МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЖИТОМИРСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА
ФІЗИКО-МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Методичні рекомендації до організації самостійної/індивідуальної роботи освітньої компоненти «Криптологія»

для підготовки здобувачів першого (бакалаврського) рівня вищої освіти

Укладачі:
Дмитрій ВЕРБІВСЬКИЙ, Юлія МІНГАЛЬОВА,
Розглянуто та схвалено на засіданні кафедри компютерних наук та інформаційних технологій
Протокол від «12» січня 2023 р. № 10
Завідувач кафедри _____ Олена УСАТА

Житомир 2023

УДК 004:056.52(075.8)

В 31

Рекомендовано до друку вченою радою Житомирського державного університету імені Івана Франка від 31 березня 2023 року (Протокол № 6)

Рецензенти:

ПОПЛАВСЬКА Світлана – кандидат педагогічних наук, доцент, доцент кафедри природничих і соціально-гуманітарних дисциплін, проректор з навчальної роботи Житомирського медичного інституту Житомирської обласної ради.

ТОПОЛЬНИЦЬКИЙ Павло – кандидат технічних наук, доцент, доцент кафедри комп'ютерних технологій і моделювання систем Поліського національного університету.

УСАТА Олена – кандидат педагогічних наук, доцент, завідувач кафедри комп'ютерних наук та інформаційних технологій Житомирського державного університету імені Івана Франка.

Методичні рекомендації до організації самостійної/індивідуальної роботи освітньої компоненти «Криптологія» / Уклад.: Д. С. Вербівський, Ю. І. Мінгальова. – Житомир: Вид-во ЖДУ ім. І. Франка, 2023. – 24 с.

Методичні рекомендації до організації самостійної/ індивідуальної роботи освітньої компоненти «Криптологія» укладено для використання здобувачами першого (бакалаврського) рівня вищої. Надаються рекомендації щодо визначення питань методів шифрування та дешифрування даних, криптографічного захисту, використання цифрового підпису.

Для викладачів ЗВО, здобувачів вищої освіти за спеціальністю 122 Комп'ютерні науки, вчителів закладів загальної середньої освіти.

ЗМІСТ

Пояснювальна записка

Сучасні інформаційно-комунікаційні технології впроваджуються в усі сфери людського життя. Інформаційні ресурси стають головною цінністю наукового, економічного та технічного розвитку будь-якої галузі як в Україні, так і у світі. При цьому великого значення набуває проблема захисту даних, що полягає у забезпеченні їх конфіденційності, цілісності та достовірності при зберіганні, обробці та передачі. Постає стратегічно важливе питання якості підготовки вищими навчальними закладами майбутніх фахівців з інформатики, які б у своїй діяльності ефективно використовували різноманітні методи захисту інформації, зокрема криптографічні. Криптографія займається розробкою алгоритмів перетворення повідомлень, в тому числі шляхом шифрування з використанням спеціальних (ключових) даних. Дослідженням вразливих місць таких алгоритмів та розробкою методів зламу зашифрованих повідомлень займається криптоаналіз. Ці два наукових напрями тісно пов’язаних між собою і разом складають науку криптологію.

Предметом вивчення освітньої компоненти є методи перетворення даних шляхом їх шифрування, з метою захисту від незаконних дій користувачів, а також методи та способи розкриття зашифрованих повідомлень.

Мета вивчення освітньої компоненти: оволодіння принципами, методами, засобами побудови класичних та сучасних алгоритмів шифрування та методів їх зламу; формування та набуття загальних та спеціальних компетентностей, практичних знань та вмінь з криптографічного захисту інформаційних ресурсів та криптографічного аналізу.

Основними завданнями вивчення освітньої компоненти є:

• забезпечення ґрунтовного оволодіння студентами основними поняттями, методами та алгоритмами криптології;

• використання класичних шифрів;

• формування у студентів практичних навичок застосування криптосистем із закритим та відкритим ключами.

Компетентності та програмні результати навчання:

Компетентності

Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі комп’ютерних наук або у процесі навчання, що передбачає застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов.

ЗК 2. Здатність застосовувати знання у практичних ситуаціях.

ЗК 6. Здатність вчитися й оволодівати сучасними знаннями.

ЗК 12. Здатність оцінювати та забезпечувати якість виконуваних робіт.

СК 3. Здатність до логічного мислення, побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проектування, розроблення й аналізу алгоритмів, оцінювання їх ефективності та складності, розв’язності та нерозв’язності алгоритмічних проблем для адекватного моделювання предметних областей і створення програмних та інформаційних систем.

СК 14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об’єктів критичної інформаційної інфраструктури.

Програмні результати навчання

ПР 2. Використовувати сучасний математичний апарат неперервного та дискретного аналізу, лінійної алгебри, аналітичної геометрії в професійній діяльності для розв’язання задач теоретичного та прикладного характеру в процесі проектування та реалізації об’єктів інформатизації.

ПР 16. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних.

Перелік питань і тем для самостійного опрацювання та індивідуального виконання. Понятійний апарат теми. Основні терміни

Перелік питань і тем для самостійного опрацювання та індивідуального виконання

1. Вступ. Історія криптології. Основні поняття та визначення.
2. Класифікація шифрів. Цілі, завдання та принципи криптології.
3. Класичні шифри: скитала, квадрат Полібія, шифр Цезаря, шифр частоколу, шифр Віженера, шифр Плейфера, криптосистема Хілла.
4. Загальні відомості про блокові шифри. Шифр одноразового блокнота. Мережа Фейстеля. Стандарт шифрування даних DES. Модифікації DES. Режими шифрування. Міжнародний стандарт шифрування IDEA. Новий стандарт шифрування AES.
5. Ідея криптосистеми з відкритим ключем. Односторонні функції. Алгоритм рюкзака. Алгоритм RSA. Алгоритм Ель-Гамаля.
6. Поняття електронного цифрового підпису (ЕЦП). Порівняння симетричної та асиметричної схеми побудови ЕЦП. Стандарт цифрового підпису DSS. Схеми цифрового підпису RSA та El Gamal. Поняття криптографічного протоколу. Протокол обміну ключами, заснований на системі з відкритим ключем (протокол Діффі-Хелмана).

Понятійний апарат теми.

Модуль І. Загальні основи криптології.

Вступ. Історія криптології. Основні поняття та визначення. Класифікація шифрів. Цілі, завдання та принципи криптології. Класичні шифри: скитала, квадрат Полібія, шифр Цезаря, шифр частоколу, шифр Віженера, шифр Плейфера, криптосистема Хілла.

Модуль ІІ. Криптосистеми із закритим та відкритим ключами.

Загальні відомості про блокові шифри. Шифр одноразового блокнота. Мережа Фейстеля. Стандарт шифрування даних DES. Модифікації DES. Режими шифрування. Міжнародний стандарт шифрування IDEA. Новий стандарт шифрування AES. Ідея криптосистеми з відкритим ключем. Односторонні функції. Алгоритм рюкзака. Алгоритм RSA. Алгоритм Ель-Гамаля. Поняття електронного цифрового підпису (ЕЦП). Порівняння симетричної та асиметричної схеми побудови ЕЦП. Стандарт цифрового підпису DSS. Схеми цифрового підпису RSA та El Gamal. Поняття криптографічного протоколу. Протокол обміну ключами, заснований на системі з відкритим ключем (протокол Діффі-Хелмана).

Основні терміни

Криптологія – наука про захист інформації, шляхом її перетворення. Криптологія поєднує два напрямки – криптографію й криптоаналіз.

Криптографія займається пошуком і дослідженням методів перетворення інформації з метою приховання її змісту. Основні напрямки використання криптографічних методів - передача конфіденційної інформації з каналів зв'язку, установлення дійсності переданих повідомлень, зберігання інформації (документів, баз даних) на носіях у зашифрованому виді.

Криптоаналіз - дослідження можливості розшифровування інформації без знання ключів. У якості інформації, що підлягає шифруванню й розшифровуванню, будуть розглядатися тексти, побудовані на деякому алфавіті.

Алфавіт — кінцева множина використовуваних для кодування інформації знаків. Слід зазначити той факт, що в якості алфавіту можуть виступати як множина символів національних алфавітів, так і множина різних символів і цифр.

Текст — упорядкований набір з елементів алфавіту.

Шифрування - процес перетворення вихідного тексту, який носить також назва відкритого тексту, у шифрований текст.

Дешифрування процес, зворотний шифруванню. На основі ключа шифрований текст перетвориться у вихідний.

Ключ - це конкретний секретний стан деяких параметрів алгоритму криптографічного перетворення даних, що забезпечує вибір тільки одного варіанта з усіх можливих для даного алгоритму. Звичайно ключ являє собою послідовний ряд символів алфавіту.

Простір ключів — це набір можливих значень ключа.

Криптографічна система являє собою сімейство перетворень відкритого тексту.

Криптосистеми підрозділяються на симетричні й асиметричні (або з відкритим ключем).

У **симетричних криптосистемах** для шифрування й для розшифровування використовується один і той самий ключ.

У **системах з відкритим ключем** використовуються два ключі-відкритий і закритий (секретний), які математично зв'язано один з одним. Інформація шифрується за допомогою відкритого ключа, який доступний усім бажаючим, а дешифровується за допомогою закритого ключа, відомого тільки одержувачу повідомлення.

Терміни «**розподіл ключів**» і «**керування ключами**» ставляться до процесів системи обробки інформації, змістом яких є вироблення й розподіл ключів між користувачами.

Електронним цифровим підписом називається його криптографічне перетворення, що приєднується до тексту, яке дозволяє при одержанні тексту іншим користувачем перевірити авторство й дійсність повідомлення.

Криптологічною стійкістю називається характеристика шифру, що визначає його стійкість до розшифровування без знання ключа (тобто криптоаналізу). Є кілька показників криптостійкости, серед яких:

• кількість усіх можливих ключів;

• середній час, необхідний для успішної криптоаналитичної атаки того або іншого виду.

Ефективність шифрування з метою захисту інформації залежить від збереження таємниці ключа й криптостійкости шифру.

Перелік видів роботи з рекомендаціями щодо їх проведення. Завдання для модульних контрольних робіт, самоконтролю

Перелік видів роботи з рекомендаціями щодо їх проведення

В рамках вивчення освітньої компоненти «Криптологія» самостійна робота студентів передбачає такі види діяльності:

- опрацювання лекційного матеріалу, допоміжної літератури;
- написання рефератів, доповідей, статей, презентації виконаної роботи;
- підготовка до тестування, модульної підсумкової роботи, заліку, екзамену;
- розв’язування математичних задач, що лежать в основі криптографічних перетворень;
- виконання практичних завдань за допомогою спеціалізованого програмного забезпечення;
- програмна реалізація алгоритмів шифрування;
- створення програм для шифрування та дешифрування за вказаними шифрами.

Потужним інструментом, що дозволить здобувачам глибше проникнути в суть криптографічних перетворень шляхом їх програмної реалізації в середовищі однієї з мов програмування (C/C++, Pascal, Java) є портал E-Olymp. Даний ресурс було створено на базі Житомирського державного університету імені Івана Франка з метою підготовки обдарованої молоді до дистанційних олімпіад та змагань з програмування. На сьогоднішній день база E-Olymp налічує тисячі задач, які охоплюють теми із криптології. На сайті представлені цікаві задачі, присвячені принципам побудови та функціонування таких криптографічних алгоритмів як шифри Юлія Цезаря, Бекона, Плейфера тощо. Водночас користувачам порталу доступні завдання підвищеної складності, зокрема такі,

що ілюструють роботу деяких алгоритмів хешування, а також основні прийоми та методи криптоаналізу. В результаті самостійного виконання здобувачами вищеописаних завдань на сайті E-Olymp відбувається закріплення, поглиблення та систематизація теоретичних знань з криптології, розвивається абстрактне та логічне мислення, посилюється мотивація до вивчення дисципліни. Варто зауважити, що усі індивідуальні завдання розподіляються викладачем з урахуванням потенційних можливостей та здібностей студентів. Як відомо, розв'язання будь-якої прикладної задачі включає етап побудови її математичної моделі. Проектування роботи криптографічних систем на порталі E-Olymp вимагає практичного застосування знань з різних розділів алгебри, комбінаторики, теорії чисел, теорії алгоритмів, теорії ймовірностей і математичної статистики.

Підготовка теоретичних питань до лабораторних занять передбачає опрацювання теми за питаннями лабораторного заняття. Ці питання могли як розглядати під час лекції, так і повністю виноситися на самостійне опрацювання.

Алгоритм підготовки

1) Визначте питання для підготовки (мають бути розглянути усі питання, вказані у плані лабораторного заняття).

2) Візьміть у бібліотеці університету (читальному залі або на кафедрі) джерела, зазначені у списку основної літератури. При підборі літератури Ви можете користуватися бібліотечними каталогами (алфавітним, предметним або систематичним).

3) Визначте розділи (теми або параграфи), у яких розкрито питання лабораторного заняття.

4) Прочитайте ці розділи.

5) Складіть план (простий або складний) відповіді на кожне питання.

6) Визначте основні поняття, які Ви повинні засвоїти.

7) Проаналізуйте, як опрацьований матеріал пов'язаний з іншими питаннями теми.

8) Для кращого засвоєння та запам’ятовування матеріалу складіть короткий конспект, схеми, таблиці або графіки по прочитаному матеріалу.

9) Визначте проблеми в опрацьованому матеріалі, які Ви недостатньо зрозуміли. З цими питаннями Ви можете звернутися на консультації до викладача.

10) Перевірте, як Ви засвоїли опрацьоване питання. Ви можете це зробити, відповівши на тестові питання до теми або розв’язавши практичні завдання.

Виконання практичних завдань до лабораторних занять передбачає розв’язання запропонованих задач або проведення самостійних досліджень, передбачених робочою програмою з дисципліни.

Алгоритм підготовки

1) Ознайомтеся з планом лабораторного заняття.

2) Перегляньте теоретичний матеріал, необхідний для виконання лабораторного заняття.

3) Детально ознайомтеся з інструкцією до лабораторного заняття.

4) Якщо Ви виконували подібні завдання, перегляньте їх.

5) Виконуйте завдання лабораторного заняття, дотримуючись інструкції.

6) Результати лабораторного заняття подайте у формі звіту.

7) Здайте звіт викладачу у зазначений термін.

Виконання індивідуальних (професійно-орієнтованих) завдань має на меті вироблення умінь, необхідних для вирішення професійних завдань.

Алгоритм виконання

1) Ознайомтеся з вимогами до індивідуального завдання.

2) Ознайомтеся зі змістом індивідуального завдання.

3) Визначте, чи доводилося Вам виконувати подібні завдання.

4) Проаналізуйте теоретичний матеріал, необхідний для виконання індивідуального завдання.

5) Визначте питання, на які Ви не можете дати відповіді самостійно, та зверніться з ними на консультації до викладача.

6) Конкретизуйте завдання, які Ви маєте вирішити в ході виконання індивідуального завдання.

7) Складіть розгорнутий план виконання завдання.

8) Підберіть методи виконання завдання.

9) Виконайте індивідуальне завдання відповідно до плану.

10) Проаналізуйте, чи всі поставлені завдання Ви виконали.

11) Вносіть, при потребі, корективи до виконаного завдання.

12) Оформіть завдання відповідно до вимог.

13) Здайте завдання викладачу у зазначений термін.

Підготовка до підсумкових модульних робіт (ПМР), заліків та екзаменів має на меті узагальнення та систематизацію знань з окремого модуля або освітньої компоненти у цілому.

Алгоритм виконання

1) Ознайомтеся з переліком питань та завдань до ПМР, заліку або екзамену.

2) Підберіть підручники, інструктивно-методичні матеріали або іншу довідкову літературу, необхідну для підготовки (її перелік Ви можете знайти в інструктивно-методичних матеріалах до модуля або курсу).

3) Перегляньте зміст кожного питання, користуючись власними конспектами або підручниками.

4) Визначте рівень знань з кожного питання.

5) Визначте питання, які потребують ретельнішої підготовки (опрацювання додаткової літератури, складання конспектів, схем, розв’язання окремих типів задач тощо). З цією метою зверніться до алгоритму підготовки теоретичних питань до семінарських занять та виконання практичних завдань до лабораторних занять.

6) Для самоперевірки перекажіть теоретичні питання або вирішить практичне завдання.

Примітка

- При виконанні завдань, винесених на самостійне опрацювання, Ви можете звертатися за консультацією до викладача. Про час проведення консультацій повідомляє викладач.
- Теми, які у повному обсязі виносяться на самостійне опрацювання, та індивідуальні завдання студент має здати викладачу на консультації (дату проведення консультації повідомляє викладач).

Завдання для модульних контрольних робіт, самоконтролю

Контрольні запитання:

1. Дайте визначення поняттям: криптологія, криптографія та криптоаналіз.
2. У чому полягає забезпечення конфіденційності, цілісності, дійсності, доступності, спостережливості інформаційних ресурсів?
3. Що таке криптографічний алгоритм та шифр?
4. Що таке криптографічний ключ?
5. Розкрийте поняття зашифрування та дешифрування даних.
6. Дайте визначення відкритого та закритого тексту.
7. Назвіть складові криптографічної системи.
8. У чому полягає криптостійкість криптографічної системи?
9. Дайте коротку класифікацію шифрів.
10. Опишіть алгоритм шифрування Цезаря.
11. У чому суть методу частотного криптоаналізу?
12. Поясніть відмінність між шифрами моноалфавітної та поліалфавітної заміни.
13. Опишіть алгоритм шифрування Віженера.
14. Які кроки потрібно виконати для визначення довжини ключа методом Казіскі?
15. Як уточнити довжину ключа та знайти саме ключове слово методом
16. Фрідмана?
17. Що таке індекс збігу?
18. У чому полягає алгоритм одноразового блокноту?
19. Що являє собою операція XOR?
20. Дайте визначення поняттю «гама». Якими властивостями повинна
21. володіти гама?
22. Які переваги і недоліки шифрування методом одноразового блокноту?
23. До яких шифрів належить стандарт шифрування даних DES?
24. Якою повинна бути довжина ключа у шифрі DES?

25. З яких кроків складається алгоритм шифрування DES.
26. Скільки разів виконується перетворення Фейстеля над блоком у DES?
27. Опишіть кроки шифрування за алгоритмом AES.
28. Від чого залежить кількість раундів шифрування за алгоритмом AES?
29. Які особливості дешифрування за алгоритмом AES.
30. У чому полягає ідея криптосистеми з відкритим ключем?
31. Поняття односторонньої функції.
32. Дайте характеристику алгоритму шифрування RSA.
33. На основі яких операцій відбувається створення закритого ключа із відкритого у RSA?
34. На чому заснована складність зламу алгоритму RSA?
35. Що являє собою гібридна криптосистема?
36. Дайте визначення поняттям «хешування», «хеш-функція».
37. Що таке електронний цифровий підпис?
38. Опишіть схему створення і перевірки ЕЦП.
39. Який порядок використання відкритого та закритого ключів при відправці і перевірці ЕЦП?
40. Як створити зв’язку ключів у GPGShell?
41. Як зашифрувати файл за допомогою GPGShell?
42. Як дешифрувати файл за допомогою GPGShell?
43. Як здійснити цифровий підпис за допомогою GPGShell?
44. Дайте визначення понять «протокол», «криптографічний протокол».
45. Дайте класифікацію криптографічних протоколів.
46. Опишіть алгоритм протоколу обміну ключами Діффі-Хелмана.
47. На чому базується криптостійкість протоколу обміну ключами Діффі-Хелмана?

Список рекомендованої літератури (основна та додаткова, Інтернет ресурси)

Основна:

1. Бабенко Т.В. Криптологія у прикладах, тестах і задачах: навч. посібник / Т.В.Бабенко, Г.М.Гулак, С.О.Сушко, Л.Я.Фомичова. - Д.: Національний гірничий університет, 2013. - 318 с.

2. Загацька Н.О. Криптологія. Методичні рекомендації до виконання лабораторних робіт. / Н.О. Загацька - Житомир: Вид-во ЖДУ, 2015. - 73 с.

3. Криптологія: навч. посібник / М.Н. Курко, П.М. Лісовський, Ю.П. Лісовська. — К.: Видавничий дім «Кондор», 2020. — 248 с.

4. Междорожній, О.М. Цифровий вимірювач переміщення з підвищеною точністю [Текст]: робота на здобуття кваліфікаційного рівня бакалавра; спец.: 171 – електроніка / О.М. Междорожній; наук. керівник І.А. Кулик. – Суми: СумДУ, 2020.– 47 с.

5. Мінгальова Ю. Огляд методів симетричного і асиметричного шифрування даних // Магістратура в умовах євроінтеграційних процесів вищої школи: збірник наукових праць / за заг. ред. С.С. Вітвицької, Н.М. Мирончук.- Житомир: Вид-во ЖДУ ім. І. Франка, 2013. -С. 366 -368

6. Мінгальова Ю. Сучасні криптографічні методи захисту інформації // Сталий розвиток: проблеми та перспективи: зб. наук. праць / за ред. О.А. Дубасенюк – Житомир: Вид-во ЖДУ ім. І.Франка, 2013. - С. 374-380

7. Мінгальова Ю.І. Електронний цифровий підпис як головний елемент електронного документообігу // Перспективні напрями української науки: Збірник статей учасників дев'ятнадцятої всеукраїнської науково-практичної конференції "Інноваційний потенціал української науки – XXI сторіччя" (26 лютого – 6 березня 2013 р.). – Том 2. природничі та точні науки. – Видавництво ПГА. – Запоріжжя, 2013. – С.52-55

8. Мінгальова Юлія. Класифікація методів шифрування // Науковий пошук молодих дослідників: збірник наукових праць студентів, магістрантів та викладачів / за ред. О.М. Королюк – Житомир : Вид-во ЖДУ ім. І. Франка, 2013. – Вип. 6. – С. 62-64.

9. Ходаковський, О.С. Криптографічний захист інформації [Текст]/ О.С. Ходаковський; наук. кер. Р.М. Літнарович. - Рівне: МЕГУ, 2012. – 108 с.

Додаткова:

1. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications [Text]: NIST Special Publication 800-22 Rev1. – Gaithersburg, Maryland: NIST, 2008. – 153 p.

2. Baigneres, T. A Classical Introduction to cryptography Exercise Book [Text] / T. Baigneres, P. Junod, Y. Lu, J. Monneart, S. Vaudenay. – Springer, 2006. – 254 p.

3. Hoffstein, J. An Introduction to Mathematical Cryptography [Text] / J. Hoffstein, J. Pipher, J.H. Silverman. – Springer, 2008. – 523 p.

4. Menezes, A. J. The Handbook of Applied Cryptography [Text] / A. J. Menezes, P. K. Oorschot, S. A. Vanstone. – New York: CRC Press, 1997. – 816 p.

5. Бабаш А., “Таємниця голови раба” Електронний журнал Infused Bytes

6. Вербіцький О.В. Вступ до криптології / О. В. Вербіцький. - Л.: Видавництво науково-технічної літератури, 1998 - 247 с.

7. Вінокуров А., Криптографія, її витоки і місце в сучасному суспільстві. електронний журнал Infused Bytes 19/Жов/98

8. Ємець В. Сучасна криптографія. Основні поняття/ Ємець В., Мельник А., Попович Р. - Л.: БаК, 2003. - 144 с.

9. Захарченко М.В., Йона Л.Г., Щербина Ю.В., Онацький О.В. Розвинення криптології та її місце в сучасному суспільстві: Навч. посібник. – Одеса: ОНАЗ ім. О.С. Попова, 2003. – 80 с.

10. Кривонос О.М. Особливості викладання програмування у вищому начальному закладі з врахуванням вимог сучасності // ВІСНИК Житомирського державного університету імені Івана Франка, 2011. – Вип. 57. - С.131-134

11. Маркова І.І. Захист інформації. Криптографічні методи: Підручник для вищих навчальних закладів. / І.І. Маркова, А.І. Рибак, Ю.С. Ямпольський. - Одеса, 2001. - 175 с.

Інтернет ресурси:

1. CrypTool-Online [Електронний ресурс]. – Режим доступу: https://www.cryptool.org/en/cto.

2. GnuPG [Електронний ресурс]. – Режим доступу: http://www.gnupg.org

3. The CrypTool Portal [Електронний ресурс]. — Режим доступу :

4. Інтернет-портал організаційно-методичного забезпечення дистанційних олімпіад з інформатики для обдарованої молоді України www.e-olymp.com

5. Історія криптології та секретного зв'язку [Електронний ресурс]. – Режим доступу: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/10069/1/%D0%86%D1%81%D1%82%D0%BE%D1%80%D1%96%D1%8F%20%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%97%20%D1%82%D0%B0%20%D1%81%D0%B5%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D0%BE%D0%B3%D0%BE%20%D0%B7%D0%B2%27%D1%8F%D0%B7%D0%BA%D1%83.pdf

6. Комп’ютерна криптографія [Електронний ресурс]. – Режим доступу: http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/12618/met_azarov_25.pdf?sequence=1

7. Криптологія [Електронний ресурс]. – Режим доступу: http://essuir.sumdu.edu.ua/handle/123456789/1026

8. Розвинення криптології та її місце в сучасному суспільстві [Електронний ресурс]. – Режим доступу: https://metod.onat.edu.ua/download/568

Для нотаток

Для нотаток

Для нотаток

Навчально-методичне видання

ВЕРБІВСЬКИЙ Дмитрій Сергійович

МІНГАЛЬОВА Юлія Ігорівна

Методичні рекомендації до організації самостійної/індивідуальної роботи освітньої компоненти «Криптологія»