарантоване умовою $\text{НСД}(a, n) = 1$ за твердженням 2.8. Більше того, a' для заданого a ефективно обчислюється за допомогою розширеного алгоритму Евкліда (приклад 2.9). Нарешті покажемо, що ті a , які не задовольняють накладену нами умову, непридатні для використання в якості ключа.

Твердження 5.2. Відображення $E : Z_n \rightarrow Z_n$, задане формулою $E(x) = (ax) \bmod n$, має обернене тоді і тільки тоді, коли $\text{НСД}(a, n) = 1$.

Доведення. В один бік твердження нами щойно було доведене. Навпаки, припустимо, що відображення E має обернене. За теоремою про обернене відображення (див. кінець пункту 1.1), E сюр'єктивне. Позначимо через ϵ прообраз одиниці: $E(\epsilon) = 1$. Це означає, що $a\epsilon \equiv 1 \pmod{n}$, звідки й випливає, що $\text{НСД}(a, n) = 1$.

Узагальненням і шифру зсуву, і лінійного шифру є

Афінний шифр.

Ключ: a, s такі, що $0 \leq s < n$, $0 < a < n$ і $\text{НСД}(a, n) = 1$.

Шифрування: У повідомленні кожна буква x заміщується буквою $E(x) = (ax + s) \bmod n$.

Дешифрування: У криптотексті кожна буква x' заміщується буквою $D(x') = (a'x' + s') \bmod n$, де пара $a' = a^{-1} \bmod n$ і $s' = (-a's) \bmod n$ є дешифруючим ключем.

Приклад 5.3. Нехай для шифрування використовується ключ $a = 2$, $s = 1$. У прикладі 5.1 було обчислене значення $a' = 17$. Далі, $s' = (-17 \cdot 1) \bmod 33 = 16$. Щоб зашифрувати повідомлення **завтра**, представляємо його у цифровій формі як послідовність **9,0,2,22,20,0**. Множення на 2 за модулем 33 було виконане у прикладі 5.1. До результату додаємо 1 і отримуємо послідовність **19,1,5,12,8,1**, яка відповідає криптотекстові **пбдїжб**.

Дешифрування криптотексту **жсжд = 8, 21, 8, 5** відбувається з використанням дешифруючого ключа $a' = 17$, $s' = 16$. Множення кожного із чисел за модулем 33 на 17 і додавання 16 дає **17,10,17,11 = нині**.

Як і кожен шифр простої заміни, афінний шифр піддається частотному аналізу. При цьому частотний метод використовується навіть не на повну потужність (завдання 5.3 і 5.4).

Завдання

5.1. Для монограмного афінного шифру перевірити співвідношення

$$D(E(x)) = x, \text{ де } x \text{ — довільний елемент із } Z_n.$$

5.2. а) Зашифрувати за допомогою афінного шифру з ключем $a = 4$, $s = 3$ повідомлення **ні**, записане українською абеткою із 33 літер.

б) Знайти дешифруючий ключ і розшифрувати криптотекст **джцзьи**, отриманий за допомогою того ж шифру з тим же ключем.

5.3. а) Каналом зв'язку передаються повідомлення, закриптовані за допомогою монограмного лінійного шифру, причому використовується 35-символьний алфавіт, у якому під номерами від 0 до 32 йдуть літери української абетки, пропуск має номер 33, а крапка — 34. Частотний аналіз показав, що у потоці криптотекстів найчастіше зустрічається літера **Щ**. Опираючись на факт, що найпоширенішим символом в україномовних текстах є пропуск, знайти дешифруючий ключ і розшифрувати криптотекст

ТЬЕПЩЧАЕОЧИЬЯЩЕ_ЛЕАМЮАФ.ГЮОЩХАС_ЕЯ

Знайти шифруючий ключ і закриптувати повідомлення

КРЕВЕТКИ_ЗАКІНЧИЛИСЬ.

б) Повідомлення криптуються з використанням того ж шифру, але використовується 33-символьний алфавіт, в якому лише літери української абетки. Згідно з результатами частотного аналізу, у потоці криптотекстів найчастіше зустрічається літера **Ф**. В числі інших перехоплено крипто текст **УФІЄФГШЖАЙХФ**. Розшифрувати його, опираючись на факт, що найпоширенішою літерою в україномовних текстах є **Ф**. Знайти шифруючий ключ і закриптувати повідомлення **ЗАВЕРШУЙТЕ**.

с) Використовується той же шифр, але над 36-символьним алфавітом. Першими символами алфавіту є крапка, кома та пропуск, які мають номери 0, 1 та 2 відповідно. Номери від 3 до 35 належать літерам української абетки. Відомо, що у потоці криптотекстів найчастіше зустрічаються літери **Є** і **Ь**, саме в такому порядку. Виходячи з того, що найпоширенішими в україномовних текстах є **пропуск** і літера **0**, знайти дешифруючий ключ і розшифрувати криптотекст

ЬЛЮЗІРЄІЄГЯЇВЖГЗИЄГФШЬЯЖ.ЄНІН.

Знайти шифруючий ключ і закриптувати повідомлення

ЗАБУДЬ_УСЕ,_Б0БЕ .

5.4. а) Каналом зв'язку передаються повідомлення, написані у 33-літерному українському алфавіті без пропусків і знаків пунктуації, і закриптовані за допомогою монограмного афінного шифру. Відомо, що у потоці криптотекстів найчастіше зустрічаються літери **У** і **0**, саме в такому порядку. Виходячи з того, що найпоширенішими літерами української абетки є **0** і **Н**, знайти дешифруючий ключ і розшифрувати криптотекст **ЗУКУОН**. Знайти шифруючий ключ і закриптувати повідомлення **ЗАГАСИТИ**.

б) Повідомлення написані англійською мовою у 26-літерному алфавіті без пропусків і розділових знаків, і закриптовані за допомогою монограмного афінного шифру. Відомо, що у потоці криптотекстів найчастіше зустрічаються літери **0** і **Н**, саме в такому порядку. Виходячи з того, що найпоширенішими літерами англійської абетки є **Е** і **Т**, знайти дешифруючий ключ і розшифрувати криптотекст **HSFOSBPSHHSFO**. Знайти шифруючий ключ і закриптувати повідомлення **NOQUESTIONS**.

5.5. а) Довести, що афінне відображення однозначно представляється у вигляді композиції лінійного відображення та зсуву.

б) Довести, що афінний шифр утворює групу (кількість букв у алфавіті відкритого тексту n фіксована).

с) Знайти порядок цієї групи як функцію від n . Обчислити його при $n = 26, 33$.

д) Довести, що лінійні шифри і шифри зсуву утворюють у цій групі підгрупи. Чи є ці підгрупи нормальними?

5.6. *Нерухомою буквою* відносно шифруючого відображення **Е** назовемо букву x із властивістю $E(x) = x$. Скільки букв залишає нерухомими відображення $E(x) = (ax + s) \bmod n$?

Лабораторна робота №6

Тема: Афінні шифри вищих порядків

Мета: Ознайомитись з афінними шифрами вищих порядків

Теоретичні відомості

6.1. Афінні шифри вищих порядків. Як можна розширити монограмні шифри попередньої практичної роботи так, щоб вони оперували з **k**-грамами для довільного $k > 1$? Спочатку введемо операцію додавання в Z_n^k . Сумою векторів $X = (x_1, \dots, x_k)$ і $S = \{s_1, \dots, s_k\}$ з Z_n^k є вектор $X + S = ((x_1 + s_1) \bmod n, \dots, (x_k + s_k) \bmod n)$. Z_n^k з операцією додавання є групою. Вектор $-S = (n - s_1, \dots, n - s_k)$ є оберненим до вектора $S = (s_1, \dots, s_k)$.

Шифр зсуву k -го порядку (шифр Віженера з періодом k).

Ключ: $S \in Z_n^k$.

Шифрування. Повідомлення розбивається на k -грами. Кожна k -грама X заміщується k -грамою $E\{X\} = X + S$.

Дешифрування. Кожна k -грама X' криптотексту заміщується k -грамою $D(X') = X' + S'$, де $S' = -S$ є дешифруючим ключем.

Перед тим як перейти до лінійного шифру нагадаємо, що через $M_k(Z_n)$ ми позначаємо множину матриць розміру $k \times k$ з коефіцієнтами з кільця Z_n , а через $GL_k(Z_n)$ — підмножину оборотних матриць.

Для $A \in GL_k(Z_n)$ обернену до неї матрицю позначаємо через A^{-1} . Добутком AX матриці $A = (a_{ij})$ з $M_k(Z_n)$ на вектор-стовпчик $X = (x_1, \dots, x_k)$ з Z_n^k є вектор-стовпчик

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1k} \\ a_{21} & a_{22} & \dots & a_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ a_{k1} & a_{k2} & \dots & a_{kk} \end{pmatrix} * \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \dots + a_{1k}x_k \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2k}x_k \\ \vdots \\ a_{k1}x_1 + a_{k2}x_2 + \dots + a_{kk}x_k \end{pmatrix}$$

Лінійний шифр k -го порядку.

Ключ: $A \in GL_k(Z_n)$.

Шифрування. Повідомлення розбивається на k -грами. Кожна k -грама X заміщується k -грамою

$E(X) = AX$.

Дешифрування. Кожна k -грама X' криптотексту заміщується k -грамою $D(X') = A'X'$, де $A' = A^{-1}$ — дешифруючий ключ.

Приклад 6.1. Лінійний шифр 1-го порядку обговорювався у попередньому пункті. Розглянемо докладніше випадок $k = 2$, тобто біграмний лінійний шифр. В якості ключа вибирається матриця

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ з коефіцієнтами $a, b, c, d \in Z_n$. Матриця A повинна бути

оберненою. Це рівнозначно умові НСД $(w, n) = 1$ для $w = ad - bc$ — визначника матриці. За цієї умови з допомогою розширеного алгоритму Евкліда ми можемо знайти в Z_n обернений елемент w^{-1} і за формулою оберненої матриці обчислити дешифруючий ключ

$$A^{-1} = \begin{pmatrix} dw^{-1} \bmod n & -bw^{-1} \bmod n \\ -cw^{-1} \bmod n & aw^{-1} \bmod n \end{pmatrix}$$

Наприклад, для $A = \begin{pmatrix} 1 & 1 \\ 32 & 1 \end{pmatrix}$ над Z_{33} маємо $w = 2$.

За розширеним алгоритмом Евкліда знаходимо $w^{-1} = 17$ (див. приклад 2.9) і

$$A^{-1} = \begin{pmatrix} 17 & 16 \\ 17 & 17 \end{pmatrix}$$

Нехай потрібно зашифрувати повідомлення *завтра*. Першій біграмі *за* відповідає вектор $\begin{pmatrix} 9 \\ 0 \end{pmatrix}$.

.....

В результаті дістаємо повідомлення **нині**.

Завдання

6.1. а) Суперник знає, що *Аліса* та *Боб* листуються українською мовою і криптують свою кореспонденцію за допомогою лінійного шифру 2-го порядку. При цьому використовується 34-символьний алфавіт, де номери від 0 до 32 належать літерам української абетки, а 33-тій символом є пропуск. Суперникові вдалося підслухати повідомлення Аліси Бобові:

ГТІШГТРЮІДЖСМАЧДИКЯ_ЄЦЖС.

Він здогадався, що останнім словом у повідомленні є підпис відправника *АЛІСА*. Виходячи з цього припущення, знайти дешифруючий ключ і розшифрувати криптотекст. Знайти шифруючий ключ і закриптувати повідомлення

ЧЕКАЮ_БІЛЯ_ФОНТАНУ_БОБ

б) У тій же ситуації, що й в попередньому пункті, суперник перехопив криптотекст

ДТЛРНІЇРЦДЄЙМЗЧОТШБЕ.

Цього разу суперник здогадався, що повідомлення починається звертанням **БОБЕ**. Розшифрувати криптотекст, виходячи з цього припущення. Знайти шифруючий ключ і закриптувати таке ж, як і в попередньому пункті, повідомлення

ЧЕКАЮ_БІЛЯ_ФОНТАНУ_БОБ

6.2. а) Відомо, що використовується біграмний лінійний шифр над 33-літерним українським алфавітом, занумерованим числами від 0 до 32. Пропуски між словами ігноруються. Статистичний аналіз показав, що в потоці криптотекстів найчастіше зустрічаються біграми **НЮ** і **ПБ**. Виходячи з припущення, що в україномовних текстах з предмету, про який йдеться у повідомленні, найпоширенішими є біграми **СТ** і **НА**, знайти дешифруючий ключ і розшифрувати повідомлення **НЮЛВПБИДИЧТ**

б) Використовується 34-символьний алфавіт, в якому 33-ом літерам російської абетки відповідають номери 0-32, а пропуск має номер 33. Статистичний аналіз показав, що в потоці криптотекстів найчастіше зустрічаються біграми **ЮТ** і **ЧМ**. Виходячи з припущення, що вони відповідають біграмам **НО** і **ЕТ**, найпоширенішим у російськомовних текстах з предмету листування, прочитати підслухане повідомлення **СХНСЬШОНЦЗ**

с) Використовується 26-літерний англійський алфавіт, занумерований числами від 0 до 25. Пропуски між словами ігноруються. Статистичний аналіз показав, що в потоці криптотекстів найчастіше зустрічаються біграми **V0** і **IT**. Припустимо, що в англійськомовних текстах на тему, яка обговорюється в повідомленнях, найчастіше зустрічаються біграми **TH** і **HE**. Знайти дешифруючий ключ і розшифрувати повідомлення **ITEJASVOQOXT**

6.3. а) Повідомлення шифруються лінійним біграмним шифром над 30-символьним алфавітом, в якому номери від 0 до 25 займає латинська абетка, а пропуск, апостроф, кома і крапка, саме в такому порядку, мають номери 26-29. Статистичний аналіз великого масиву криптотекстів показав, що найчастіше трапляються біграми **EI** і **QQ**. Припустимо, що вони відповідають найпоширенішим в англійській мові біграмам E_n і S_n цього алфавіту. Встановити дешифруючий ключ і розшифрувати криптотекст

LHV,QQQWUHESLSEIWYRVGYQUBRBC

б) Відомий розвідник користується біграмним лінійним шифром над 34-символьним алфавітом, у який входять українські літери (0—32) і пропуск (33). Втім, щоб ускладнити криптоаналіз, досвідчений розвідник при шифруванні ігнорує всі пропуски між словами (таким чином, у відкритому тексті немає пропусків, але у криптотексті вони можуть з'явитись). Суперник перехопив повідомлення **ОЩРФНААИЗЖЕБИЗПЗ** розвідника в центр і здогадався, що останні п'ять символів криптотексту відповідають підпису відправника ІСА6В. Провести дешифрування.

6.4. а) Перехоплено криптотекст **ЮВЧРУЗІНДШЛЗТАЬВБЯІТЬГКІ** , отриманий за допомогою лінійного біграмного шифру над 33-літерним алфавітом (пропуски між словами ігноруються). Відомо, що повідомлення закінчується підписом відправника **НАТАЛКА**. Знайти дешифруючий ключ і прочитати по відомлення.

б) Перехоплено криптотекст **ШЩЕВЛОІЩШАФУАРІАБННЕЮ**, отриманий за допомогою лінійного біграмного шифру над 34-символьним алфавітом, у який входить українська абетка (0-33) і пропуск (33). Відомо, що повідомлення закінчується підписом відправника **ВАНГА**. Знайти дешифруючий ключ і прочитати повідомлення.

6.5. Каналом зв'язку передаються повідомлення, закриптовані за допомогою афінного біграмного шифру над 34-символьним алфавітом, у який входить українська абетка (0-33) і пропуск (33). Статистичний аналіз виявив, що найчастіше в потоці криптотекстів зустрічаються біграми РТ, ГД і ІВ. Виходячи з припущення, що вони відповідають найпоширенішим в українській мові біграмам ИП, ИВ та ИИ цього алфавіту, знайти дешифруючий ключ й розшифрувати перехоплений криптотекст

ЛЖІВФХЗРТОЖГДШУССЯВПГЗДБЬІУ

6.6. Перехоплено повідомлення

ЕЬЩИЦЕПІДНІПТЛЧТХХИШХКПСГТНВТУ

отримане за допомогою лінійного шифру 3-го порядку над 33-літерним алфавітом (пропуски між словами ігноруються). Повідомлення закінчується підписом відправника **ДЖЕЙМСБОНД**, що дає можливість встановити відповідність між трьома триграмами повідомлення і криптотексту. Знайти дешифруючий ключ і прочитати повідомлення.

Лабораторна робота №7

Тема: Криптосистеми з відкритим ключем. Система Рабіна

Мета: Ознайомитись з криптосистеми з відкритим ключем та її різновидом системою Рабіна.

Теоретичні відомості

Система Рабіна

Генерування ключів. Вибирають два великі прості числа p і q . Обчислюють їх добуток $n = pq$. Покладають

Відкритий КЛЮЧ: n .

Таємний КЛЮЧ: p, q .

Шифрування відбувається блоками подібно до системи RSA, згідно з формулою

$$E(M) = M^2 \bmod n.$$

Дешифрування. Якщо $E(M) = C$, то M є квадратним коренем числа C за модулем n . За умови НСД $(C, n) = 1$, в Z_n таких коренів є рівно чотири (пункт 3 твердження IV.4.1). Результати пунктів IV.4.3 і IV.4.2 дають ефективний алгоритм добування всіх квадратних коренів за модулем n , який використовує співмножники p і q (тобто таємний ключ!). Саме цей алгоритм використовується в системі Рабіна при дешифруванні. Після знаходження всіх чотирьох коренів з них вибирається той, який є числовим еквівалентом осмисленого тексту.

ЗАУВАЖЕННЯ 7.1. В системі Рабіна шифруюче відображення не є ін'єктивним, але може бути зробленим таким шляхом простої модифікації. Однозначності можна досягти за рахунок передачі разом із крипто-текстом деякої додаткової незашифрованої інформації (вправа 3.2). Це справді необхідно, коли шифрується не текстова, а суто числова інформація.

ЗАУВАЖЕННЯ 7.2. При описі алгоритму шифрування ми виходили з припущення, що НСД $(C, n) = 1$ (це еквівалентно з НСД $(M, n) = 1$). Посилання повідомлень C , для яких НСД $(C, n) > 1$, слід виключити, бо з їх перехопленням суперник отримує нетривіальний дільник НСД (C, n) числа n , тобто дізнається таємний ключ.

ПРИКЛАД 7.3. Нехай таємний ключ вибрано так: $p = 53$ і $q = 67$. Тоді відкритим ключем буде $n = 3551$.

Розглянемо шифрування повідомлення ПРОДАЙ. Як це було зроблено у прикладі 2.1, спочатку повідомлення записується у цифровій формі і розбивається на блоки по чотири цифри: 1920 1805 0013. Перший блок 1920 перетворюється у $1920^2 \bmod 3551 = 0462$. Подібно шифруються наступні два блоки, і в результаті виходить криптотекст 0462 1758 0169.

Припустимо тепер, що ми отримали криптотекст 1497. Для дешифрування слід з нього добути квадратні корені за модулем 3551. З цією метою добуваємо корені за простими модулями 53 і 67 із лишків $1497 \bmod 53 = 13$ і $1497 \bmod 67 = 23$, відповідно. Застосовуємо алгоритм із пункту IV.4.2. Модуль 53 належить до випадку 2, а 67 до випадку 1. Знаходимо $\sqrt{13} \bmod 53 = 15, 38$ і $\sqrt{23} \bmod 67 = 31, 36$. За допомогою алгоритму з Китайської теореми про остачі визначаємо чотири корені з 1497 за модулем 3551: $(15,31) = 0969$, $(15,36) = 1711$, $(38,31) = 1840$, $(38,36) = 2582$. Як зразу видно, лише другий корінь є числовим еквівалентом тексту в українській абетці, а саме повідомлення НІ.

Ефективність. Зауважимо, що при $p \equiv q \equiv 3 \pmod{4}$ алгоритм дешифрування буде особливо простим.

Надійність. Зрозуміло, що задача розкриття системи Рабіна, тобто знаходження за C такого M , що $E(M) = C$, є нічим іншим, як задачею добування квадратного кореня за модулем $n = pq$.

Доведено, що остання задача є такою ж складною, як задача факторизації числа $n = pq$ (яка, до речі, у нашому випадку є задачею знаходження таємного ключа за відкритим).

Завдання

7.1. Нехай $p = 59$ і $q = 67$.

а) Зашифрувати повідомлення ДЕСЯТЬ.

б) Розшифрувати криптотекст 0753 2556.

7.2. Нехай x — квадратичний лишок за модулем $n = pq$, де n є цілим Блюма, тобто p і q — різні прості з властивістю $p \equiv q \equiv 3 \pmod{4}$. Довести, що кожен із чотирьох квадратних коренів з x в Z_n однозначно визначається парою бітів b_1, b_2 , які для $y \in Z_n^*$ рівні

$$b_1 = \begin{cases} 1, & \text{якщо } \left(\frac{y}{n}\right) = 1 \\ 0, & \text{інакше} \end{cases} \quad b_2 = \begin{cases} 1, & \text{якщо } y - \text{непарне ціле} \\ 0, & \text{інакше} \end{cases}$$

7.3. Показати, що система Рабіна нестійка до атаки з вибраним криптотекстом.

Джерела інформації

Основні

1. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ-Петербург, 2000. – 384 с.
2. Блюк О.В., Живко О.О. Захист інформації від промислового шпигунства у сучасному інформаційному просторі. Актуальні проблеми економіки. - 2008. - № 10. - С. 25-34. - ISSN 21- 482.
3. Бойко К. Система технічного захисту інформації в Україні: стан та напрямки розвитку. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - 2005. - № 10. - С. 7-8.
4. Васильєва Є.Н., Пасько Н.Б. Технологія захисту інформації в мережах. Вісник Сумського державного аграрного університету. - 1999. - № 3. - С. 164-168.
5. Вербіцкий О. В. Вступ до криптології. Львів: ВНТА, 1998. – 247 с.
6. Домарёв В. В. Защита информации и безопасность компьютерных систем.- Киев: Diasoft, 1999. – 453 с.
7. Ємець В. та ін. Сучасна криптографія. Основні поняття. Львів: Бак, 2003. – 144 с.
8. Живко М.О., Босак Х.С., Живко І.Ю. Особливості технічно-правового захисту інформації. Актуальні проблеми економіки. - 2008. - № 10. - С. 90-99. - ISSN 21-482.
9. Капіца Ю. Проблеми правової охорони конфіденційної інформації в Україні. Інтелектуальна власність. - 2004. - № 2. - С. 21-28. - ISSN 1608-6422.
10. Корнієнко Т. та ін. Алгоритм та процеси симетричного блокового шифрування. Львів: Бак, 2003. - 168 с.
11. Коталейчук С. Реалізація та захист персоніфікованої інформації у законодавстві України: правове забезпечення. Право України. - 2006. - № 1. - С. 46-50. - ISSN 0132-1331.
12. Люцарев Б. С. и др. Безопасность компьютерных сетей на основе Windows NT. 1998. – 340 с.
13. Маїк Г. Захист інформації- основа безпеки бізнесу. Податкове планування. - 2004. - № 3. - С. 31-40. - ISSN 21-888.
14. Меняйленко А.С. Практикум по основам информатики и вычислительной техники. Ч. 3. Учеб. пособие. - Луганск: Альма-матер, 1999. - 196 с.
15. Меняйленко А.С., Чужба В.А. Методы защиты информации в учебных компьютерных сетях // Наук.-метод. семінар "Комп'ютерні та інноваційні технології у навчальному процесі". 20-21 жовтня 2000 р. (м. Алчевськ). - Алчевськ, 2000. - С. 30-33.

16. Олійник О. Захист інформації в умовах інформаційного суспільства. Право України. - 2005. - № 10. - С. 100-103. - ISSN 0132-1331.
17. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы технологии, протоколы. Учебник для вузов. - СПб.: Питер, 2006. – 672 с.
18. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб. пособие для вузов/ Белкин П.Ю., Михальский О.О., Першаков А.С. и др.- М.: Радио и связь, 2000. – 168 с.

Додаткові

1. Авраменко В.Ф. Правові основи охорони інформації/ Авраменко В.Ф., Брудний Г.О., Жлобін С.І., Лазарев Г.П., Дорошко В.О.- К.: ТОВ „Поліграф Консалтинг", 2003.-173 с.
2. Алферов А.П. Основы криптографии / Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.// Учебное пособие, 2-е изд., испр. и доп.- М.: Гелиос АРВ, 2002. – 480 с., ил.- ISBN 5-85438-025-0.
3. Аникин И.В. Методы и средства защиты компьютерной информации /И.В. Аникин, В.И. Глова // Учебное пособие. Казань: Изд-во Казан. гос. техн. ун-та, 2005. - с. 417.
4. Аршинов М.Н., Садовский Л.Е. Коды и математика (Рассказы о кодировании).- М.: Наука, 1983. – 144 с.
5. Баричев С.Г., Серов Р.Е. Основы современной криптографии. V 1.3. – М.: Горячая линия-Телеком, 2001.- 140 с.
6. Баричев С.Г. Основы современной криптографии / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. –М.: Горячая Линия – Телеком, 2002.- 175 с. - ISBN: 5-93517-075-2
7. Биячуев Т.А. / под ред. Л.Г.Осовецкого Безопасность корпоративных сетей. – СПб: СПб ГУ ИТМО, 2004.- 161 с.
8. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Алгоритмические основы эллиптической криптографии.- М.: Изд. Московского энергетического института.- 2000, 110 с. (классика, подпись DSS, RSA)
9. Брассар Ж. Современная криптология: Пер. с англ.- М.: Издательско-полиграфическая фирма ПОЛИМЕД, 1999. -176 с. ил.- ISBN 5-8832-010-2.
10. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии. -М.: МЦНМО, 2003.-328 с. - ISBN 5-94057-103-4.
11. Введение в криптографию /Под общ. ред. В. В. Яценко – М.: МЦНМО, 2000. - 272 с.- ISBN 5-900916-26-X.
12. Галуев Г.А. Математические основы криптологии: Учебно-методическое пособие. Таганрог: Изд-во ТРТУ, 2003.-120 с.
13. Галатенко В.А. Основы информационной безопасности. Интернет-

- университет информационных технологий - ИНТУИТ.ру, 2008.
14. Гарден М. От мозаик Пенроуза к надежным шифрам: Пер. с англ.-М.: Мир, 1993.- 416 с., ил.-ISBN 5-03-001991-X.
 15. Державний стандарт України ДСТУ 3396.0-96. Захист інформації. Терміни та визначення. - К.: Держстандарт України, 1996. -16с.
 16. Державний стандарт України ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні поняття, - К.: Держстандарт України, 1996.-8с.
 17. Державний стандарт України ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. - К.: Держстандарт України, 1996.-11 с.
 18. Ерош И.Л. Дискретная математика. Математические вопросы криптографии: Учеб. пособие/ СПбГУАП. СПб., - 2001, 56 с.
 19. Жельников В. Криптография от папируса до компьютера. – М.: АБФ, 1997. – 336 с. - ISBN 5-87484-054-0.
 20. Закон України "Про інформацію" від 02.10. 1992 р. №2657-XII.
 21. Закон України "Про науково-технічну інформацію" від 25.06. 1993 р. №3322-XII.
 22. Закон України "Про державну таємницю" від 21.01. 1994 р. №3855-XII.
 23. Закон України "Про захист інформації в автоматизованих системах" від 05.07. 1994р.№80/94-ВР.
 24. Закон України "Про Концепцію Національної програми інформатизації" від 04.02. 1998 р. №75/98-ВР.
 25. Закон України "Про ліцензування певних видів господарської діяльності" від 01.06. 2000 р. №1775-III.
 26. Закон України "Про стандартизацію" від 17.05. 2001 р. №2408-III.
 27. Закон України "Про авторське право і суміжні права" від 23.12. 1993 р. №3792-XII (в редакції закону України від 11.07. 2001 р. №2627-III, з подальшими змінами та доповненнями).
 28. Закон України "Про електронні документи та електронний документообіг" від 22.05. 2003 р. №851-IV.
 29. Закон України "Про електронний підпис" від 22.05. 2003 р. № 852-IV.
 30. Закон України "Про охорону прав на промислові зразки" від 15.12.1993 р. №3688-XII (із змінами і доповненнями станом на 01.01. 2004р.).
 31. Закон України "Про охорону прав на знаки для товарів і послуг" від 15.12. 1993 р. №3689-XII (із змінами і доповненнями станом на 01.01. 2004 р.).
 32. Захист інформації та криптологія. Тимчасова навчальна програма навчальної дисципліни для підготовки бакалаврів напряму 6050 "Економіка та підприємництво" спеціальності 6.050100 - "Економічна кібернетика"/ Арапов С.М., Денисюк В.О. - Вінниця: ВДАУ, 2009.-16 с.
 33. Зензин О.С., Иванов М.А. Стандарт криптографической защиты – AES.

- Конечные поля / Под ред. М.А. Иванова – М.: КУДИЦ-ОБРАЗ, 2002.- 176 с. – ISBN 5-93378-046-4.
34. Зубов А.Ю. Совершенные шифры.- М.: Гелиос АРВ, 2003.- 160 с., ил. – ISBN 5-85438-076-5.
35. Институт криптографии, связи и информатики Академии ФСБ. [Электронный ресурс]. Режим доступа: <http://www.fssr.ru/>
36. Казарин О.В. Теория и практика защиты программ. – М.:Издательство МГУЛ, 2004. – 450 с.
37. Коблиц Н. Курс теории чисел и криптографии. – М.: Научное изд-во ТВП, 2001.- 254 с.
38. Конеев И. Р., Беляев А. В. Информационная безопасность предприятия. – СПб: БХВ-Петербург, 2003.- 752 с. – ISBN 5-94157-280-8.
39. Коутинхо С. Введение в теорию чисел. Алгоритм RSA/ С. Коутинхо.- М.: Постмаркет, 2001.- 328 с. - ISBN: 5-901095-09-X .
40. Куприянов А.И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений / А.И.Куприянов, А.В.Сахаров, В.А.Шевцов.- М.: Издательский центр “Академия”, 2006. - 256 с.- ISBN 5-7695-2438-3.
41. Лапони́на О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. Интернет-университет информационных технологий - ИНТУИТ.ру, 2005.
42. Лидовский В.В. Теория информации: Учебное пособие.- М.: Компания Спутник+, 2004. – 111 с.- ISBN 5-93406-661-7.
43. Лу́жецкий В.А. Інформаційна безпека: навчальний посібник/ Лу́жецкий В.А., Войтович О.П., Дудатьєв А.В. – Вінниця: УНІВЕРСУМ-Вінниця, 2009.- 240 с. ISBN 978-966-641-297-6.
44. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. Пособие для вузов.- М.:Горячая линия-Телеком, 2004.- 280 с.- ISBN 5-93517-197-X.
45. Математические и компьютерные основы криптологии: Учеб. Пособие / Ю.С.Харин, В.И.Берник, Г.В.Матвеев, С.В.Агиевич,- Мн.: Новое знание, 2003.- 382 с.- ISBN 985-475-016-7.
46. Международная ассоциация криптологических исследований. [Электронный ресурс]. Режим доступа: <http://www.iacr.org/>
47. Національний стандарт України. Інформаційні технології. Криптографічний захист інформації. Терміни та визначення. ДСТУ (проект) [Електронний ресурс]. Режим доступу: <http://dstszi.gov.ua/dstszi/doccatalog/document?id=47895>.
48. Нечаев В.И. Элементы криптографии (Основы теории защиты информации): Учеб. Пособие для ун-тов и пед. Вузов/ Под ред. В.А.Садовниченко – М.: Высш. шк., 1999. – 109 с. – ISBN 5-06-003644-8.
49. Новиков Ф.А. Дискретная математика для программистов/ Ф.А.Новиков.-

- Спб.: Питер, 2000.- 304 с.:ил.- ISBN 5-272-00183-4.
50. Озеров В. В. Енигма. [Електронний ресурс]. Режим доступу: http://re.mipt.ru/infsec/2003/essay/2003_History_of_cryptography_Enigma__Ozerov.pdf
 51. Петраков А.В. Основы практической защиты информации. - М.: Радио и связь, 1999.- 368 с. – ISBN 5-256-01507-9.
 52. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000.- 448 с.: ил. – ISBN 5-89818-064-8.
 53. Постанова Кабінету Міністрів України "Про затвердження Концепції технічного захисту інформації в Україні" від 08.10. 1997 р. № 1126.
 54. Правила обов'язкової сертифікації засобів обчислювальної техніки (Затв. наказом Держстандарту України від 25.06. 1997 р. №366).
 55. Правила обов'язкової сертифікації технічних засобів охоронної та охоронно-пожежної сигналізації (Затв. наказом Держстандарту України від 10.04. 1997р. №191).
 56. Рекомендований перелік основних нормативно-правових актів України для використання при провадженні робіт, які здійснюються у межах господарської діяльності у галузі технічного захисту інформації (ТЗІ) та криптографічного захисту інформації (КЗІ). [Електронний ресурс]. Режим доступу: http://www.bezpeka.com/library/law_ua
 57. Романец Ю. В.Защита информации в компьютерных системах и сетях/ Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин – М.: Радио и связь, 2001.- 376 с.- ISBN 5-256-01518-4.
 58. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: Учебное пособие для вузов.- М.: Горячая линия-Телеком, 2005.- 229 с. – ISBN 5-93517-265-8.
 59. Саломаа А. Криптография с открытым ключом: Пер. с англ. – М.: Мир, 1995.- 318 с., ил. – ISBN 5-03-001991-X.
 60. Сمارт Н. Криптография.- М.:Техносфера, 2005.- 528 с. - ISBN 5-94836-043-1.
 61. Сидельников В.М. Криптография и теория кодирования. – М.: Физматлит, 1989.- 128 с.
 62. Тимошенко А.О. Методи аналізу та проектування систем захисту інформації. Текст лекцій. Національний технічний університет України “Київський політехнічний інститут”. Фізико-технічний інститут.- К., 2005.- 174 с.
 63. Фомичев В.М. Дискретная математика и криптология. Курс лекций/ Под общ. ред. д-ра физ.-мат. н. Н.Д.Подуфалова.- М.: Диалог-МИФИ, 2003.- 400 с.- ISBN 5-86404-185-8.
 64. Ховард М., Лебланк Д. Защищенный код: Пер. с англ. — 2-е изд., испр. М.: Издательско-торговый дом “Русская Редакция”, 2004. — 704 стр.: ил.-

ISBN 5-7502-0238-0.

65. Хореев П.Б. Методы и средства защиты информации в компьютерных системах / П. Б. Хореев.- М.: Академия, 2005.- 256 с. -ISBN 5-7695-1839-1.
66. Хорошко В. А. Методы и средства защиты информации/ В. А. Хорошко, А. А. Чекатков. – М.: Юниор, 2003.- 504 с. - ISBN: 966-7323-29-3.
67. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс.- М.: Феникс, 2008.-173 с.- ISBN 978-5-222-13164-0.
68. Цуканова О.А., Смирнов С.Б. Экономика защиты информации: Учебное пособие. – СПб.: СПб ГУИТМО, 2007. – 59 с.
69. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии.-М.: МЦНМО, 2002.- 104 с. – ISBN 5-94057-060-7.
70. Черчхаус Р. Коды и шифры. Юлий Цезарь, "Энигма" и Интернет.- М.: Весь Мир.- 2007, 320 с. - ISBN: 978-5-7777-028104.
71. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. 2-е издание испр. - : издатель-ство "Триумф", 2003.- 815 с. - ISBN 978-5-89392-055-0.
72. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайер. — СПб.: Питер, 2003. — 368 с.: ил. — ISBN 5-318-00193-9.
73. Щербаков Л. Ю., Домашен А. В. Прикладная криптография. Использование и синтез криптографических интерфейсов. — М: Издательско-торговый дом “Русская Редакция”, 2003. — 406 с.: ил. - ISBN 5-7502-0215-1.
74. Эллисон Карл (Carl Ellison) - статьи об инфраструктуре открытого ключа. [Электронный ресурс]. Режим доступа: world.std.com/~cme/.
75. Яковлев А.В./ Криптографическая защита информации : учебное пособие / А.В. Яковлев, А.А. Безбогов, В.В. Родин, В.Н. Шамкин. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2006. – 140 с. – ISBN 5-8265-0503-6.
76. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. — М.: Академический Проект; Гаудеамус, 2-е изд.— 2004. — 544 с. - ISBN 5-8291-0408-3.
77. Horst Feistel, Cryptography and Computer Privacy, Scientific American, May 1973, Vol.228, No. 5, pp. 15-23. Існує російський переклад: Файстель Хорст. Криптография и компьютерная безопасность. [Электронный ресурс]. Режим доступа: <http://www.chat.ru/~avin/feistel.zip>.
78. Orange Book. [Электронный ресурс]. Режим доступа: <http://wnnv.cfnamoo.com/orange>.
79. Shannon C.E. Communication Theory of Secrecy Systems. Bell System Technical Journal. V.28, n.4, 1949, pp. 656-715. Існує російський переклад: Шеннон Клод. Теория связи в секретных системах. [Электронный ресурс]. Режим доступа: http://www.enlight.ru/crypto/articles/shannon/shann_i.htm

Абетки

Українська абетка

А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И
0	1	2	3	4	5	6	7	8	9	10
І	Ї	Й	К	Л	М	Н	О	П	Р	С
11	12	13	14	15	16	17	18	19	20	21
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
22	23	24	25	26	27	28	29	30	31	32

Російська абетка

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
0	1	2	3	4	5	6	7	8	9	10
К	Л	М	Н	О	П	Р	С	Т	У	Ф
11	12	13	14	15	16	17	18	19	20	21
Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
22	23	24	25	26	27	28	29	30	31	32

Латинська абетка

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25