МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ
Кафедра Комп’ютерної інженерії та інноваційних технологій

Йона Л.Г., Байрамова Ю.М.

МЕТОДИ ПОБУДОВИ КРИПТОГРАФІЧНИХ СИСТЕМ

Методичні рекомендації для самостійної роботи здобувачів

Одеса 2024

Затверджено Вченою Радою Міжнародного гуманітарного університету
(протокол № 13 від 16.08.2024 р.)

Йона Л.Г., Байрамова Ю.М. Методи побудови криптографічних систем
методичні рекомендації для самостійної роботи здобувачів [Електронне видання]. / **Йона Л.Г., Байрамова Ю.М.** Кафедра Комп'ютерної інженерії та інноваційних технологій, Одеса, 2024. – 32 с.

Методичні рекомендації з курсу «**Методи побудови криптографічних систем**» розроблено відповідно до навчального плану. Матеріали складаються з навчальної програми курсу, методичних рекомендацій з проведення практичних занять і завдань для самостійної роботи здобувачів, списку рекомендованої літератури. Призначено для студентів другого (магістерського) рівня вищої освіти факультету Кібербезпеки, програмної інженерії та комп'ютерних наук Міжнародного гуманітарного університету.

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td rowspan="10">Кількість кредитів – 4, загальна кількість годин – 120</td><td rowspan="10">Галузь 12 – Інформаційні технології
Спеціальність – 125 «Кібербезпека та захист інформації»</td><td colspan="2">обов’язкова</td></tr>
<tr><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">2-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>2-й</td><td>2-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td>22 год.</td><td>6год</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>22 год.</td><td>6 год</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>год.</td><td>год.</td></tr>
<tr><td rowspan="6">Мова навчання – українська</td><td rowspan="6">Рівень вищої освіти – другий (магістерський) рівень</td><td colspan="2">Самостійна робота та індивідуальні завдання</td></tr>
<tr><td>76 год.</td><td>108год</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>залік</td><td>залік</td></tr>
</table>

Дисципліна **Методи побудови криптографічних систем** є складовою частиною навчального процесу у підготовці фахівців зі спеціальності 125 «Кібербезпека та захист інформації», а також обов’язковим компонентом освітньої програми для здобуття освітнього рівня «магістр» та має на меті формування у здобувачів уявлення про принципи побудови симетричних та асиметричних криптографічних систем, проблеми захисту інформації від порушення її конфіденційності, цілісності та доступності; принципи побудови та режими роботи блокових алгоритмів шифрування; розгляд концепції криптосистем з відкритим ключем; методи побудови схем електронно-цифрових підписів та керування криптографічними ключами.

Метою викладання навчальної дисципліни Методи побудови криптографічних систем є забезпечення здобувачів знаннями з питань принципів побудови криптографічних систем та проблем захисту інформації у системах комунікацій від порушення її конфіденційності, цілісності та доступності з урахуванням сучасного стану та перспективних напрямів розвитку криптографії.

Передумови для вивчення дисципліни – знання і вміння, отримані студентом при вивченні навчальних дисциплін бакалаврської підготовки.

2. ОЧІКУВАНІ КОМПЕТЕНТНОСТІ, ЯКІ ПЛАНУЄТЬСЯ СФОРМУВАТИ ТА ДОСЯГНЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ

У процесі реалізації програми дисципліни «Інформаційна безпека інноваційної діяльності» формуються наступні компетентності із передбачених освітньо-професійною програмою «Кібербезпека» зі спеціальності 125 Кібербезпека.

Інтегральна компетентність

ІК. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КЗ2. Здатність проводити дослідження на відповідному рівні.

Фахові компетентності

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Програмні результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та

критичної інфраструктури.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури.

РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

Заплановані результати навчання за навчальною дисципліною

У результаті вивчення цієї навчальної дисципліни студент має набути такі компетентності.

Знати:

- Основні поняття криптографії: конфіденційність, цілісність, доступність;
- Правові та етичні аспекти застосування криптографії в Україні;
- Види криптографічних систем: симетричні, асиметричні, гібридні криптосистеми;
- Основи теорії чисел, математичний апарат криптографії;
- Алгоритми симетричного шифрування;
- Режими роботи блокових шифрів;
- Потокові шифри: принципи роботи та застосування.
- Генерація та керування ключами в симетричних системах.
- Основи шифрування з відкритим ключем;
- Протоколи узгодження ключів;
- Криптографічні методи цифрового підпису;
- Принципи побудови інфраструктури відкритих ключів;
- Атаки на симетричні та асиметричні криптосистеми;
- Методи аналізу стійкості шифрів;
- Використання хешування для забезпечення цілісності даних та цифрових підписів;
- Протоколи автентифікації;
- Використання криптосистем для захисту конфіденційної інформації в різних галузях (електронна комерція, банківські системи, захист персональних даних);
- Сучасні тенденції у криптографії (основи квантової криптографії);

Вміти:

- Здійснювати аналіз існуючих криптографічних систем і оцінювати їхню стійкість до атак;
- Розуміти та порівнювати різні типи криптосистем (симетричні,

асиметричні, гібридні);
- Розробляти та впроваджувати симетричні та асиметричні криптографічні алгоритми;
- Вибирати відповідні криптографічні алгоритми та протоколи для різних задач і систем;
- Генерувати, зберігати, розповсюджувати та керувати криптографічними ключами в різних системах.
- Застосовувати протоколи узгодження ключів (Diffie-Hellman, ECDH) для безпечного обміну ключами;
- Використовувати криптографічні хеш-функції для забезпечення цілісності даних та створення цифрових підписів;
- Реалізовувати протоколи аутентифікації користувачів і вузлів мережі (TLS, SSL, Kerberos);
- Виявляти потенційні слабкі місця криптосистем і здійснювати оцінку стійкості до атак;
- Інтегрувати криптографічні рішення в сучасні інформаційні системи та програми;
- Слідкувати за новітніми розробками у сфері криптографії та впроваджувати сучасні рішення для підвищення безпеки інформаційних систем.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Актуальність питань методів побудови криптосистем для забезпечення надійного захисту інформації. Аналіз погроз інформації при передачі по каналах зв'язку. Вимоги до принципів побудови криптосистем.

Тема 2. Симетричні криптосистеми. Шифри на базі мережі Фейстеля. Дослідження алгоритму шифрування DES. Режими роботи. Недоліки алгоритму шифрування DES. Методи підвищення криптостійкості криптосистеми. Алгоритм 3-DES.

Тема 3. Європейський стандарт шифрування IDEA. Особливості побудови блокової криптосистеми.

Тема 4. Сучасні стандарти шифрування, що побудовані на SP-мережі. Схема SP- мережі. Реалізація SP-мережі в криптосистемах AES. Режими роботи стандарту. Вимоги щодо побудови криптосистеми AES.

Тема 5. Стандарт шифрування України ДСТУ 7624:2014 «Калина». Режими роботи криптосистеми.

Тема 6. Порівняльний аналіз сучасних криптоалгоритмів за призначенням.

Тема 7. Асиметричні алгоритми шифрування. Особливості побудови систем з відкритим ключем.

Тема 8. Принципи керування ключовою системою. Генерування та розподілення ключів методом Діффі-Хеллмана.

Тема 9. Криптосистема Ель Гамаля. Процедури шифрування в криптосистемі Ель– Гамаля.

Тема 10. Алгоритм шифрування в криптосистемі RSA. Процедури генерування ключів та шифрування.

Тема 11. Системи ідентифікації та автентифікації. Біометричні методи автентифікації.

Тема 12. Методи побудови схем електронного підпису. Різновиди ЕП.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин							
	денна форма				Заочна форма			
	усього	у тому числі			усього	у тому числі		
		лекц.	практ.	сам. роб.		лекц.	прак	сам. роб.
Змістовий модуль 1. Архітектура симетричних систем ЗІ								
Тема 1. Актуальність питань методів побудови криптосистем для забезпечення надійного захисту інформації. Типи й класифікація алгоритмів шифрування.	10	2		8	10			10
Тема 2. Шифри на базі мережі Фейстеля. Недоліки алгоритму шифрування DES. Алгоритм 3-DES	10	2	2	6	10	2		8
Тема 3. Європейський стандарт шифрування IDEA. Особливості побудови блокової криптосистеми.	10		2	8	10			10
Тема 4. Сучасні стандарти шифрування, що побудовані на SP-мережі. Стандарт шифрування AES.	10	2	2	6	10		2	8
Тема 5. Стандарт шифрування України ДСТУ 7624:2014 «Калина».	10	2	2	6	10			10
Тема 6. Порівняльний аналіз сучасних криптоалгоритмів за призначенням	10	2	2	6	10	2		8
Змістовий модуль 2 . Криптосистеми з відкритим ключем.								
Тема 7. Асиметричні алгоритми шифрування.	10	2	2	6	10	2		8
Тема 8. Принципи керування ключовою системою.	10	2	2	6	10			10
Тема 9. Процедури шифрування в	10	2	2	6	10		2	8

криптосистемі Ель–Гамаля.								
Тема 10. Шифрування в криптосистемі RSA.	10	2	2	6	10			10
Тема 11. Системи ідентифікації та автентифікації.	10	2	2	6	10			10
Тема 12. Методи побудови схем електронного підпису	10	2	2	6	10		2	8
Усього годин	**120**	**22**	**22**	**76**	**120**	**6**	**6**	**108**
ПІДСУМКОВИЙ КОНТРОЛЬ – Залік								

5. ПРАКТИЧНІ ЗАНЯТТЯ

№ з/п	Назва теми	Кількість годин	
		Денна форма	Заочна форма
1	Принципи побудови криптосистем за призначенням.	2	
2	Дослідження симетричних криптосистем, що побудовані на мережі Фейстеля. (DES; 3-DES; ДСТУ-28147-2009; IDEA)	4	2
3	Дослідження стандартів шифрування, що побудовані на SP-мережі. Стандарт шифрування AES.	2	
4	Дослідження стандарту шифрування України ДСТУ 7624:2014 «Калина».	4	
5	Дослідження асиметричних алгоритмів. Алгоритм шифрування RSA та Ель Гамаля.	4	2
6	Дослідження алгоритмів генерування та розподілення ключів. Алгоритм Діффі-Хеллмана.	2	
7	Дослідження алгоритмів електронного підпису RSA, Ель Гамаля та DSA.	4	2
	Всього	22	6

7. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни **«Інформаційна безпека інноваційної діяльності»** включаються наступні тематики завдання.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	**Назва теми**	**Кількість годин**	
		денна форма	**заочна форма**
1	**Тема 1. Актуальність питань методів побудови криптосистем для забезпечення надійного захисту інформації.** Аналіз погроз інформації при передачі по каналах зв’язку. Вимоги до принципів побудови криптосистем	8	10

2	**Тема 2. Шифри на базі мережі Фейстеля.** Дослідження алгоритму шифрування DES. Режими роботи. Недоліки алгоритму шифрування DES. Методи підвищення криптостійкості криптосистеми. Алгоритм 3-DES.	6	8
3	**Тема 3. Європейський стандарт шифрування IDEA**. Особливості побудови криптосистеми.	8	10
4	**Тема 4. Сучасні стандарти шифрування, що побудовані на SP-мережі.** Схема SP-мережі. Реалізація SP-мережі в криптосистемах AES Режими роботи стандарту. Вимоги щодо побудови криптосистеми AES.	6	8
5	**Тема 5. Стандарт шифрування України ДСТУ 7624:2014 «Калина».** Порівняльний аналіз симетричних криптосистем.	6	10
6	**Тема 6.** Порівняльний аналіз сучасних криптоалгоритмів за призначенням	6	8
7	**Тема 7. Асиметричні алгоритми шифрування.** Особливості побудови систем з відкритим ключем.	6	8
8	**Тема 8. Принципи керування ключовою системою**. Генерування та розподілення ключів методом Діффі-Хеллмана.	6	10
9	**Тема 9. Криптосистема Ель Гамаля.** Процедури шифрування в криптосистемі Ель–Гамаля.	6	8
10	**Тема 10. Алгоритм шифрування в криптосистемі RSA.** Процедури генерування ключів та шифрування.	6	10
11	**Тема 11. Системи ідентифікації та автентифікації.** Біометричні методи автентифікації.	6	10
12	**Тема 12. Методи побудови схем електронного підпису.** Різновиди ЕП.	6	8
	Всього	**76**	**108**

8. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Робоча програма навчальної дисципліни передбачає наступні види та методи контролю:

Види контролю	Складові оцінювання
Поточний контроль, який здійснюється у ході: проведення практичних та лабораторних занять, виконання індивідуального завдання; проведення консультацій та відпрацювань.	50%
Підсумковий контроль, який здійснюється у ході проведення іспиту (заліку).	50%

Методи діагностики знань (контролю)	Фронтальне опитування, лабораторні завдання, індивідуальні завдання, робота у групах, розв`язання практичних завдань, залік

Питання до заліку

1. Що таке конфіденційність інформації?

2. Чим забезпечується захист конфіденційної інформації?

3. Що таке цілісність інформації?

4. Чим забезпечується захист цілісності інформації?

5. Що таке доступність інформації?

6. Дати поняття процесу шифрування інформації.

7. Ключ шифрування. Різновиди ключів шифрування.

8. Класичні методи шифрування. Поясніть сутність методів шифрування: підставляння, переставляння та гамування.

9. З яких простих перетворювань складається складний шифр?

10. Які вимоги до захисту персональних даних існують у рамках законодавства України?

11. Що таке криптографія і яку роль вона відіграє в захисті інформації?

12. Класифікація криптосистем за призначенням.

13. Привести вимоги для побудови блочних криптосистем.

14. Поясніть сутність понять “перемішування” та “розсіювання” за К.Шенноном?

15. Пояснити метод каскадування, який використовується для побудови

надійних блочних шифрів.

16. Принципи побудови симетричних криптосистем.

17. Побудова симетричних криптосистем за мережею Фейстеля.

18. Пояснити принцип побудови криптосистеми 3-DES.

19. Пояснити принцип побудови криптосистеми IDEA.

20. Порівняти відомі симетричні криптоалгоритми за параметрами: довжина ключа; кількість етапів шифрування; кількість ключів для одного етапу шифрування; реалізація мережі Фейстеля.

21. Пояснити принцип побудови алгоритму Діффі-Хеллмана.

22. Переваги та недоліки алгоритму розподілення ключів методом Діффі-Хеллмана.

23. Привести схему секретної системи зв’язку для симетричних криптосистем.

24. Привести схему секретної системи зв’язку для асиметричних криптосистем.

25. Принципи керування ключовою системою.

26. Привести алгоритм формування цифрового підпису.

27. Які існують класи криптоалгоритмів?

28. Пояснити принцип рівноміцного захисту в інформаційних системах.

29. З яких етапів складається алгоритм електронного цифрового підпису?

30. Які алгоритми називають несиметричними?

31. Призначення асиметричних криптосистем.

32. Принципи побудови асиметричних криптосистем.

33. Пояснити принцип побудови криптосистеми Ель Гамаля.

34. Пояснити принцип побудови криптосистеми AES.

35. Пояснити принцип побудови криптосистеми Калина.

36. Як вирішується питання автентифікації в телекомунікаціях?

37. Призначення хеш функції в алгоритмах електронного підпису.

38. Привести алгоритм формування цифрового підпису на базі системи RSA.

39. Пояснити принцип мультиплікативної атаки. Яка криптосистема має цей недолік?

40. Призначення Персонального ідентифікаційного номеру (PIN).

41. Призначення стеганографічного захисту інформації.

42. Як забезпечується поєднання криптографічних та стеганографічних методів захисту інформації?

43. Протоколи захисту електронних транзакцій.

44. Методи біометричної автентифікації.

45. Багатофакторна автентифікація.

9. КРИТЕРІЇ ПІДСУМКОВОЇ ОЦІНКИ ЗНАНЬ СТУДЕНТІВ (для заліку)

Рівень знань оцінюється:

- «відмінно» / «зараховано» A − від 90 до 100 балів. Студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях, практичних та лабораторних заняттях, під час яких виконував усі поставленні завдання та давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, виконав лабораторні роботи та завдання до самостійної роботи, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» B − від 82 до 89 балів. Студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях, практичних та лабораторних заняттях, під час яких виконував усі поставленні завдання та давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, виконав лабораторні роботи та завдання до самостійної роботи, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» C − від 74 до 81 балів. Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність виконаних лабораторних робіт та завдань до самостійної роботи та активність у науково-дослідній роботі;
- «задовільно» / «зараховано» D - від 64 до 73 балів. Студент був присутній не на всіх лекціях та практичних заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність виконаних лабораторних робіт та завдань до самостійної роботи;
- «задовільно» / «зараховано» E − від 60 до 63 балів. Студент був присутній не на всіх лекціях та практичних заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, виконав не всі завдання до самостійної роботи;
- «незадовільно з можливістю повторного складання» / «не зараховано» FX – від 35 до 59 балів. Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу;
- «незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 1 до 34 балів. Студент не володіє навчальним матеріалом.

Таблиця відповідності результатів контролю знань за різними шкалами

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	Зараховано
74-81	C		
64-73	D	Задовільно	Зараховано
60-63	E		
35-59	Fx	Незадовільно	Не зараховано
1-34	F		

План-конспект лекцій з дисципліни
Методи побудови криптосистем

Змістовий модуль 1. Архітектура симетричних систем захисту інформації

Методи побудови криптосистем відіграють критично важливу роль у забезпеченні захисту інформації. Різноманіття алгоритмів, кожен із яких має свої особливості та сфери застосування, дозволяє вибирати найбільш оптимальні рішення для конкретних задач. З огляду на швидкий розвиток технологій, постійне вдосконалення криптографічних методів є необхідною умовою для підтримання належного рівня безпеки в інформаційному середовищі.

Тема 1. Актуальність питань методів побудови криптосистем для забезпечення надійного захисту інформації.

1. Актуальність питань криптографічного захисту інформації

У сучасному цифровому світі обсяг переданої, обробленої та збереженої інформації постійно зростає. Інформаційна безпека стала критично важливою через залежність від інтернету, комп'ютерних систем і мобільних пристроїв. З розвитком технологій зростає кількість кіберзлочинів, зловмисники застосовують все складніші методи атак на системи захисту інформації, в тому числі крадіжку даних, фальсифікацію інформації та втручання в конфіденційні комунікації. Одним із найефективніших методів захисту інформації є криптографія. Використання криптосистем дозволяє забезпечити конфіденційність, цілісність та автентичність інформації, що надзвичайно важливо як для приватного сектору, так і для державних установ.

2. Основні цілі криптографії

Конфіденційність: Забезпечення захисту інформації від доступу неавторизованих осіб.

Цілісність: Захист даних від змін під час зберігання чи передавання.

Автентичність: Переконання у достовірності джерела отриманої інформації.

Невідмовність: Забезпечення гарантії, що відправник не зможе заперечити факт відправлення повідомлення.

3. Типи та класифікація алгоритмів шифрування

3.1 Класифікація за принципом дії

Симетричні алгоритми (алгоритми з секретним ключем): Використовують один і той самий ключ для шифрування і дешифрування. Вони мають високу швидкість роботи та є ефективними для захисту великих обсягів даних (AES (Advanced Encryption Standard), DES (Data Encryption Standard).

Переваги: Швидкодія, економічність в обчисленнях.

Недоліки: Потреба у безпечній передачі ключів.

Асиметричні алгоритми (алгоритми з відкритим ключем): Використовують два різні ключі — відкритий для шифрування та закритий для дешифрування. Асиметричні алгоритми зазвичай застосовуються для обміну ключами, цифрового підпису та автентифікації.(RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography)).

Переваги: Відсутність необхідності передачі секретного ключа.

Недоліки: Складніші обчислення, що знижують швидкодію.

3.2 Класифікація за типом обробки даних

Блочне шифрування: Дані розбиваються на блоки фіксованого розміру, кожен з яких шифрується окремо. Це підвищує стійкість шифрування, але може вимагати додаткових налаштувань для обробки даних, обсяги яких не кратні розміру блоку. (AES, 3DES).

Потокове шифрування: Дані шифруються побітово або побайтово, тобто кожен елемент шифрується поступово. Такий підхід є більш гнучким і часто використовується для безперервної передачі даних.(RC4).

3.3 Класифікація за призначенням

Алгоритми шифрування даних: Використовуються для захисту переданої інформації. Приклади включають AES для симетричного шифрування та RSA для асиметричного.

Алгоритми хешування: Використовуються для перевірки цілісності даних. Вони генерують хеш-код, який змінюється при будь-якій зміні вихідних даних.

Цифрові підписи: Забезпечують автентифікацію і невідмовність. Використовуються для підтвердження особи та гарантують, що дані надіслані саме відправником і не були змінені.(ECDSA (Elliptic Curve Digital Signature Algorithm).

4. Перспективи розвитку криптосистем

Квантова криптографія: Із розвитком квантових обчислень зростає загроза для традиційних криптосистем, особливо асиметричних алгоритмів. Квантові комп'ютери потенційно здатні розв'язувати складні математичні задачі, що лежать в основі таких алгоритмів, набагато швидше.

Постквантова криптографія: Напрямок, що досліджує нові алгоритми, стійкі до атак з використанням квантових обчислень.

Розвиток стандартів: Важливо оновлювати стандарти захисту даних та впроваджувати нові алгоритми, адаптовані до сучасних потреб і загроз.

Тема 2. Шифри на базі мережі Фейстеля. Недоліки алгоритму шифрування DES. Алгоритм 3-DES.

Мережа Фейстеля, яка лежить в основі DES і 3-DES, забезпечує зручну структуру для шифрування і розшифрування даних, а також високу криптографічну стійкість. Проте з часом 56-бітний ключ DES став недостатньо стійким, що призвело до розробки 3-DES, який забезпечує вищий рівень безпеки завдяки триразовому шифруванню. Однак обмеження продуктивності 3-DES і його недоліки в умовах сучасних загроз стимулюють перехід до більш досконалих алгоритмів, зокрема AES, який повністю замінив DES і 3-DES у багатьох системах.

1. Мережа Фейстеля: Основи та особливості

Визначення: Мережа Фейстеля — це криптографічна структура, яка лежить в основі багатьох сучасних алгоритмів симетричного шифрування. Її особливість полягає в тому, що вона дозволяє використовувати той самий алгоритм для шифрування і дешифрування, що підвищує зручність реалізації та ефективність обчислень.

Структура мережі Фейстеля: Вхідні дані поділяються на дві рівні частини — ліву (L) та праву (R). Алгоритм працює за принципом кількох раундів, під час яких права частина змінюється на основі лівої, а ліва — на основі результатів обчислень у правій частині з використанням спеціальної функції F та ключів.

Функція F: В кожному раунді функція F обробляє праву частину та генерує результат, який комбінується з лівою частиною.

Обмін частинами: Наприкінці кожного раунду ліва і права частини обмінюються місцями.

Розшифрування: Завдяки симетричності структури мережі Фейстеля, процес дешифрування аналогічний шифруванню, що спрощує реалізацію алгоритму.

Важливість мережі Фейстеля: Мережа дозволяє створювати надійні криптосистеми на основі простих перетворень і забезпечує високу стійкість до атак, особливо якщо кількість раундів достатньо велика.

2. Алгоритм DES.

Огляд алгоритму DES (Data Encryption Standard): DES — симетричний алгоритм блочного шифрування, який було розроблено компанією IBM у 1970-х роках і затверджено Національним бюро стандартів США як стандарт шифрування у 1977 році.

Структура DES: DES є алгоритмом блочного шифрування з розміром блоку 64 біти, де кожен блок шифрується окремо. Алгоритм використовує ключ розміром 56 біт, що комбінується з початковою перестановкою блоку та проходить 16 раундів мережі Фейстеля.

Процес шифрування: В кожному раунді ключ проходить трансформацію за допомогою функції F, яка складається з перестановок, підстановок і об'єднання з правою частиною блоку.

Недоліки DES:

Малий розмір ключа: 56-бітний ключ був достатньо стійким на момент розробки, але з розвитком обчислювальних потужностей став уразливим для атаки перебором. У сучасних умовах DES може бути зламано за допомогою брутфорс-атаки за кілька годин.

Розмір блоку: 64-бітний блок створює обмеження для шифрування великих обсягів даних, що може призвести до повторення блоків шифротексту і, відповідно, до уразливості для атак, таких як атака по виявленню шаблонів.

Уразливість до криптоаналізу: Алгоритм схильний до різних видів криптоаналітичних атак, таких як диференціальний криптоаналіз. Внаслідок цього, DES більше не відповідає сучасним вимогам безпеки і замінюється більш надійними алгоритмами.

3. Алгоритм 3-DES: Принцип роботи і переваги

Алгоритм 3-DES був розроблений як тимчасова заміна DES, щоб підвищити стійкість шифрування, але при цьому зберегти сумісність із існуючими системами, які використовували DES. У 3-DES шифрування проводиться тричі із застосуванням кількох ключів.

Процес шифрування: 3-DES використовує три етапи шифрування з чергуванням ключів:

Перший етап: Шифрування даних за допомогою першого ключа (K1) з використанням DES. Другий етап: Розшифрування отриманих даних за допомогою другого ключа(K2). Третій етап: Повторне шифрування результату за допомогою третього ключа (K3).

Типи ключів у 3-DES:

Три різні ключі (3-DES-EEE): Використовуються три різні ключі (K1, K2, K3), що забезпечує максимальну стійкість шифрування.

Два ключі (3-DES-EDE): Перший і третій ключі збігаються (K1 = K3), а другий ключ відрізняється. Це дозволяє досягти високого рівня безпеки при менших обчислювальних витратах.

Переваги 3-DES:

Вища стійкість до атак: Триразове шифрування значно ускладнює проведення атаки перебором.

Сумісність: Алгоритм зберігає сумісність із DES, що дозволило його широке застосування у період, коли були відсутні більш потужні стандарти.

Недоліки 3-DES:

Низька продуктивність: Триразове шифрування значно знижує швидкість роботи алгоритму порівняно з DES та іншими сучасними алгоритмами.

Недостатня стійкість для майбутніх загроз: Хоча 3-DES є стійкішим, ніж DES, його продуктивність і розмір блоку (64 біти) не відповідають вимогам сучасних криптосистем. У зв’язку з цим, у багатьох системах 3-DES також замінюють більш надійними алгоритмами, такими як AES.

Тема 3. Європейський стандарт шифрування IDEA. Особливості побудови блокової криптосистеми.

IDEA є значущим європейським стандартом шифрування, що забезпечує високу криптостійкість завдяки комбінації різних операцій та ефективній структурі блочного шифру. Він виявився надзвичайно ефективним для свого часу, зокрема завдяки 128-бітному ключу, і став популярним у захисті електронної пошти та інших засобів комунікації. Незважаючи на появу більш сучасних алгоритмів, IDEA залишається одним із найвідоміших прикладів блочної криптосистеми, важливим для вивчення принципів побудови надійних криптографічних систем.

1. Європейський стандарт шифрування IDEA

IDEA (International Data Encryption Algorithm): IDEA — симетричний блочний алгоритм шифрування, розроблений в 1991 році Джеймсом Л. Массі та Ксав'єром Лейманом у Швейцарії. Він став відомим як один з найбільш стійких шифрів свого часу і широко використовувався у європейських криптосистемах. IDEA був розроблений як альтернатива для DES, з вищим рівнем безпеки і більшою стійкістю до криптоаналітичних атак.

Основні характеристики:

Розмір блоку: 64 біти; довжина ключа: 128 біт; кількість раундів: 8 раундів і одного вихідного перетворення.

2. Структура та особливості побудови блочного шифру IDEA

Принцип дії: IDEA використовує специфічну комбінацію операцій додавання, множення та побітових операцій XOR. Таке поєднання дозволяє досягти високого рівня стійкості до атак, зокрема до диференціального та лінійного криптоаналізу.

Операції в кожному раунді: **Додавання по модулю 2^16**: Додає значення з перенесенням на 16-бітовому рівні; **Множення по модулю 2^16 + 1**: Використовується для змішування даних; **Операція XOR**: Побітове виключне "або" для забезпечення додаткового змішування.

Ключова структура: 128-бітний ключ розбивається на 52 субключі по 16 біт кожен, які використовуються у кожному раунді. Ця структура ключа забезпечує високу криптостійкість та захист від простого перебору.

Етапи шифрування в IDEA

Поділ блоку на частини: 64-бітовий блок поділяється на чотири 16-бітові підблоки, які обробляються у кожному раунді.

Вісім основних раундів: Кожен раунд включає застосування трьох типів операцій (додавання, множення, XOR) до підблоків з використанням субключів, що забезпечує глибоке змішування даних.

Останній раунд трансформації (вихідне перетворення): Останній раунд IDEA завершується додатковим набором операцій над підблоками без повного використання всіх операцій. Це забезпечує підвищену стійкість до криптоаналітичних атак.

Зворотний процес розшифрування: Оскільки IDEA є симетричним алгоритмом, для дешифрування використовується зворотний процес із застосуванням інверсійних значень тих самих субключів.

3. Переваги та недоліки алгоритму IDEA

Переваги:

Висока криптостійкість: IDEA вважається стійким до диференціального та лінійного криптоаналізу завдяки використанню комбінації різних операцій, що робить структуру алгоритму складною для атак.

Стійкість до перебору: Завдяки довжині ключа 128 біт IDEA є значно стійкішим до атак перебором, ніж DES з його 56-бітним ключем.

Ефективність: Шифр можна ефективно реалізувати в апаратному забезпеченні, і він добре працює з обмеженими ресурсами, що зробило його популярним у різних криптографічних системах у 1990-х роках.

Недоліки:

Малий розмір блоку: IDEA має 64-бітний розмір блоку, що робить його менш ефективним для шифрування великих обсягів даних і потенційно уразливим до атак, які використовують повторювані блоки шифротексту.

Обмеження патентів: IDEA був запатентований, що обмежувало його використання у деяких країнах і для певних цілей до закінчення патенту.

Складність у порівнянні з сучасними алгоритмами: У зв'язку з появою більш потужних та гнучких алгоритмів, таких як AES, IDEA поступово втратив популярність у сучасних системах.

4. Сфери застосування та історична роль IDEA

Використання в PGP (Pretty Good Privacy): IDEA є популярним з 1990-х років і використовувався як стандартний алгоритм у програмному забезпеченні для захисту електронної пошти — PGP, що забезпечувало його широке застосування серед користувачів по всьому світу.

Роль у розвитку європейської криптографії: IDEA став символом незалежного європейського підходу до захисту інформації і є важливим етапом у розвитку європейських стандартів шифрування.

Перспективи: Хоча IDEA зараз використовується не так широко, він залишається важливим для розуміння історії криптографії і розвитку методів захисту інформації.

Тема 4. Сучасні стандарти шифрування, що побудовані на SP-мережі. Стандарт шифрування AES.

SP-мережа є надійною структурою для побудови блокових алгоритмів шифрування, що базується на послідовності операцій підстановки та перестановки. AES, як один з найвідоміших алгоритмів, побудованих на SP-мережі, став сучасним стандартом шифрування завдяки своїй стійкості, ефективності та гнучкості у використанні. AES широко застосовується у різних сферах захисту даних, забезпечуючи надійний захист інформації від сучасних загроз.

SP-мережа: Основи та принципи побудови

Що таке SP-мережа (Substitution-Permutation Network): SP-мережа — це криптографічна структура, яка використовує чергування операцій підстановки (Substitution) та перестановки (Permutation) для шифрування даних. Ця модель відрізняється від класичної мережі Фейстеля, зокрема, своїм підходом до створення стійкості через змішування і дифузію даних.

Основні принципи SP-мережі:

Підстановки (S-блоки): Набір нелінійних перетворень, які використовуються для заміни значень у бітових групах, що ускладнює аналіз структури шифру.

Перестановки (P-блоки): Перетасування бітів або груп бітів для рівномірного розподілу змін даних по всьому блоку шифротексту.

Раундові ключі: В кожному раунді застосовуються унікальні ключі для забезпечення криптостійкості, створюючи додаткову нелінійність та стійкість до атак.

Розширена структура: SP-мережа зазвичай складається з декількох раундів, у кожному з яких застосовуються підстановки та перестановки. Така структура дозволяє створювати стійкіші до криптоаналізу алгоритми.

2. Стандарт шифрування AES: Основні характеристики

Огляд AES (Advanced Encryption Standard): AES — це сучасний симетричний блоковий алгоритм шифрування, який був затверджений Національним інститутом стандартів і технологій США (NIST) у 2001 році як заміна застарілого DES. AES став глобальним стандартом шифрування завдяки високому рівню безпеки, ефективності та гнучкості у застосуванні.

Структура AES: AES — це алгоритм, побудований на SP-мережі, що використовує комбінацію підстановок, перестановок та побітових операцій XOR для створення криптографічно стійкого шифрування.

Розмір блоку та ключа: AES працює з фіксованим розміром блоку 128 біт і підтримує три варіанти довжини ключа: 128, 192 і 256 біт. Кожна довжина ключа визначає кількість раундів шифрування: **AES-128**: 10 раундів; **AES-192**: 12 раундів; **AES-256**: 14 раундів.

3. Принципи роботи AES: Етапи шифрування

1. Початкове додавання ключа (AddRoundKey): Початковий раунд починається з операції XOR між блоком даних і раундовим ключем.

2. Байтове заміщення (SubBytes): Кожен байт даних проходить через нелінійний підстановчий блок (S-блок), який забезпечує криптостійкість алгоритму.

3. Перестановка рядків (ShiftRows): Байтова структура блоку зазнає циклічної перестановки, при якій кожний рядок зміщується на певну кількість позицій, щоб забезпечити дифузію.

4. Змішування стовпців (MixColumns): Кожен стовпець матриці даних множиться на фіксовану матрицю, що сприяє подальшому поширенню змін по всьому блоку.

5. Додавання раундового ключа (AddRoundKey): У кожному раунді блок даних комбінується з ключем за допомогою операції XOR, що додає ще один рівень захисту.

Фінальний раунд: В останньому раунді шифрування виконується послідовність підстановок і перестановок без етапу змішування стовпців, щоб зберегти симетрію для зворотного розшифрування.

4. Ключові особливості та переваги AES

Стійкість до атак: AES має високий рівень стійкості до відомих типів атак, зокрема до диференціального і лінійного криптоаналізу. Це досягається за рахунок кількох раундів підстановок та перестановок, що забезпечують складну структуру для аналізу.

Гнучкість у використанні: Підтримка кількох розмірів ключа (128, 192, 256 біт) дозволяє використовувати AES для різних рівнів безпеки та для різних цілей. Зокрема, AES-256 є рекомендованим стандартом для захисту інформації найвищої секретності.

Ефективність: AES оптимізований для ефективного виконання як у програмних, так і в апаратних реалізаціях, що дозволяє використовувати його на різних платформах, включаючи обмежені пристрої.

5. Порівняння AES з іншими сучасними алгоритмами

Переваги над DES і 3-DES: AES значно перевершує DES і 3-DES за рівнем безпеки, стійкості до атак та ефективністю обчислень. На відміну від DES, який використовує 56-бітний ключ, AES має значно більші ключі (128, 192, 256 біт), що унеможливлює злам шляхом перебору.

Використання в міжнародних стандартах: Завдяки своїм характеристикам AES став міжнародним стандартом шифрування і широко використовується у різних криптографічних протоколах, таких як SSL/TLS, IPsec, а також у системах захисту інформації багатьох держав та організацій.

Тема 5. Стандарт шифрування України ДСТУ 7624:2014 «Калина».

ДСТУ 7624:2014 «Калина» — це сучасний національний стандарт України для симетричного блочного шифрування, який забезпечує високий рівень захисту даних і стійкість до сучасних видів атак. Алгоритм побудований на основі SP-мережі і демонструє гнучкість у використанні завдяки підтримці різних розмірів блоку та ключа. «Калина» є важливим елементом в системі національної безпеки України і підходить для захисту конфіденційної інформації на державному рівні.

1. ДСТУ 7624:2014 «Калина»

ДСТУ 7624:2014: ДСТУ 7624:2014, відомий також як «Калина», — це державний стандарт України з блочного симетричного шифрування. Він був розроблений з метою забезпечення надійного захисту інформації та задоволення потреб національної криптографічної безпеки. «Калина» орієнтований на забезпечення криптостійкості для державних установ, військових організацій та різноманітних інформаційних систем в Україні. Вона відповідає сучасним вимогам щодо захисту інформації, демонструючи високу ефективність та стійкість до атак.

Основні характеристики алгоритму «Калина»

«Калина» підтримує розмір блоку 128, 256 і 512 біт, що дозволяє ефективно захищати різні обсяги даних.

Алгоритм також підтримує різні довжини ключа: 128, 256 і 512 біт.

Кількість раундів в алгоритмі залежить від розміру блоку та ключа: для 128-бітного блоку — 10 раундів; для 256-бітного блоку — 14 раундів; для 512-бітного блоку — 18 раундів.

3. Структура та принцип роботи алгоритму «Калина»

SP-мережа як основа: «Калина» побудована на основі SP-мережі (Substitution-Permutation Network), що забезпечує високий рівень дифузії та змішування даних. Ця структура дозволяє досягти високої криптостійкості та захисту від багатьох видів криптоаналітичних атак.

S-блоки: Підстановчі блоки, які реалізують нелінійні перетворення для створення складної структури шифру.

P-блоки: Перестановки, що забезпечують рівномірний розподіл змін у блоці даних.

Раундові операції: Кожен раунд алгоритму включає комбінацію операцій XOR, перестановок, підстановок і лінійних перетворень, що підвищує стійкість алгоритму до атак.

Додавання раундового ключа: На кожному етапі блоку даних додається раундовий ключ, що збільшує стійкість алгоритму до простих атак.

Лінійні перетворення: Використовуються для змішування бітів у блоці, забезпечуючи складність для криптоаналізу.

Модифіковані S-блоки: Спеціальні підстановчі блоки в алгоритмі «Калина» створюють нелінійність та забезпечують стійкість до диференціального аналізу.

4. Стійкість до атак і особливості безпеки «Калина»

Стійкість до диференціального та лінійного криптоаналізу: Завдяки складній структурі SP-мережі, підстановкам та лінійним перетворенням, «Калина» має високу стійкість до диференціального криптоаналізу, що захищає її від багатьох типів атак.

Великі розміри блоку: Підтримка розміру блоку до 512 біт забезпечує стійкість до атак, що використовують повторення шифрованих блоків у великих обсягах даних, роблячи алгоритм ефективним для захисту інформації в державних системах.

Висока криптостійкість: Алгоритм має високу стійкість до методів криптоаналізу, зокрема, до атак на ключ і диференціального криптоаналізу, завдяки комбінуванню операцій SP-мережі та великим розмірам блоку і ключа.

5. Застосування та значення стандарту «Калина»

Національна безпека: Алгоритм «Калина» був розроблений спеціально для потреб державних установ України, де висока стійкість до криптоаналітичних атак має вирішальне значення.

Альтернатива іноземним стандартам: Розробка власного стандарту шифрування дозволяє Україні уникнути залежності від іноземних криптографічних алгоритмів, таких як AES, і створити незалежну систему захисту інформації.

Перспективи використання: «Калина» підходить для використання у державних інформаційних системах, системах військового зв’язку, а також у комерційних рішеннях, що вимагають високої стійкості до атак.

Тема 6. Порівняльний аналіз сучасних криптоалгоритмів за призначенням.

Сучасні криптоалгоритми мають свої унікальні властивості та застосування залежно від вимог до безпеки, швидкості та ресурсів. Симетричні алгоритми використовуються для швидкого шифрування, асиметричні — для аутентифікації та обміну ключами, а алгоритми хешування — для забезпечення цілісності даних. Вибір відповідного алгоритму залежить від конкретних задач і середовища застосування.

1. Вступ до класифікації криптоалгоритмів

Криптоалгоритми є основою захисту інформації у сучасному світі. Їх можна класифікувати за призначенням та типом використання. Основні категорії криптоалгоритмів включають:

Симетричні алгоритми шифрування: Використовують один і той самий ключ для шифрування і дешифрування.

Асиметричні алгоритми шифрування: Використовують пари ключів (відкритий та закритий) для шифрування і дешифрування.

Алгоритми хешування: Призначені для перевірки цілісності даних шляхом створення унікального цифрового відбитка.

Ці алгоритми можуть застосовуватись для різних цілей, включаючи захист даних, аутентифікацію, підтвердження цілісності та інші задачі.

2. Симетричні алгоритми шифрування

Призначення: Захист конфіденційності даних у каналах зв'язку та в збережених файлах шляхом шифрування

AES (Advanced Encryption Standard): Стандарт, який широко використовується в комерційних і державних системах для захисту даних. Побудований на основі SP-мережі, AES забезпечує високу стійкість завдяки великим розмірам ключів (128, 192, 256 біт).

DES і 3-DES: Застарілі стандарти, які раніше широко застосовувались, але в даний час майже не використовуються через їхню низьку стійкість до сучасних атак. 3-DES є модифікацією DES, що збільшує стійкість, але поступається AES.

ДСТУ 7624:2014 «Калина»: Національний стандарт України для симетричного блочного шифрування, який використовує SP-мережу та підтримує різні розміри блоків і ключів для гнучкого захисту державної інформації.

Переваги: Висока швидкість роботи, особливо для великих обсягів даних; відносно низькі вимоги до ресурсів.

Недоліки: Проблеми з передачею ключів, оскільки симетричні алгоритми вимагають, щоб обидві сторони мали один і той самий секретний ключ.

3. Асиметричні алгоритми шифрування

Призначення: Безпечний обмін ключами, цифровий підпис і аутентифікація.

RSA (Rivest–Shamir–Adleman): Один із найвідоміших асиметричних алгоритмів, який забезпечує безпечний обмін даними через використання відкритих і закритих ключів. Застосовується для шифрування та цифрового підпису.

Елліптичні криві (ECC - Elliptic Curve Cryptography): Використовує математичні властивості еліптичних кривих для забезпечення криптографічної стійкості. ECC забезпечує таку саму стійкість як і RSA, але при меншій довжині ключів, що робить його оптимальним для пристроїв з обмеженими ресурсами.

Diffie-Hellman: Алгоритм для безпечного обміну ключами, який дозволяє двом сторонам створити спільний секретний ключ через відкритий канал зв'язку без необхідності попереднього обміну секретами.

Переваги: Не потребує спільного секрету; дозволяє безпечний обмін даними через незахищені канали.

Недоліки: Більш ресурсомісткий і повільніший у порівнянні з симетричними алгоритмами.

4. Алгоритми хешування

Призначення: Забезпечення цілісності даних, створення цифрових підписів, захист паролів.

SHA-2 і SHA-3 (Secure Hash Algorithm): Високоефективні алгоритми, що створюють унікальний 256- або 512-бітний хеш для перевірки цілісності даних. SHA-3 був розроблений як новіший стандарт із покращеною стійкістю до певних типів атак.

MD5 (Message Digest Algorithm 5): Один із перших хеш-алгоритмів, нині вважається небезпечним через слабкості до колізій і не використовується для критично важливих додатків.

RIPEMD: Алгоритм, який забезпечує 160-бітний хеш і застосовується в окремих криптографічних протоколах. Має кілька модифікацій із різними розмірами хешу.

Переваги: Забезпечують швидку перевірку цілісності великих обсягів даних; часто використовуються для створення цифрових підписів і забезпечення цілісності файлів.

Недоліки: Деякі хеш-алгоритми мають вразливості до колізій (наприклад, MD5 і SHA-1).

5. Порівняльна таблиця криптоалгоритмів за призначенням

Категорія	Приклад алгоритму	Призначення	Переваги	Недоліки
Симетричне шифрування	AES, Калина	Захист конфіденційності даних	Висока швидкість, ефективність	Потреба в захищеному обміні ключами
Асиметричне шифрування	RSA, ECC	Безпечний обмін ключами, цифровий підпис	Не потребує спільного секрету	Більш ресурсомісткі, повільніші
Алгоритми хешування	SHA-2, SHA-3	Перевірка цілісності, захист паролів	Швидкі, забезпечують унікальність відбитків	Деякі схильні до колізій (MD5, SHA-1)

6. Вибір алгоритмів залежно від задачі

Захист даних у реальному часі: Для швидкого та безпечного шифрування великих обсягів даних у реальному часі зазвичай застосовуються симетричні алгоритми, такі як AES або Калина, через їхню ефективність і високу швидкість.

Цифровий підпис та аутентифікація: Для створення надійного цифрового підпису та забезпечення аутентифікації часто використовуються асиметричні алгоритми, зокрема RSA або ECC, оскільки вони дозволяють перевіряти підпис без необхідності обміну ключами.

Перевірка цілісності: Хеш-алгоритми (SHA-2, SHA-3) оптимальні для забезпечення цілісності переданих чи збережених даних. Вони дозволяють швидко перевірити, чи не було змін у повідомленні або файлі.

Змістовий модуль 2 . Криптосистеми з відкритим ключем.

Асиметричні алгоритми є важливими інструментами у забезпеченні безпеки інформації, дозволяючи здійснювати безпечний обмін ключами, аутентифікацію та контроль цілісності даних. Вибір конкретного алгоритму залежить від вимог до рівня безпеки, продуктивності та специфіки використання. У сучасних інформаційних системах комбінація симетричних і асиметричних методів дозволяє досягти максимального рівня захисту та ефективності.

Тема 7. Асиметричні алгоритми шифрування.

1. Вступ до асиметричних алгоритмів шифрування

Асиметричні алгоритми шифрування, також відомі як алгоритми з відкритим ключем, використовуються для безпечного обміну інформацією. На відміну від симетричних методів, які потребують одного секретного ключа, асиметричні алгоритми працюють із двома ключами.Ця технологія дозволяє уникнути проблем, пов'язаних із безпечним обміном ключами, що є значною перевагою над симетричними методами шифрування.

Відкритий ключ: Використовується для шифрування повідомлень. Цей ключ доступний всім користувачам.

Закритий ключ: Застосовується для розшифрування повідомлень . Цей ключ зберігається в секреті у власника.

2. Основні асиметричні алгоритми шифрування

1. Алгоритм RSA (Rivest–Shamir–Adleman) базується на складності факторизації добутку двох великих простих чисел. Відкритий ключ складається з великого числа, яке є добутком двох простих чисел, і експоненти, а закритий ключ — це інша експонента, пов'язана з цими числами.

Призначення: RSA використовується для шифрування, цифрового підпису і безпечного обміну ключами. Це один із найпопулярніших алгоритмів, що застосовується в системах захисту інформації.

Переваги: Високий рівень безпеки для даних за умов значної довжини ключів (2048 біт і більше).

Недоліки: Велика обчислювальна складність і повільна робота порівняно з симетричними алгоритмами.

2. **Алгоритм Ель-Гамаля —** це асиметричний криптоалгоритм, розроблений Тахером Ель-Гамалем у 1985 році. Цей алгоритм базується на складності обчислення дискретного логарифма, що робить його стійким до зломів. Він застосовується для забезпечення конфіденційності інформації та створення цифрових підписів.

Алгоритм Ель-Гамаля використовує:

Відкритий ключ: складається з трьох значень, відомих усім користувачам.

Закритий ключ: використовується для розшифрування повідомлень та зберігається в секреті у власника.

Порівняння з іншими асиметричними алгоритмами

Алгоритм Ель-Гамаля подібний до RSA за рівнем безпеки, але має більший обсяг шифротексту, що робить його менш ефективним для передачі великих обсягів даних. Натомість, його варіації використовуються в системах, які потребують додаткового рівня захисту, наприклад, у гібридних криптосистемах.

3. Алгоритми на еліптичних кривих (ECC - Elliptic Curve Cryptography) використовують математичні властивості еліптичних кривих над скінченними полями. Захист базується на складності обчислення дискретного логарифма на еліптичній кривій.

Призначення: ECC застосовується для шифрування, цифрових підписів, безпечного обміну ключами, а також у криптографічних протоколах для пристроїв з обмеженими ресурсами.

Переваги: Забезпечує високу криптостійкість при меншій довжині ключів порівняно з RSA. Ключі ECC коротші, що робить цей метод ефективним для мобільних пристроїв та систем з обмеженими ресурсами.

Недоліки: Ускладнення в реалізації і вища ймовірність помилок при впровадженні.

Тема 8. Принципи керування ключовою системою.

Ефективне керування ключами є критично важливим компонентом інформаційної безпеки. Дотримання принципів безпеки, таких як секретність, цілісність та доступність, а також впровадження надійних протоколів і використання сучасних інструментів дозволяє забезпечити надійний захист інформації в цифрових системах.

1. Керування ключовою системою

Ключі є основою безпеки криптографічних систем, і ефективне керування ними є критично важливим для забезпечення надійності захисту інформації. Під керуванням ключовою системою розуміють всі аспекти генерації, розподілу, зберігання, використання та утилізації криптографічних ключів.

Завдання керування ключами включають: забезпечення конфіденційності та цілісності ключів; уникнення компрометації ключів; забезпечення своєчасного оновлення або заміни ключів.

2. Основні компоненти керування ключами

Система керування ключами складається з кількох ключових компонентів:

Генерація ключів: Процес створення криптографічних ключів, який має відповідати високим стандартам випадковості та непередбачуваності. Для цього використовуються генератори випадкових чисел або криптографічно безпечні генератори псевдовипадкових чисел (CSPRNG). Ключі мають бути випадковими та надійно згенерованими. Недостатньо надійні генератори випадкових чисел можуть стати причиною компрометації всієї системи.

Розподіл ключів: Процес передачі ключів між учасниками системи, який повинен бути захищеним від несанкціонованого доступу. Серед методів передачі ключів — протокол Діффі-Хеллмана та інші асиметричні методи, які забезпечують безпечний обмін ключами через незахищені канали.

Зберігання ключів: Ключі повинні зберігатися у безпечному середовищі, наприклад, в апаратних модулях захисту (HSM) або на захищених серверах, щоб уникнути їхнього витоку. Потрібно слідкувати за строками використання ключів, оскільки тривале використання одного ключа збільшує ризик його зламу.

Використання ключів: Ключі повинні застосовуватися строго у визначених межах, що знижує ризик їх компрометації. Це включає контроль за тим, як часто використовується ключ і для яких цілей. Потрібно слідкувати за строками використання ключів, оскільки тривале використання одного ключа збільшує ризик його зламу.

Оновлення і ротація ключів: Регулярне оновлення ключів є необхідним для забезпечення стійкості системи до атак. Ключі можуть замінюватися через певні інтервали або після досягнення ліміту використання.

Відкликання і утилізація ключів: У разі компрометації або закінчення терміну використання, ключі відкликаються і безпечно утилізуються, щоб звести до мінімуму ризик їхнього несанкціонованого використання.

3. Методи керування ключами

Симетричне керування ключами: У симетричних системах обидві сторони використовують один і той самий ключ. Це вимагає забезпечення безпечного каналу для передачі ключів. Основним викликом є безпечний обмін ключами, оскільки витік ключа призводить до повного компрометування даних.

Асиметричне керування ключами:

У асиметричних системах ключова пара складається з відкритого та закритого ключів. Відкритий ключ можна вільно розповсюджувати, а закритий зберігається у таємниці. Ключовою перевагою є відсутність необхідності передавати закритий ключ, що значно підвищує безпеку системи.

Гібридні методи:

Поєднують симетричне і асиметричне шифрування: асиметричні ключі використовуються для обміну симетричними ключами, які надалі застосовуються для шифрування даних. Це забезпечує високу ефективність і безпеку, дозволяючи використовувати симетричні алгоритми для шифрування великих обсягів даних.

4. Протоколи керування ключами

Протокол Диффі-Хеллмана:

Використовується для безпечного обміну симетричними ключами між двома сторонами без попередньої обміну секретами. Використовується в багатьох мережевих протоколах, таких як SSL/TLS.

PKI (Інфраструктура відкритих ключів):

PKI — це система, яка використовує сертифікати для автентифікації ключів. Сертифікати підписуються центром сертифікації (CA), що дозволяє стороні, яка приймає ключ, бути впевненою у його справжності. PKI широко використовується в електронній комерції та системах захищених комунікацій, де важлива довіра до автентичності ключів.

Протокол Kerberos:

Використовується для автентифікації в комп'ютерних мережах. Ключі у протоколі Kerberos генеруються центром розподілу ключів (KDC), який видає тимчасові квитки для доступу до ресурсів. Kerberos застосовується в корпоративних мережах для контролю доступу до внутрішніх ресурсів.

5. Принципи безпеки в керуванні ключами

Секретність: Приватні ключі повинні зберігатися у захищених місцях і не передаватися через незахищені канали.

Цілісність: Система повинна гарантувати, що ключі не будуть змінені або скомпрометовані.

Доступність: Необхідно забезпечити постійний доступ до ключів для уповноважених користувачів.

Відстеження та аудит: Система повинна підтримувати реєстрацію подій, пов'язаних з ключами, щоб забезпечити можливість аналізу в разі підозри на витік.

6. Інструменти для керування ключами

Сьогодні використовуються спеціалізовані інструменти та системи для автоматизації процесів керування ключами, такі як:

HSM (Hardware Security Module): Апаратні модулі для захищеного зберігання та обробки ключів.

KMS (Key Management Service): Хмарні сервіси для централізованого керування ключами, наприклад, AWS KMS.

OpenSSL: Бібліотека з відкритим кодом, яка забезпечує базові функції для створення і керування ключами, підтримує стандарти PKI.

Тема 9 Процедури шифрування в криптосистемі Ель– Гамаля

Криптосистема Ель-Гамаля базується на складності обчислення дискретного логарифма та використовує принципи обміну ключами алгоритму Діффі-Хеллмана для створення асиметричної системи шифрування. Її стійкість заснована на тому, що обчислення приватного ключа з відкритого ключа є надзвичайно складним завданням, яке практично неможливо виконати за прийнятний час при правильному виборі параметрів.

Криптосистема Ель-Гамаля складається з трьох основних процедур:

Генерація ключів; шифрування повідомлень; розшифрування повідомлень.

Алгоритм Ель Гамаля призначений для зашифрування та розшифрування повідомлення за допомогою узгодженого сеансового ключа на підставі протоколу Діффі-Хеллмана. Ключ, який використовується спільно двома користувачами для обміну повідомленнями, повинен мати таку ж довжину, як і відкритий текст, і бути представленим у двійковому форматі. Шифрування відбувається методом гамування, де відкритий текст, що представлений у двійковому форматі зашифровується ключем (гамою). Зворотнє перетворення, тобто розшифрування криптограми, відбувається за допомогою тієї самої гами методом гамування.

Застосування криптосистеми Ель-Гамаля

Алгоритм Ель-Гамаля знаходить застосування в різних криптографічних протоколах та стандартних криптографічних рішеннях, як-от цифрові підписи та захист даних у мережах. Він є основою для багатьох сучасних асиметричних систем шифрування.

10 Шифрування в криптосистемі RSA.

RSA (Rivest-Shamir-Adleman) — це криптосистема з відкритим ключем, заснована на математичних операціях із великими простими числами. Основою її безпеки є складність факторизації великих чисел,

які є добутком двох простих чисел. Це робить RSA популярним вибором для шифрування, цифрових підписів і обміну ключами.

RSA працює в три етапи: генерація ключів (відкритого та відповідного секретного ключа); шифрування повідомлень за допомогою відкритого ключа; розшифрування криптограми за допомогою секретного ключа.

Користувач генерує пару ключів: відкритий ключ для шифрування та приватний ключ для розшифрування, кожен з яких має бути щонайменше 2048 біт.

Переваги та недоліки RSA

Переваги: підтримує як шифрування, так і цифрові підписи та має високу безпеку при правильному виборі ключів.

Недоліки: повільне шифрування і розшифрування великих даних; схильність до деяких специфічних атак, якщо використовуються слабкі ключі або погано реалізовані методи захисту.

RSA широко використовується в таких сферах, як: захищений обмін ключами у протоколах SSL/TLS; системи цифрового підпису для автентифікації та забезпечення цілісності даних; безпечна передача конфіденційних даних у системах електронної комерції та фінансах.

Тема 11. Системи ідентифікації та автентифікації.

Системи ідентифікації та автентифікації є важливим елементом кібербезпеки, оскільки дозволяють запобігати несанкціонованому доступу до ресурсів, що значно знижує ризик витоку даних і шахрайських дій.

1. Вступ до систем ідентифікації та автентифікації

Ідентифікація та автентифікація є фундаментальними елементами забезпечення інформаційної безпеки в будь-якій системі. Ідентифікація дозволяє системі визначити, хто намагається отримати доступ до її ресурсів, а автентифікація підтверджує, що цей користувач є тим, за кого себе видає.

2. Відмінності між ідентифікацією та автентифікацією

Ідентифікація: Процес, при якому користувач повідомляє систему про свою особу (наприклад, за допомогою логіна або ID).

Автентифікація: Процес підтвердження особи користувача, зазвичай шляхом перевірки пароля, біометричних даних або інших даних автентифікації.

3. Методи автентифікації

Сучасні системи автентифікації використовують різні методи перевірки користувача, які можна поділити на три основні категорії:

Що знає користувач: Це можуть бути паролі, PIN-коди або відповіді на секретні запитання.

Що має користувач: Смартфони, токени, магнітні картки та інші фізичні пристрої, які можуть генерувати одноразові паролі (OTP).

Що являє собою користувач: Біометричні дані, такі як відбитки пальців, сканування райдужки або розпізнавання обличчя.

4. Двофакторна та багатофакторна автентифікація

Двофакторна автентифікація (2FA): Поєднання двох з трьох факторів автентифікації для посилення захисту, наприклад, пароль + одноразовий код, надісланий на смартфон.

Багатофакторна автентифікація (MFA): Використання трьох або більше методів автентифікації для додаткового захисту, що підвищує стійкість до атак.

5. Основні типи систем автентифікації

Однофакторна автентифікація: Найбільш поширений метод, який використовує лише один спосіб ідентифікації (наприклад, пароль).

Системи з OTP (одноразовими паролями): Паролі, які генеруються лише на один сеанс або транзакцію. Вони можуть бути програмними (генерація додатками) або апаратними (наприклад, апаратні токени).

Біометричні системи автентифікації: Включають використання унікальних фізичних або поведінкових характеристик для підтвердження особи користувача. Біометрія важлива для автентифікації, оскільки важко підробити чи відтворити фізичні характеристики.

6. Протоколи автентифікації

Системи автентифікації реалізуються через різні протоколи, які забезпечують обмін даними між користувачем та сервером. Основні протоколи:

Kerberos: Протокол, заснований на квитках, який забезпечує автентифікацію на основі секретних ключів та симетричного шифрування. Використовується в корпоративних мережах.

OAuth: Протокол, що дозволяє авторизацію через сторонні сервіси (наприклад, Facebook або Google) без необхідності надавати пароль. Це зручний спосіб доступу до сторонніх ресурсів.

SAML (Security Assertion Markup Language): Використовується для передачі даних автентифікації між серверами в корпоративних середовищах. SAML підтримує одноразову автентифікацію (SSO), що дозволяє користувачам входити в декілька систем після першого успішного входу.

7. Методи захисту систем ідентифікації та автентифікації

Шифрування паролів: Використання хешування та солі (salt) для збереження паролів у захищеному вигляді на сервері.

CAPTCHA та reCAPTCHA: Додаються до процесу автентифікації, щоб відрізнити людину від бота.

Обмеження кількості спроб входу: Запобігання брутфорс-атакам через блокування акаунта після певної кількості невдалих спроб.

Контроль доступу на основі ролей (RBAC): Визначення рівнів доступу для користувачів на основі їх ролей у системі, що знижує ризики несанкціонованого доступу.

Системи автентифікації широко застосовуються у корпоративних середовищах для захисту доступу до ресурсів; онлайн-банкінгу та фінансових сервісах; соціальних мережах і комерційних платформах, де потрібна безпека особистих даних; урядових структурах для захисту інформації державного значення.

Тема 12. Методи побудови схем електронного підпису

Електронний підпис (ЕП) — це криптографічний механізм, який забезпечує автентифікацію особи підписувача, цілісність і незмінність документа. Електронний підпис підтверджує авторство та забезпечує довіру до цифрових документів. Основні вимоги до електронного підпису:

Автентифікація: підтвердження особи, яка підписує документ.

Цілісність даних: гарантія того, що дані не змінені після підпису.

Незаперечність: підписувач не може відмовитися від факту підписання.

Сучасні електронні підписи побудовані на основі асиметричних криптосистем, що використовують пару ключів:

Закритий ключ: відомий тільки підписувачу та використовується для створення підпису.

Відкритий ключ: використовується для перевірки підпису та може бути доступним будь-кому.

Електронний підпис складається з наступних етапів: генерування пари ключів; процесу створення підпису; процесу перевірки ключів.

Процес створення електронного підпису

Хешування документа: Документ обробляється криптографічною хеш-функцією (наприклад, SHA-256), щоб отримати фіксовану довжину хеш-коду (хеш-значення). Цей хеш є унікальним для кожного документу.

Шифрування хешу: Підписувач використовує свій приватний ключ для шифрування хеш-значення, і це зашифроване значення стає електронним підписом документа.

Додавання підпису до документа: Підпис додається до документа, створюючи підписаний документ.

Процес перевірки електронного підпису

Хешування документа: Одержувач також хешує отриманий документ, отримуючи хеш-код, що має збігатися з оригіналом.

Розшифрування підпису: Підпис розшифровується за допомогою відкритого ключа підписувача для отримання хеш-значення, що було створене підписувачем.

Порівняння хешів: Якщо хеш-значення, отримане після розшифрування, співпадає з хешем отриманого документа, підпис вважається автентичним.

Методи побудови електронних підписів в різних алгоритмах

Алгоритм RSA: Використовує асиметричне шифрування, де закритий ключ шифрує хеш, створюючи підпис. Надійність забезпечується складністю розкладу великих чисел на прості множники.

Електронний підпис на основі алгоритму DSA (Digital Signature Algorithm): DSA використовує еліптичні криві для генерування підпису. Він є стандартом США для цифрових підписів і забезпечує високу безпеку.

ECDSA (Elliptic Curve Digital Signature Algorithm): Вдосконалена версія DSA на основі еліптичних кривих, яка забезпечує високу безпеку при меншій довжині ключів, що знижує обсяг даних.

Алгоритм Ель-Гамаля: Створює цифровий підпис на основі складності обчислень з дискретним логарифмуванням. Цей алгоритм рідше використовується, однак забезпечує високу стійкість при відповідних параметрах.

Стандарти електронного підпису

PKCS #1: Стандарт для використання електронного підпису з RSA. Забезпечує сумісність між різними системами, які використовують RSA для підпису.

FIPS 186-4: Федеральний стандарт США, який описує методи створення цифрового підпису, включаючи DSA та ECDSA.

XAdES (XML Advanced Electronic Signatures): Стандарт для електронного підпису XML-документів, що забезпечує цілісність і юридичну силу підписаних документів.

PAdES (PDF Advanced Electronic Signatures): Стандарт для підпису PDF-документів, що дозволяє зберігати юридично значущі документи в PDF-форматі.

Електронний підпис широко застосовується у: системах електронного документообігу (для підпису контрактів, угод); системах онлайн-банкінгу та фінансових операцій; юридичних системах та судових процесах; електронному урядуванні для забезпечення безпеки та автентичності документів державного значення.

10. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. **Мартинюк, В. М., Гуменюк, О. В., & Слободянюк, В. В.** Криптографічні методи захисту інформації : навч. посіб. / В. М. Мартинюк, О. В. Гуменюк, В. В. Слободянюк. – Київ : Техніка, 2020. – 304 с.
2. **Семенко, І. В., Копиленко, С. П.** Інформаційна безпека та криптологія: теорія і практика : підручник / І. В. Семенко, С. П. Копиленко. – Харків : Основа, 2021. – 352 с.
3. **Петренко, О. І., Корж, А. В.** Захист інформації в комп'ютерних системах та мережах : навч. посіб. / О. І. Петренко, А. В. Корж. – Львів : ЛНУ ім. І. Франка, 2019. – 278 с.
4. **Онацький О.В., Йона Л.Г., Бєлова Ю.В.** Криптографічний захист інформації: Навч. посіб./ О.В.Онацький, Л.Г.Йона , Ю.В. Бєлова. - Одеса: ДУІТЗ, 2023. – 250 с..

Допоміжна

1. **Шевченко, В.** Прикладна криптографія : підручник / В. Шевченко. – Київ : Наукова думка, 2019. – 320 с.

Інформаційні ресурси

1 Наказ МОН № 332 від 18.03.2021 року Про затвердження стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти. URL: https://osvita.ua/legislation/Vishya_osvita.
2 Національна бібліотека України ім. В.І. Вернадського. URL: http://www.nbuv.gov.ua.
3 Портал кіберполіції України. URL: https://cyberpolice.gov.ua/
4 Портал урядової команди реагування на комп’ютерні надзвичайні події України (CERT-UA). URL: https://cert.gov.ua/
5 Coursera. Стенфорд, Мічіганський університет та інші.Coursera.org
6 Cryptography Stack Exchange. crypto.stackexchange.com
7 MIT OpenCourseWare. ocw.mit.edu
8 IEEE Xplore Digital Library.ieeexplore.ieee.org