КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА КІБЕРНЕТИКИ

Кафедра інтелектуальних програмних систем

«ЗАТВЕРДЖУЮ»
Заступник декана
з навчальної роботи

_____ Кашпур О.Ф.

«____»_____2019 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
МАТЕМАТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ

для студентів

галузь знань	**12 «Інформаційні технології»** *(шифр і назва)*
спеціальність	**121 «Інженерія програмного забезпечення»** *(шифр і назва спеціальності)*
освітній рівень	**бакалавр** *(молодший бакалавр, бакалавр, магістр)*
освітня програма	**«Програмна інженерія»** *(назва освітньої програми)*

вид дисципліни обов'язкова

Форма навчання	**денна**
Навчальний рік	**2018/2019**
Семестр	8
Кількість кредитів ECTS	**4**
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**іспит**

Викладачі: **д.ф.-м.н., проф. Кривий С. Л.** (лекції, лабораторні заняття),

Пролонговано: на 20__/20__ н.р. _____(_____) «__»___ 20__р.
(підпис, ПІБ, дата)

на 20__/20__ н.р. _____(_____) «__»___ 20__р.
(підпис, ПІБ, дата)

КИЇВ – 2019

Розробник: Кривий Сергій Лук’янович д.ф.-м.н., професор кафедри «інтелектуальних програмних систем

»

ЗАТВЕРДЖЕНО

Зав. кафедри «інтелектуальних програмних систем»

_____ (Провотар О.І.)
(підпис) (прізвище та ініціали)

Протокол № від « » 2019 р.

Схвалено науково-методичною комісією факультету комп’ютерних наук та кібернетики _____

Протокол від « X » xxxxxxx 2019 року №_

Голова науково-методичної комісії _____ (Омельчук Л.Л)
(підпис) (прізвище та ініціали)

«_____» _____ 20___ року

1. Анотація дисципліни. Дисципліна „ Математичні основи захисту інформації ” є вибірковою дисципліною длоку „Інтелектуальні системи”, що викладається у 8 семестрі для бакалаврів в обсязі 120 год (4-х кредитів), зокрема: 20 годин лекційних, 18 години лабораторних робіт, 80 години самостійної роботи, 2 години консультації. Викладання дисципліни закінчується **іспитом.**

2. Предмет навчальної дисципліни „ Математичні основи захисту інформації ” включає в себе основні поняття симетричних та асиметричних криптографічних систем як класичного так некласичного типу і які ґрунтуються на застосуваннях теорії ймовірностей, теорії складності алгоритмів, теорії груп, кілець та полів, теорії чисел та алгоритми, які використовуються в цих теоріях (найефективніші з алгоритмів). До таких алгоритмів відносяться алгоритми тестування чисел на простоту, алгоритми модульної арифметики та чисельні алгоритми в групах, алгоритми обчислення дискретного логарифма тощо.

3. Попередні вимоги до опанування або вибору навчальної дисципліни

Для успішного вивчення дисципліни «Математичні основи захисту інформації» студент повинен відповідати наступним вимогам:

1. Успішне опанування курсів:
    1. Дискретна математика.
    2. Основи загальної алгебри.
    3. Основи криптології
    4. Основи теорії ймовірностей.
    5. Основи теорії чисел і скінченних автоматів.
    6. Теорія складності алгоритмів і програм
    7. Основи програмування..
2. Знання:
    1. Основних понять та методів дискретної математики.
    2. Основних класів складності та аналізу складності алгоритмів.
    3. Основних дискретних розподілів випадкової величини.
    4. Основних алгебраїчних структур.
    5. Основних алгоритмів теорії чисел.
3. Вміти:
    1. Виконувати аналіз проблеми, що виникає.
    2, Будувати математичні моделі відповідних предметних областей.
    3. Оцінювати стійкість системи до зламу за результатами аналізу.
    4. Користуватися генераторами випадкових чисел, знати їх характеристики.
4. Володіти:
    1. Базовими навичками використання інтегрованих середовищ розробки програмного забезпечення.
    2. Англійською мовою на рівні не нижче Intermediate.

4. Завдання (навчальні цілі):

Основними завданнями дисципліни «Математичні основи захисту інформації» є засвоєння основних математичних ідей, методів та програмних засобів захисту інформації, відповідно до кваліфікації фахівець з інформаційних технологій. Зокрема, розвивати:

- Здатність до абстрактного мислення, аналізу та синтезу (ЗК-1).
- Здатність застосовувати знання у практичних ситуаціях (ЗК-2).
- Здатність спілкуватися державною мовою як усно, так і письмово (ЗК-3).

- Здатність вчитися і оволодівати сучасними знаннями (ЗК-5).
- Здатність до пошуку, обробки та аналізу інформації з різних джерел (ЗК-6).
- Здатність працювати в команді (ЗК-7).
- Здатність приймати обґрунтовані рішення (ЗК-14).

5. Результати навчання за дисципліною:

Результат навчання (1. знати; 2. вміти; 3. комунікація; 4. автономність та відповідальність)		**Форми (та/або методи і технології) викладання і навчання**	**Методи оцінювання та пороговий критерій оцінювання (за необхідності)**	**Відсоток у підсумковій оцінці з дисципліни**
Код	**Результат навчання**			
РН1.1	*Знати основні математичні поняття, які використовуються в криптографічних засобах захисту інформації*	*Лекція, лабораторне заняття*	*Тест, 60% правильних відповідей, екзамен*	15%
РН1.2	*Знати базові типи криптографічних систем, технології проектування, налагодження та тестування правильності роботи систем захисту*	*Лекція, лабораторне заняття*	*Тест, 60% правильних відповідей, екзамен*	20%
РН1.3	*Знати основні алгоритми, які складають основу криптографічного захисту інформаційних систем*	*Лекція, лабораторне заняття*	*Тест, 60% правильних відповідей, екзамен*	15%
РН2.1	*Вміти застосовувати на практиці інструментальні програмні засоби проектування та розробки програмного забезпечення.*	*Лабораторне заняття, самостійна робота*	*Захист лабораторної роботи, екзамен*	14%
РН3.1	*Обґрунтовувати власний погляд на задачу, спілкуватися з колегами з питань проектування та розробки програм, складати письмові звіти*	*Лабораторне заняття*	*Поточне оцінювання, захист ЛР*	10%
РН3.3	*Обгрунтовувати вибір засобів розробки та проектні рішення. Оцінювати стійкість криптосистеми*	*Лабораторне заняття, самостійна робота*	*Поточне оцінювання, захист ЛР*	10%
РН4.1	*Організовувати свою самостійну роботу для досягнення результату*	*Самостійна робота*	*Поточне оцінювання, Захист лабораторної роботи*	8%
РН4.2	*Відповідально ставитися до виконуваних робіт, нести відповідальність за їх якість*	*Лабораторна робота*	*Захист лабораторної роботи*	8%

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання

Результати навчання дисципліни Програмні результати навчання	**РН 1.1**	**РН 1.2**	**РН 1.3**	**РН 2.1**	**РН 3.1**	**РН 3.3**	**РН 4.1**	**РН 4.2**
ПР-13. Знати і застосовувати методи розробки алгоритмів, конструювання програмного забезпечення та структур даних.	+		+	+				
ПРН21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.	+	+	+			+	+	+
ПРН25.1. Знати і застосовувати методи розробки алгоритмів, конструювання програмного забезпечення та структур даних і знань.			+		+	+	+	+
ПРН26.1. Знати та вміти застосовувати методи захисту інформації при створенні програмних систем.			+	+	+	+		+

7. Схема формування оцінки

7.1. Форми оцінювання студентів

Семестрове оцінювання:

1. Контрольна робота 1: РН 1.1, РН 1.2, РН 3.1, РН 4.1, РН 4.2 – 15 балів/9 балів.
2. Контрольна робота 2: РН1.2, РН 1.3, РН 3.1, РН 4.1, РН 4.2 – 15 балів/9 балів.
3. Лабораторні роботи 1-4: РН1.1, РН 1.2, РН 2.1, РН3.1, РН3.2, РН3.3, РН 4.1, РН 4.2, РН 4.3 – 10 балів/6 балів (кожна).
4. Лабораторна робота 5-9: РН1.2, РН1.3, РН 2.1, РН3.1, РН3.2, РН3.3, РН 4.1, РН 4.2, РН 4.3 – 10 балів/6 балів (кожна) .

Підсумкове оцінювання (у формі екзамену):

- максимальна кількість балів які можуть бути отримані студентом: 40 балів;
- результати навчання які будуть оцінюватись: РН1.1, РН1.2, РН1.3, РН2.1;
- форма проведення і види завдань: письмова;
- види завдань: 5 письмових завдань (2 теоретичних питання та 3 практичних завдання);
- для отримання загальної позитивної оцінки з дисципліни оцінка за екзамен повинна бути не меншою ніж 24 бали;
- студент не допускається до екзамену, якщо протягом семестру він набрав менше ніж 36 балів;
- студент не допускається до екзамену, якщо протягом семестру він не виконав та не здав 100 % лабораторних робіт передбачених планом.

Критерії оцінювання на екзамені

Завдання	Тема завдання	Максимальний відсоток від 40 балів	Всього відсотків
Завдання 1	Теоретичні питання за матеріалами курсу	15%	15%
Завдання 2		22,5%	22,5%
Завдання 3	Практичне завдання на основі теоретичного матеріалу курсу	25%	25%
Завдання 4		20%	20%
Завдання 5		17,5%	17,5%
			100%

7.2. Терміни проведення форм оцінювання:

1. Контрольна робота 1: до 7 тижня семестру.
2. Контрольна робота 2: до 14 тижня семестру.
3. Лабораторна робота 1: до 2 тижня семестру.
4. Лабораторна робота 2: до 3 тижня семестру.
5. Лабораторна робота 3: до 4 тижня семестру.
6. Лабораторна робота 4: до 5 тижня семестру.
7. Лабораторна робота 5: до 6 тижня семестру.
8. Лабораторна робота 6: до 7 тижня семестру.
9. Лабораторна робота 7: до 8 тижня семестру.
10. Лабораторна робота 8: до 9 тижня семестру.
11. Лабораторна робота 9: до 10 тижня семестру.

Студент має право на одне перескладання кожної контрольної роботи у визначений викладачем термін.

У випадку відсутності студента з поважних причин відпрацювання та перездачі контрольних робіт здійснюються у відповідності до «Положення про порядок оцінювання знань студентів при кредитно-модульній системі організації навчального процесу» від 1 жовтня 2010 року. Якщо студент пропустив без поважних причин більше половини занять, не виконав хоча б однієї лабораторної роботи або не писав контрольної роботи, то він не допускається до складання екзамену.

Студент повинен здавати лабораторні роботи у назначені викладачем терміни. Якщо лабораторні робота не здається в назначені терміни, вона вважається такою, що не виконана студентом.

8. Шкала відповідності оцінок

Відмінно / Excellent	90-100
Добре / Good	75-89
Задовільно / Satisfactory	60-74
Незадовільно / Fail	0-59
Зараховано / Passed	60-100
Не зараховано / Fail	0-59

ТЕМАТИЧНИЙ ПЛАН ЛЕКЦІЙ І ЛАБОРАТОРНИХ ЗАНЯТЬ

№ Лекції	Назва лекції	Лекції	Лаборат роботи	Самост. робота

1	Предмет математичних основ захисту інформації. Етапи розвитку методів захисту інформації. Основні поняття криптології. Основні види криптографічних атак.	2		6
2	Машинні моделі складності. Машини Тюрінга (МТ) та їх варіації. Детерміновані і не детерміновані МТ. Тристрічкові МТ і складність в часі і пам'яті..	2	2	6
3	Класи складності P і NP. Поняття односторонньої функції та його роль в криптографії. Приклади односторонніх функцій.	2	2	4
4	Основні поняття теорії ймовірностей. Випадкові величини та їх властивості. Рівномірний, біноміальний та інші розподіли. Цілком таємна криптосистема по Шеннону.	2	2	10
5	Основні поняття теорії груп. Розклад групи за підгрупою. Нормальний дільник групи. Теорема Лагранжа та її наслідки. Приклади застосування теорії груп в криптографії. Групи підстановок та циклічні групи. Основні властивості таких груп.	2	2	10
Контрольна робота 1				
6	Кільця та їх властивості. Ідеали кільця та його властивості. Поняття дискретного логарифму та алгоритм його обчислення. Поля, побудова скінченних полів. Проблема передачі ключів та її розв'язання. Системи обміну ключами Діффі-Хеллмана та Ель Гамаля.	2	2	10
7	Факторизація цілих чисел. Найпростіші методи факторизації. Метод Рабіна, ро-метод..Функція Ойлера та її властивості.	2	2	10
8	Порівняння за модулем. Властивості порівнянь. Китайська теорема про остачі. Розв'язання порівнянь.	2	2	4
9	Алгоритми обчислення числових функцій та алгоритми тестування чисел на простоту. Генератори псевдовипадкових чисел. Еліптичні криві та криптосистеми на цих кривих.	2	2	10
10	Криптографічні системи та їх класифікація. Характеристика криптосистем. Симетричні системи та асиметричні системи. Асиметричні системи та їх властивості.	2	2	10
Контрольна робота 2				
ВСЬОГО		**20**	**18**	**80**

Загальний обсяг **120 годин**, в тому числі:
Лекцій – 20 **год.**,
Лабораторних робіт – 18 **год.**,
Самостійної роботи – 80 **год.**,
Консультації – 2 **год.**

Змістовна частина 1. *Задачі і проблематика теорії ймовірностей, теорії чисел та загальної алгебри.*

Лекція 1. Предмет математичних основ захисту інформації. Етапи розвитку методів захисту інформації. Основні поняття криптології. Основні види криптографічних атак. Приклади. – **2год.**

Вступ до області математичних основ захисту інформації. Історія розвитку криптографічних методів, їх класифікація та основні етапи розвитку. [1,2].

Завдання для самостійної роботи. (6 год.)

Алгоритми переходу від однієї основи систем числення до іншої основи. Складність таких алгоритмів та їх реалізація. Складність алгоритмів обчислення додавання, віднімання, множення та ділення в різних системах числення. *3], [4].*

Лекція 2. Машинні моделі. Детерміновані, недетерміновані та три стрічкові машини Тюрінга.. Поняття складності обчислення в часі і пам'яті. - **2год.**

Основні математичні поняття: відношення, відношення порядку та функціональні відношення. Властивості функціональних відношень та їх класифікація: ін'єкції, сюр'єкії, бієкції. Порядок росту функцій та методи їх знаходження. [4],[5].

Завдання для лабораторної роботи 1. (2 год.)

Обчислення асимптотики функцій складності. Рекурсивні програми та методи їх складнісного аналізу: підстановки, розв'язання рекурентної залежності, метод генератрис.

Завдання для самостійної роботи. (6 год.)

Приклади на обчислення складності функцій. Оцінки складності алгоритмів обчислення поліномів, множення матриць.. *3], [4].*

Лекція 3. Класи складності P і NP. Поняття односторонньої функції та його роль в криптографії. Приклади побудови односторонніх функцій. **– 2год.**

Розглядається теорія складності за Тюрінгом. Описуються класи складності P і NP. Формулюється необхідна умова стійкості криптографічної системи. *[1], [2], [3].*

Завдання для лабораторної роботи 3. (2 год.)

Оцінка складності в моделі Тюрінга алгоритмів обчислення НСД та НСК та їх реалізація в різних мовах програмування: C, JAVA, Pyton. Порівняння часових оцінок виконання алгоритмів в різних реалізаціях.

Завдання для самостійної роботи. (10 год.)

Алгоритми переходу від однієї основи систем числення до іншої основи. Складність таких алгоритмів та їх реалізація. Складність алгоритмів обчислення додавання, віднімання, множення та ділення в різних системах числення. *3], [4].*

Лекція 4. Основні поняття теорії ймовірностей. Випадкові величини та їх властивості. Рівномірний, біноміальний та інші розподіли. Поняття стійкості криптосистеми. Теорема Шеннона. - **2год.**

Наводяться основні поняття теорії ймовірностей: поняття випадкової величини, її ймовірності, основні дискретні розподіли та умовна ймовірність. Ілюстрація понять на прикладах. [1], [2], [3].

Завдання для лабораторної роботи 5. (2 год.)

Основні дискретні розподіли. Ланцюги Маркова та робота з ними. Обчислення матриці переходів за початковими даними.

Завдання для самостійної роботи. (10 год.)

Основні дискретні розподіли. Ланцюги Маркова та робота з ними. Приклади поудови ланцюга Маркова, обчислення матриці переходів за початковими даними. Ентропія і інформація, основні властивості. Частотна характеристика *[1], [3], [4].*

Лекція 5. Основні поняття теорії груп. Розклад групи за підгрупою. Нормальний дільник групи. Теорема Лагранжа та її наслідки . **– 2 год.**

Завдання для лабораторної роботи 6. (2 год.)

Алгоритми і приклади застосування методів теорії груп в криптографії. Дискретний логарифм та його криптоаналіз.

Завдання для самостійної роботи. (10 год.)

Побудова скінченних груп та їх підгруп. Приклади побудови криптосистеми на основі кілець. Обчислення в скінченних групах і кільцях та алгоритми їх реалізації

ТИПОВЕ ЗАВДАННЯ КОНТРОЛЬНОЇ РОБОТИ

1. Знайти твірні елементи скінченної циклічної групи лишків за модулем 29.
2. Навести характеристику криптографічних систем та напрямки їх розвитку. Дати означення односторонньої функції та охарактеризувати її значення в криптографії.
3. Знайти розв'язки системи конгруенцій x=3 (mod 5), x= 2 (mod 12), x= 7 (mod 3)/.

Контрольні запитання до змістовної частини І.

1. Дати означення проблеми P та NP. Навести приклади проблем з цих класів.
2. Охарактеризувати значення проблеми P≠NP в криптографії. Дати означення односторонньої функції та її властивостей.

3. Дати означення складності алгоритму в часі і пам'яті. Навести класифікацію проблем, виходячи з цього означення.
4. Навести означення детермінованої МТ, недетермінованої МТ та багато стрічкової МТ. Який часовий зв'язок існує між цими моделями обчислень.
5. Довести примітивну рекурсивність арифметичних операцій, функцій НСД і НСК.
6. Дати означення випадкової величини та функції її розподілу. Навести основні дискретні розподіли та їх функції.
7. Означення групи, кільця та поля. Навести основні властивості цих алгебр та їх роль у криптографії.
8. Ентропія і інформація. Ентропія природної мови та ентропія на символ джерела тексту. Метод частотного аналізу природо мовних текстів та його роль в крипто аналізі. Навести приклади застосування методу.
9. Алгоритми обчислення теоретико-числових функцій. Класифікація криптосистем. Та основні загрози таким системам.
10. Симетричні шифри підстановки та їх користь. Шифр Віженера та його роль в симетричній криптографії Теорема Шеннона про абсолютно стійку криптосистему.

Змістовна частина II. *Основні області застосування симетричних та асиметричних криптосистем. Проблеми обміну ключами та основні методи генерації та обміну ключами. Принципи побудови асиметричних криптосистем. Приклади асиметричних шифрів.*

Лекція 6. Кільця та їх властивості. Ідеали кільця та його властивості. Поняття дискретного логарифму та алгоритм його обчислення..Поле, характеристика поля та побудова скінченних полів. **-2 год.** *[7], [8], [9].*

Кільця та їх основні властивості. Кільце лишків цілих чисел та його властивості. Дільники нуля, дільники одиниці, ідеали кільця. Основні твердження про породжуючи елементи скінченного кільця. [1], [2], [4],[5], [10].

Завдання для лабораторної роботи . (2 год.)

Обчислення в скінченних кільцях та алгоритми їх реалізації. Незвідні поліноми над скінченними полями лишків. Побудова полів порядку p^n та обчислення в таких полях. Застосування в криптографії.

Завдання для самостійної роботи. (4 год.)

Розглянути відповідні розділи загальної алгебри стосовно скінченних кілець полів. Повторити основні властивості цих алгебр. *[1], [3], [7].*

Лекція 7. Елементи теорії чисел. Відношення подільності та його властивості. НСД і НСК, примітивна рекурсивність цих функцій. Алгоритм Евкліда знаходження НСД та його варіації. Факторизація. – **2год.**

Означення відношення подільності та його властивості. Основна теорема арифметики та наслідки з неї. Проблема факторизації та її зв'язок з проблемою тестування чисел на простоту. Приклади використання.

Завдання для лабораторної роботи . (2 год.)

Основна теорема арифметики та наслідки з неї. Проблема факторизації та її зв'язок з проблемою тестування чисел на простоту. Алгоритми побудови простого числа великої розрядності та їх реалізація. *[1], [3], [7].*

Завдання для самостійної роботи. (6 год.)

Методи розв'язання рівнянь та порівнянь в полях та кільцях лишків. Алгоритм розв'язання системи порівнянь та його реалізація Алгоритим модульної. Арифметики та їх реалізація в різних мовах програмування: C, JAVA, Pyton. Порівняння часових оцінок виконання алгоритмів в різних реалізаціях. *[1], [3], [4].*

Лекція 8. Факторизація цілих чисел. Найпростіші методи факторизації. Метод Ферма, Рабіна та ро-метод..Функція Ойлера та її властивості. – **2 год.**

Розглядаються найпростіші методи факторизації: решето Ератосфена, пробного ділення, на основі малої теореми Ферма. Приклади роботи цих методів.

Завдання для лабораторної роботи . (2 год.)

Факторизація цілих чисел. Найпростіші методи факторизації: решето Ератосфена, метод Ферма. Функція Ойлера та її властивості. Алгоритми розв'язання конгруенцій.

Завдання для самостійної роботи. (8 год.)

Методи факторизації. Реалізація основних алгоритмів та їх часова характеристика. *[1], [3], [4]*.

Лекція 9. Криптографічні системи та їх класифікація. Характеристика криптографічних систем. Симетричні та асиметричні системи. Протоколи обміну ключами та їх генерація. Шифр Щаміра та RSA, їх властивості. .

Розглядаються два шифри, які відносяться до криптосистем з відкритим ключем. Досліджуються їх властивості та недоліки. Ілюстрація методів на прикладах. **– 2 год.**

Завдання для лабораторної роботи. (2 год.)

Реалізація: шифру Шаміра та RSA. Оцінка стійкості цих шифрів.

Завдання для самостійної роботи. (10 год.)

Побудувати 6-7 прикладів, які ілюструють роботу шифру Шаміра та оцінити складність кожного приклада на предмет стійкості до зламу.. Порівняння реалізації шифру в різних мовах програмування. *[1], [3], [4]*.

Лекція 10. Протоколи обміну ключами та їх реалізація: Діффі-Хеллмана та Ель Гамаля. Шифр Щаміра та його властивості. Порівняльна характеристика цих методів.

Розглядаються порівняння за модулем та методи їх розв'язання. Єдиність розв'язку та його існування. Теорема Діріхле. Ілюстрація методів на прикладах. **– 2 год.**

Завдання для лабораторної роботи . (2 год.)

Реалізація: алгоритмів Діффі-Хеллмана та Ель Гамаля. Шифр Щаміра та його властивості.

Завдання для самостійної роботи. (10 год.)

Шифр Діффі-Хеллмана електронного підпису та його реалізація в різних мовах програмування. Порівняння часових характеристик реалізацій шифрів в різних мовах програмування. *[1], [3], [4]*.

ТИПОВЕ ЗАВДАННЯ КОНТРОЛЬНОЇ РОБОТИ

1. Побудувати поле з 9 елементів та навести його таблицю Келі для операцій додавання та множення.
2. Охарактеризувати переваги та недоліки методів заміни, підстановки, шифру гомофонічного.
3. Виконати обмін повідомленням CAB з абонентом за допомогою шифру RSA.
4. Виконати обмін повідомленням CAB з абонентом за допомогою шифру Шаміра.
5. Згенерувати десять псевдовипадкових чисел за допомогою ЛКГ з початковими параметрами 3,11 та 9.

Контрольні запитання до змістовної частини II.

1. Охарактеризувати переваги та недоліки симетричних та асиметричних криптосистем. Яка користь симетричних систем.
2. Які загрози виникають в симетричних системах при обміні ключами?
3. Сформулювати теорему Шеннона про абсолютно стійку криптосистему. Які практичні наслідки випливають з цієї теореми?
4. Охарактеризувати методи Діффі-Хеллмана та Ель Гамаля . Навести приклади їх застосування.
5. Основні об'єкти алгоритму RSA та їх роль у використанні цього шифру.
6. Метод електронного підпису та його використання. Яким умовам повинен задовольняти цей метод.

Рекомендована література

1. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. - М.: МЦНМО. - 2003.- 328 с.
2. Венбо Мао. Современная криптография. - СПб.: ``Вильямс". - 2005.- 763 с.
3. Виноградов И.М. Основы теории чисел. - М.: Наука. - 1972.- 167 с.
4. Вирт Н. Систематическое программирование. - М.: Мир. - 1985.- 183 с.
6. Кнут Д. Искусство программирования для ЭВМ. т. 2 Получисленные алгоритмы. - М.: Мир. - 1977.- 723 с.
7. Коблиц Н. Курс теории чисел и криптографии. - М.: Изд-во ТВП. - 2001.- 260 с.
8. Коробейников А.Г., Гатчин Ю.А. Математические основы криптологии. - СПб.: Издатво ИТМО. - 2004.- 110 с.
9. Кривий С.Л. Дискретна математика: вибрані питання. - Київ: Видавничий дім ``Києво-Могилянська академія". - 2007. - 570 с.
10. Кривий С.Л. Дискретна математика. - Чернівці: Букрек. - 2014. - 567 с.
11. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография.- СПб: Изд. ``Лань". - 2001. - 218 с.
12. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. - М: Горячая линия -- Телеком. - 2005. - 229 с.
13. Шеннон К. Работы по теории информации и кибернетике. - М.:ИЛ. - 1963. - С. 333-369.
14. Шнейер Б. Криптография для практиков..- СПб: Изд. ``Вильямс". - 2002. - 899 с.
15. Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии. - М: МЦНМО. - 2002. - 103 с.
16. Ященко В.В. и др. Введение в криптографию. - М:МЦНМО. - 2000. - 287 с.
17. Diffe W., Hellman M.E. New direction in cryptography. - IEEE Transaction on Information Theory. - 1976. - v. 22. - P. 644-654.
18. Stallings William. Ochrona danych w sieci i intersieci. - Warszawa: Wydawnictwo Naukowo Techniczne. - 1997. - 474s.
20. Merkle R. and Hellman H. Hiding Information and Signatures in Trap Door Knapsacks. – IEEE Transac. on Inform. Theory, September, - 1978. P. 241-245.
21. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signature and Public Key Cryptosystems. - Communic. of the ACM, February. - 1978. P. 36-45.
22. Matyas S. Key Handling with Control Vektors. - IBM System Journ. - N 2. - 1991. - P. 43-54.
23. Miller G. Riman's Hypothesis and Tests for Primality. - Procieedings of the Seventh Annual ACM Symposium on the Theory of Computing, May. 1975. - P. 47-49.
24. Rabin M. Probabilistic Algorithm for Primality Testing. - Journal of Number Theory, December. 1980. - P. 70-79.
25. Matyas S., Le A., Abracham D. A Key Management Scheme Based onh Control Vektors. – IBM System Journ. N 3. - 1991. - P. 21--29.
26. Stoll C. Stalking the Wily Hackers. - Communications of the ASM. - May. - 1988. - P. 16-19.
27. Safford D., Shales D., Hess D. The TAMU Security Package. An Ongoing Response to Internet. Intruders in an Academic Environment. - Proceedings UNIX Security Simposium IV. - October. - 1993. - P. 17 - 22.
28. Madsen J. World Record in Password Checking. - Usernet, comp.security.misc. newgroup. – August.- 18. - 1993.
29. Papadimtriou C. H. Zlozonosc obliczeniowa. - Wydawnictwo Naukowo-Techniczne, Warszawa. - 2002. - 540 s.

Додаткова література

30. Alvare A. How Krackers Crack Passwords or What Password to Avoid. - Proceedings UNIX Security Workshop II.- August. - 1990.
31. Spafford E. Observing Reuzable Password Choises or What Password to Avoid. Proceed. of UNIX Security Simposium III. - September. - 1992.
32. Anderson J. Computer Security Threat Monitoring and Surveillance. - Fort Washington, PA: James P. Anderson CO., April. - 1980. Barbara. - July. - 1992.
33. Bloom B. Space/time Trade-offs in Hash Coding with Allowable Errors. - Communications of the ACM. - july. - 1970.
34. Nechvatal J. Public Key Cryptography. - Piscataway, NJ: IEEE Press. - 1992.
35. Yuval C. How to Swindle Rabin. - Cryptologia. - July. - 1979.
36. Menezes A., van Oorschot P., Vanstons S. Handbook of Applied Cryptography. -CRC Press. - 1996. - 661 p.
37. .Bockmair A., Weispfenning V. Solving Numerical Constraints. - In Handbook of Automated Reasoning. - Elsevier Science Publishers B.V. - 2001. - P. 753-842.