МІНІСТЕРСТВО ОСВІТИ І НАУКИ,
МОЛОДІ ТА СПОРТУ УКРАЇНИ

Запорізький національний технічний університет

КОНТРОЛЬНА РОБОТА
та методичні вказівки до неї з дисципліни
«Захист інформації в телекомунікаційних системах»
для студентів напряму підготовки 6.05093
«Телекомунікації»
заочної форми навчання

2011

Контрольна робота та методичні вказівки до неї з дисципліни «Захист інформації в телекомунікаційних системах» для студентів напряму підготовки 6.05093«Телекомунікації» заочної форми навчання /Укл. В.П. Дмитренко. – Запоріжжя : ЗНТУ, 2011. – 30с.

Укладач: В.П. Дмитренко, доцент, к.т.н.

Рецензент: Б.М. Бондарев, доцент, к.т.н.

Відповідальний
за випуск: В.П. Дмитренко, доцент, к.т.н.

Затверджено
на засіданні кафедри
«Радіотехніка та телокомунікації»
Протокол №3

Від «23» листопада 2011р.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АК	–	асиметрична криптографія
ВА	–	випадкова антена
ВГ	–	випромінювач Гюйгенса
ВЧ	–	висока частота
ДТЗС	–	допоміжні технічні засоби і системи
ЕЕВ	–	елементарний електричний вібратор
ЕМВ	–	елементарний магнітний вібратор
ЕМХ	–	електромагнітна хвиля
ЕЦП	–	електронний цифровий підпис
КЗ	–	контрольована зона
ЛРЗ	–	лінійний регістр зсуву
ЛФ	–	логічна функція
НД	–	несанкціонований доступ
НЛ	–	нелінійний локатор
НСД	–	найбільший спільний дільник
НСК	–	найменше спільне кратне
СК	–	симетрична криптографія
СФ	–	сітка Фейштеля
ТЗПІ	–	технічні засоби передачі інформації
ФХ	–	функція хешування
DES	–	стандарт блочного шифрування в СК
RSA	–	система шифрування в АК

ЗАВДАННЯ НА КОНТРОЛЬНУ РОБОТУ

В задачах параметр k – номер варіанту . Значення k дорівнює номеру в списку групи.

Завдання 1. Розрахунок параметрів сигналів

1. На території режимного об'єкту установлено апаратуру радіопротидії з потужністю $P_ш = k \cdot 5$(Вт). Вона створює перешкоди у смузі частот $\Delta f_ш = k \cdot 10$ (КГц) при середній частоті шумового сигналу, котра співпадає з середньою частотою спектру небезпечного сигналу, створюваного ТЗПІ режимного об'єкту. Антена станції протидії направлена на місце можливого розташування пристрою перехоплення за межами контрольованої зони на відстані R= 1000(М), та має коефіцієнт підсилення G = 2. У місці можливого перехоплення проводяться виміри радіочастотної обстановки за допомогою селективного мікровольт метра з антеною (приймачем). Смуга частот приймача при вимірюванні була встановлена $\Delta f_п = k \cdot 2$ (КГц). При цьому виміри показали, що при відключенні станції протидії рівень напруженості електричного поля, створюваного ТЗПІ об'єкту у місці можливого перехоплення $E_{ТЗПІ} = k \cdot 4$ (мВ/м).

Визначити, яким буде відношення С/Ш у місці можливого перехоплення, якщо станція перешкод буде працювати та у випадку, якщо станція перешкод не буде працювати.

2. Випромінювальна антена у вигляді диполя розташована у повітрі, та має дієву висоту $h=k \cdot 2$(М) та випромінює сигнал на частоті f=10/k (МГц).

Визначити величину струму, який потрібно підвести до антени, щоб забезпечити потужність випромінювання $P_{вип}$=40 (Вт).

Завдання 2. Модульна математика.

1. Знайти розв'язок порівняння першого степеня $(25+k) \cdot x \equiv 1 \bmod 107$;
2. З використанням алгоритму послідовного підведення до квадрата обчислити величину $15^{(34+k)} \bmod 107$.

Завдання 3. Алгоритм шифрування RSA

Згенерувати відкритий і закритий ключі в алгоритмі шифрування RSA, обравши прості числа p і q з таблиці простих чисел

(додаток Б). Зашифрувати повідомлення, що складається з Ваших ініціалів: ПІБ. Правильність перевірити дешифруванням.

Завдання 4. Функції хешування

Знайти хеш-образ свого прізвища, використовуючи (згідно з рекомендацією х.509 МККТТ) хеш-функцію $H_i=(H_{i-1} + M_i)^2 \bmod n$, де $n=p \cdot q$; p,q – взяти з Завдання 3. Значення H_0 задати довільно.

Завдання 5. Електронний цифровий підпис (ЕЦП)

З використанням хеш-образу свого Прізвища, обчислити ЕЦП за схемою RSA. Виконати перевірку обчисленого ЕЦП.

МЕТОДИЧНІ ВКАЗІВКИ ТА ПРИКЛАДИ ВИКОНАННЯ ЗАВДАНЬ

Завдання 1. Розрахунок параметрів сигналів

1. Амплітудне значення E_m(В/М) напруженності електричного поля на відстані r(М) від антени з коефіцієнтом підсилення G розраховується за формулою:

$$E_m = \frac{\sqrt{60 \cdot P_\Sigma \cdot G}}{r},$$

де P_Σ (Вт) – потужність випромінювання антени.

2. Опір випромінення R_Σ (Ом) антени у вигляді диполя з дієвою довжиною h(М) розраховується за формулою:

$R_\Sigma = 80 \cdot \pi^2 \cdot (h/\lambda)^2$, де λ (М) – довжина хвилі.

3. Потужність випромінення P_Σ (Вт) лінійної антени з опором випромінення R_Σ (Ом) визначається за формулою:

$$P_\Sigma = 0,5 \cdot I^2 \cdot R_\Sigma,$$

де I(А) – струм, підведений до антени (амплітуда).

При цьому вважається, що струм розподілено рівномірно по довжині антени.

4. Ефективна шумова температура джерела шумів T_e(в градусах Кельвіна) вводиться, як коефіцієнт, що зв'язує потужність шумів $P_ш$ (Вт) та смуги пропускання Δf (Гц)

$Ð_ø = Ê_À \cdot Ò_å \cdot \Delta f$, де $K_Б$=1.38 · 10^{-23} Вт·с/°k – стала Больцмана.

Завдання 2. Модульна математика

1. Знайти розв'язок порівняння першого степеня

65 · x ≡ 1 mod 107 з використанням розширеного алгоритму Евкліда (a=65, m=107).

а) Знаходимо послідовно залишки від ділення:

107 = 65 · **1** + 42
65 = 42 · **1** + 23
42 = 23 · **1** + 19
23 = 19 · **1** + 4
19 = 4 · **4** + 3

$4 = 3 \cdot \mathbf{1} + 1$
$3 = 1 \cdot 3$
б) Складаємо таблицю

i	0	1	2	3	4	5	6	7
q_i		1	1	1	1	4	1	3
P_i	1	1	2	3	5	23	28	107

$P_0=1$; $P_1=1$; $P_i=q_i \cdot P_{i-1} + P_{i-2}$; $P_7=107$

в) розв'язком порівняння $65 \cdot x \equiv 1 \bmod 107$ є
$x = (-1)^{7-1} \cdot P_{7-1} = (-1)^6 \cdot 28 = 28.$
Перевірка: $65 \cdot 28 = 1820 \bmod 107 = 1.$
2. Обчислимо $b = 15^{74} \bmod 107$ ($a = 15$, $k = 74$, $m = 107$) методом послідовного підведення до квадрата.
а) $k = 0 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^7 + 1 \cdot 2^3 + 0 \cdot 2^4 + 0 \cdot 2^5 + 1 \cdot 2^6 \rightarrow$
(0,1 , 0,1 , 0 , 0,1); t=6.
б) b := 1
в) A:= 15
г) k_0:=0
д) i=1, k_1=1,A:=15^2mod107=225mod107=11
в:=11 · 1mod107=11 b=11
i=2, k_2=0,A:=11^2mod107=121mod107=14
i=3, k_3=1,A:=14^2mod107=196mod107=89
b:=89 · 1mod107=979mod107=50 b=50
i=4, k_4=0,A:=89^2mod107=7921mod107=3
i=5, k_5=0,A:=3^2mod107=9mod107=9
i=6, k_6=1,A:=9^2mod107=81mod107=81
b:=81 · 50mod107=4050mod107=91 b=91
є) b=91 Відповідь: 15^{74}mod107=91

Завдання 3. Алгоритм шифрування RSA
Згенерувати відкритий ***e*** та закритий ***d*** ключі і зашифрувати ініціали ДВП.

1. Генерування ключів Оберемо два прості числа p=13, q=19. Тоді модуль n=p · q=13 · 19=247 і функція Ейлера

φ(n)=(p-1) · (q-1)=12 · 18=216.

Закритий ключ обираємо з умов:

а) d<φ(n);

б)НСД(d,φ(n))=1.

Нехай *d*=25. Відкритий ключ *e* обираємо з умов:

а) e<φ(n);b) d · e≡1mod φ(n), тобто треба знайти рішення порівняння першого степеня 25 · e≡1mod 216.

Знаходимо послідовно залишки від ділення:

216=25 · **8** +16

25=16 · **1** +9

16=9 · **1** +7

9=7 · **1** +2

7=2 · **3** +1

2=1 · **2**

Складаємо таблицю:

i	0	1	2	3	4	5	6
q_i		8	1	1	1	3	2
P_i	1	8	9	17	26	95	216

P_0=1, P_1=3, $P_i=q_i \cdot P_{i-1} \cdot P_{i-2}$, P_6=216

Розв'язком порівняння 25 · e≡1mod 216

є $e=(-1)^{n-1} \cdot P_{n-1}=(-1)^5 \cdot 95$ mod216= -95mod216=121;

Відповідь: e=121.

Таким чином, відкритий ключ e{121,247}, а закритий d{25,247}.

2. Шифрування Представимо повідомлення ДВП, як послідовність цілих чисел-номерів відповідних літер в абетці. Тоді вихідне повідомлення M буде M{5,3,17}. Тут M_1=5,M_2=3,M_3=17 – це блоки відкритого повідомлення. Тоді блоки C_i зашифрованого повідомлення будуть (e{121,247} – відкритий ключ):

$C_1=5^{121}$mod247=226;

$C_2=3^{121}$vod247=185;

$C_3=17^{121}\text{mod}247=225$;

обчислення виконано за допомогою алгоритму послідовного підведення до квадрату.

Таким чином, відкритому повідомленнюM{5,3,17} відповідає шифрограма C{226,185,225}.

3. Дешифрування Розшифруємо поблоково повідомлення C{226,185,225}, користуючись закритим ключем d{25,247}:

$M_1=226^{25}\text{mod}247 = 5$;

$M_2=185^{25}\text{mod}247 = 3$;

$M_3=225^{25}\text{mod}247 = 17$;

обчислення виконано за допомогою алгоритму послідовного підведення до квадрата

Таким чином, із криптограми C{226,185,225} отримали після дешифрування закритим ключем вихідне повідомлення M{5,3,17}, тобто ДВП.

Завдання 4. Будемо використовувати хеш-функцію $H_i= (H_{i-1}+M_i)^2\text{mod } n$ для знаходження хеш-образу повідомлення ВІКТОР.

Представимо це слово послідовністю чисел M{3,10,12,20,16,18} по номерам відповідних літер в абетці. Оберемо два прості числа p = 13, q = 19, тоді n= p · q = 13 · 19 = =247 та візьмемо значення H_0= 8. Знайдемо хеш-образи H_i блоків M_i, i=1,2,…,6:

$H_1 = (H_0 + M_1)^2 \text{ mod}247 = (8+3)^2\text{mod}247 = 121 \text{ mod}247 = 121$;

$H_2 = (H_1 + M_2)^2 \text{ mod}247 = (121+10)^2\text{mod}247 = 17161 \text{ mod}247 = 118$;

$H_3 = (H_2 + M_3)^2 \text{ mod}247 = (118+12)^2\text{mod}247 = 16900 \text{ mod}247 = 104$;

$H_4 = (H_3 + M_4)^2 \text{ mod}247 = (104+20)^2\text{mod}247 = 15376 \text{ mod}247 = 62$;

$H_5 = (H_4 + M_5)^2 \text{ mod}247 = (62+16)^2\text{mod}247 = 6084 \text{ mod}247 = 156$;

$H_6 = (H_5 + M_6)^2 \text{ mod}247 = (156+18)^2\text{mod}247 = 30276 \text{ mod}247 = 142$.

Відповідь: хеш-образ повідомлення ВІКТОР – число 142.

Завдання 5. По хеш-образу повідомлення ВІКТОР (r = 142) з використанням закритого ключа алгоритму RSA d,n{25,247} розраховуємо ЕЦП S цього повідомлення:

$$S = 142^{25}\text{mod}247 = 194.$$

Розрахунок виконано за алгоритмом послідовного підведення до квадрата.

Для перевірки ЕЦП знайдемо $r^1=S^e \bmod n$, де {e, n} відкритий ключ {121, 247}. Тоді $r^1=194^{121} \bmod 247 = 142$

Розрахунок виконано за алгоритмом послідовного підведення до квадрата.

Результат: $r^1 = 142$. Таким чином, $r = r^1$, тобто підпис (ЕЦП) правильний, відправник той, за кого себе видає та повідомлення не було фальсифіковане при його передачі в каналі зв'язку.

ПИТАННЯ ДО ІСПИТУ

1. Інформація, як економічна категорія. Система захисту інформації.(СЗІ).
2. Захищена інформаційна система. Компоненти СЗІ.
3. Основні засоби захисту інформації. Підвищення ефективності програмного захисту.
4. Ідентифікація, аутентифікація, авторизація. Розширення парольного доступу.
5. Основні об'єкти технічного захисту інформації. Основні визначення (контрольована зона, сторонні провідники, випадкові антени і т.і.).
6. Технічні канали витоку інформації (ТКВІ). Принципи створення небезпечних сигналів.
7. Класифікації і характеристики ТКВІ.
8. Побічні (сторонні) електромагнітні випромінення і наведення (ПЕМВН)
9. Канали витоку мовної інформації.
10. Акустичні та віброакустичні канали витоку інформації.
11. ТКВІ при її передачі по каналам зв'язку.
12. Технічні канали витоку видової інформації.
13. Несанкціонований доступ (НД) до інформації, оброблюваної обчислювальною технікою. Різновиди атак на програмне забезпечення.
14. Випромінення елементарного електричного вібратору.
15. Випромінення елементарного магнітного вібратору.
16. Випромінення елементу Гюйгенса.
17. Турнікетний випромінювач.
18. Випромінення антен зі скінченними розмірами.
19. Закладні пристрої. Призначення, Різновиди, Діапазони.
20. Закладні пристрої без використання радіоканалу. (Цифровий диктофон)
21. Різновиди мікрофонів. Спрямовані мікрофони.
22. Лазерний мікрофон.
23. Технічні засоби захисту мовної інформації. Звукоізоляція.
24. Акустичні хвилеводи. Виникнення, Особливості. Захист.
25. Скремблери – різновиди, Характеристики.
26. Пошуковий комплекс СРМ – 700 «Акула»
27. Пошуковий комплекс ST – 031 «Піранья»

28. Аналізатори телефонних ліній.
29. Індикатори поля.
30. Випалювачі телефонних закладних пристроїв.
31. Системи віброакустичного зашумлення.
32. Придушувачі диктофонів та ВЧ електронних пристроїв.
33. Нелінійні радіолокатори. Принципи дії. Параметри.
34. Історія криптографії, найпростіші шифри.
35. Шифри одноалфавітної заміни. Парний шифр.
36. Шифри багатоалфавітної заміни. Шифрувальний блокнот.
37. Шифри Віжінера, Тритеміуса. Використання операції додавання за модулем.
38. Перестановчі шифри.
39. Шифр Вернама. Застосування логічної операції XOR.
40. Класифікація шифрів. Стійкість шифрів. Розмір ключа. Принцип Кергофа.
41. Криптоаналіз. Найпростіші алгоритми криптоаналізу.
42. Криптографічні алгоритми із симетричними ключами.
43. Поточні і блочні шифри. Схема шифрування поточним шифром. Вибір функції перетворення в поточному шифрі
44. Властивості логічної функції XOR та інверсії. Шифри гамування. Організація генератора шифрувальної послідовності. Лінійні регістри зсуву.
45. Блочне шифрування. Сітка Фейштеля. Алгоритм DES.
46. Основні визначення та поняття теорії чисел. Канонічне розкладання. Взаємно прості числа.
47. НСК, НСД. Алгоритм Евкліда пошуку НСД. Залишки від ділення.
48. Функція Ейлера та правила її знаходження.
49. Порівняння та їх властивості. Теореми Ферма та Ейлера.
50. Порівняння першого степеня, їх властивості та вирішення.
51. Обрахунок величини $b = a^k \bmod m$ методом послідовного підведення до квадрата.
52. Основні принципи АК. Ключі в АК. Система RSA. Етапи.
53. Генерування ключів в системі RSA.
54. Шифрування та дешифрування в RSA.
55. Властивості ЕЦП. Задачі АК та ЕЦП.
56. Функції хешування (ФХ). Задачі ФХ та вимоги до них.
57. Алгоритм RSA для розрахунку ФХ.
58. Класична система ЕЦП. Схема підпису в системі RSA.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1.Конахович Г.Ф., Климчук В.П.,Паук С.М., Потапов В.Г, Защита информации в телекоммуникационных системах. – Киев: «МК-Пресс», 2005- 288с

2. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам. – М: Горячая линия-Телеком,2003.-416с.

3. Конеев Н.Р., Беляев А.В. Информационная безопасность предприятия – СПБ: БХВ – Петербург, 2003.-725с.

4. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. –М.: Горячая линия – Телеком, 2001 . – 120с.

5. О защите информации в автоматизированных системах: Закон Украины от 05.07.1994 № 80194-ВС// Безопасность информации. - 1995.-№1.-с.72-75.

Додаток А

Основні визначення і поняття теорії чисел

Просте число – будь яке натуральне число, яке не має других дільників, окрім самого себе та 1.

Приклад 1,2,3,5,7,11,…,373,…,599,…

Складене число – ділиться (без залишку), окрім 1 та самого себе ще й на другі числа.

Приклади: число 12 має дільники 2 та 3, бо числа 4, 6 не можна розглядати, як дільники, оскільки вони самі складені;

число 77-дільники 7 та 11;

число 1 розглядається особливо.

Теорема Евкліда – множина простих чисел нескінчена.

Основна теорема арифметики - будь – яке ціле додатне число можна представити в вигляді добутку простих чисел, причому єдиним чином.

Приклад: $27=3\cdot3\cdot3$, $33=3\cdot11$,$126=2\cdot3^2\cdot7$,$1026=2\cdot503$,$4151=7\cdot593$.

Канонічне розкладання натурального числа n (витікає з основної теореми арифметики)- представлення числа в вигляді

$$n=P_1^{\alpha1}\cdot P_2^{\alpha2}\ldots P_n^{\alpha n}, \qquad (A.1)$$

де $P_1,P_2,\ldots,P_n$ – попарно різні прості числа,

$\alpha_1, \alpha_2,\ldots,\alpha_n$ – натуральні числа.

Взаємно прості числа – не мають жодного загального дільника, окрім 1. Приклад: 27 та 28- взаємно прості, а 27 та 33 ні, бо у них є загальний дільник 3.

Найбільший спільний дільник (НСД) двох чисел a та b позначають НСД (a,b), або (a,b). Якщо a та b взаємно прості, то $(a,b)=1$.

Найменше спільне кратне (НСК) двох чисел a та b визначається за фомулою

$$НСК(a,b)=\frac{a\cdot b}{(a,b)}. \qquad (A.2)$$

Якщо α та b взаємно прості, то НСК $(a,b)=a\cdot b$.

Алгоритм Евкліда пошуку НСД

Є два натуральні числа a та b. Хай $a<b$. Для пошуку (a,b) будемо послідовно знаходити залишки від ділення

$$b = à \cdot q_0 + r_1$$

$$a = r_1 \cdot q_1 + r_2$$

$$r_1 = r_2 \cdot q_2 + r_3$$

$$r_2 = r_2 \cdot q_3 + r_4$$

.....

$$r_{n-2} = r_{n-1} \cdot q_n + r_n$$

$$r_{n-1} = r_n \cdot q_n + 0$$

Í ÑÄ (à,b)=r_n

ßêùî r_n =1, òî à òà b âçàºì í î ï ðîñò³

Ï ðèêëàä: Í ÑÄ (114,534)

$534 = 114 \cdot 4 + 78$

$114 = 78 \cdot 1 + 36$

$78 = 36 \cdot 2 + 6$

$36 = 6 \cdot 6 + 0$

Í ÑÄ (114,534) = 6

Залишок від ділення цілих чисел

Розглянемо два цілих числа m та a. Хай $a > m$. Залишимо a в формі $a=m \cdot q+r$

Тут q – дільник, тобто результат ділення цілого числа a на ціле число m з **недостачею,** величина якої дорівнює r, тобто $q = \left\lfloor \frac{a}{m} \right\rfloor$.

Таким чином $a = m \cdot \left\lfloor \frac{a}{m} \right\rfloor + r$. Число r називається **залишком** від ділення a на m. Залишок прийнято позначати $r = a \bmod m$.

В криптографії використовуються і цілочисельні операції з **надлишком,** що позначається символом $\lceil ..... \rceil$.

Функція Ейлера φ(N)

φ(N) натурального числа N зветься **кількість тих чисел в ряді 1,2,3…., N-1, які є взаємно простими з N.**

Правила пошуку φ(N)

1. Якщо *a* та *b* взаємно прості, то
$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b). \quad (A.3)$$
2. Якщо *p* – просте число , то
$$\varphi(p) = p - 1. \quad (A.4)$$
3. Якщо *p* – просте число, *a* – натуральне, то
$$\varphi(p^{\alpha}) = p^{\alpha-1} \cdot (p-1). \quad (A.5)$$
4. Якщо *n* представлено канонічним розкладанням типу (A.1), то
$$\varphi(n) = P_1^{\alpha_1-1} \cdot P_2^{\alpha_2-1} \cdots P_K^{\alpha_K-1} \cdot (p_1-1) \cdot (p_2-1)...(p_k-1), \quad (A.6)$$
$$\text{або } \varphi(n) = n \cdot (1-\frac{1}{p_1}) \cdot (1-\frac{1}{p_2})....(1-\frac{1}{p_k}). \quad (A.7)$$

Приклади: $\varphi(15) = \varphi(3 \cdot 5) = \varphi(3) \cdot \varphi(5) = (3-1) \cdot (5-1) = 8$
(3 та 5 – взаємно прості);

$\varphi(45) = \varphi(9) \cdot \varphi(5) = \varphi(3^2) \cdot \varphi(5) = 3^{2-1} \cdot (3-1) \cdot (5-1) = 24$
(9 та 5- взаємно прості, але число 9 є складеним).

$\varphi(90) = \varphi(9 \cdot 5 \cdot 2) = \varphi(3^2 \cdot 5^1 \cdot 2^1) = 3^{2-1} \cdot 5^{1-1} \cdot 2^{1-1} \cdot (3-1) \cdot (5-1) \cdot (2-1) = 24.$

Визначення: Два цілих числа *a* та *b* є порівняними за модулем *m*, якщо різниця *a*-*b* ділиться на *m* без залишку.

Позначення: $a \equiv b \bmod m$

Властивості порівнянь (конгруенцій)

$$a \equiv a \bmod m. \quad (A.8)$$
$$a \equiv b \bmod m \Rightarrow b \equiv a \bmod m. \quad (A.9)$$
$$a \equiv b \bmod m \text{ òà } b \equiv a \bmod m \Rightarrow a \equiv b \bmod m. \quad (A.10)$$
$$a \equiv b \bmod m,\ k + b \equiv (k + a) \bmod m,\ \text{k-ö³ëå}. \quad (A.11)$$
$$a \equiv b \bmod m \Rightarrow k \cdot b \equiv (k \cdot a) \bmod m,\ \text{k-ö³ëå}. \quad (A.12)$$

$$k \cdot b \equiv k \cdot a \mod m \text{ òà } (k,m) = 1 \Rightarrow a \equiv b \mod m. \quad (A.13)$$

$$a \equiv b \mod m \text{ òà } c \equiv d \mod m \Rightarrow a \cdot c \equiv b \cdot d \mod m. \quad (A.14)$$

$$a \equiv b \mod m \text{ òà } c \equiv d \mod m \Rightarrow a + c \equiv (b + d) \mod m. \quad (A.15)$$

$$a \equiv b \mod m \Rightarrow a^n \equiv b^n \mod m, \text{ n-ö}^3\text{ëå}. \quad (A.16)$$

$$a \equiv b \mod m \Rightarrow a = b + m \cdot t, \text{ t-ö}^3\text{ëå}. \quad (A.17)$$

Запис $a \equiv 0 \mod m$ означає, що саме число *a* ділиться на m без залишку, тобто $a = k \cdot m$, k- ціле.

Якщо зафіксувати деякий модуль порівняння n, то **будь – яке натуральне** число **єдиним чином можна** представити у вигляді

$$c \equiv q \cdot n + r, \quad (A.18)$$

де q – дільник, r – залишок, що співпадає з одним з чисел 0,1,2,3,…..,(n-1).

З рівності (А.18) витікає, що

$$c \equiv r \mod n \quad (A.19)$$

тобто **будь-яке ціле число є порівняним зі своїм залишком за модулем n.**

Відмітимо, що **за модулем m=1 порівнянні будь–які два числа.**

Приклади порівнянь

1. $1 \equiv -5 \mod 6$ - правильне, бо $\frac{1-(-5)}{6} = 1 + 0$;

2. $121 \equiv 123456789876543 \mod 2$ – правильне, бо молодші розряди чисел *a* та *b* – непарні числа, а різниця **непарних чисел – парне число**, яке ділиться на 2 без залишку;

3. $121345678987 \equiv 12345678987 \mod 10$ - правильне, бо в молодших розрядах чисел a та b – однакові числа , тому різниця a-b буде мати в молодшому розряді 0, тобто така різниця ділиться на 10 без залишку;

4. $23 \equiv 1 \bmod 4$ – неправильне бо $\frac{23-1}{4} = 5$ залишок 2 (в той же час порівняння $23 \equiv -1 \bmod 4$, буде вірним, бо $\frac{23-(-1)}{4} = 6+0$);

5. $30 \cdot 17 \equiv (81 \cdot 19) \bmod 6$ – невірне, бо $30 \cdot 17 = 2 \cdot 3 \cdot 5 \cdot 17$, а $81 \cdot 19 = 9 \cdot 3 \cdot 3 \cdot 19$ і тоді в різниці $6 \cdot 5 \cdot 17 - 9 \cdot 3 \cdot 3 \cdot 19$ перше число ділиться на 6 без залишку, а друге – з залишком.

Теореми

Теорема 1**(Мала теорема Ферма)**
Якщо p- просте число, то

$$a^{p-1} \equiv 1 \bmod p. \qquad \text{(A.20)}$$

Наслідок:

$$a^{p-1} \bmod p = 1. \qquad \text{(A.21)}$$

Приклад: 1. $p = 3; a = 2; 2^2 \bmod 3 = 1;$

2. $p = 599; a = 5; 5^{598} \bmod 599 = 1.$

Теорема 2 **(Теорема Ейлера)**
Якщо *a* та n – взаємно прості, то

$$a^{\varphi(n)} \equiv 1 \bmod n. \qquad \text{(A.22)}$$

Наслідок:

$$a^{\varphi(n)} \bmod n = 1 \qquad \text{(A.23)}$$

Теорема Ферма є частинним випадком теореми Ейлера, коли p – просте число

Приклади: 1. $a = 3$, $n = 5$; $3^{\varphi(5)} \bmod 5 = 3^4 \bmod 5 = 81 \bmod 5 = 1$;

2. $a = 3$, $n = 4$; $3^{\varphi(4)} \bmod 5 = 3^{\varphi(2^2)} \bmod 5 = 3^2 \bmod 4 = 1$.

Теорема 3 (**близька до теореми Ейлера)**
Якщо p та q – прості числа, $p \neq q$ та k – довільне ціле число, то

$$a^{k\cdot\varphi(p\cdot q)+1} \bmod (p\cdot q) = a. \qquad \text{(A.24)}$$

Приклад: 1. $10^{49} \bmod 35 = 10$, бо при k=2 та 35=7·5 (7 та 5 – прості) буде $\varphi(35) = \varphi(5)\cdot\varphi(7) = 24$ і $k \cdot j\,(p\cdot q) + 1 = 2\cdot 24 + 1 = 49$. В той же час для умов цього прикладу теорему Ейлера (А.23) застосувати не можна, бо (10,35)=5, тобто 10 та 35 не взаємно прості.

2. $10^{106} \bmod 35 = 10$ – теж саме, що і в прикладі 1, але при k=3.

Вирішення порівнянь першого степеня

Визначення:

1.Порівнянням першого степеня є

$$a\cdot x \equiv 1 \bmod m \qquad \text{(A.25)}$$

де a,m – цілі , $0<a<m$.

2.Вирішенням порівняння (А.25) є таке ціле число $0<x<m$, що різниця $(a\cdot x-1)$ ділиться на m **без залишку.**

Властивості порівнянь першого степеня

1. Якщо a та m не взаємно прості, то порівняння $a\cdot x \equiv 1 \bmod m$ не має жодного розв'язку.

2. Якщо a та m взаємно прості, то порівняння $a\cdot x \equiv 1 \bmod m$ має єдиний розв'язок.

Знаходження розв'язку порівнянь першого степеня

1. Метод перебору Вибираємо із послідовності 1,2,3,…,m-1 ті числа, які є взаємно простими з m і підставляємо в (А.25). Число x, яке задовольняє (А.25), є роз в'язком.

2. Розширений алгоритм Ейлера Складається з 4 етапів:

а) перевіряємо число a та m на взаємну простоту. Якщо $(a,m)>1$, то розв'язку не існує;

б) Знаходимо послідовно залишки від ділення

$$m = a\cdot q_1 + r_1$$
$$a = r_1\cdot q_2 + r_2$$
$$r_1 = r_2\cdot q_3 + r$$
$$\cdots\cdots\cdots\cdots$$
$$r_{n-2} = r_{n-1}\cdot q_n + r_n$$
$$r_{n-1} = r_n\cdot q_{n+1} + 0$$

в) Складаємо таблицю

i	0	1	2	3	…….	n-1	n
q		q_1	q_2	q_3	…….	q_{n-1}	q_n
p_i	1	P_1	P_2	P_3	…….	P_{n-1}	p_n

Тут: $P_0=1$; $P_1=q$; $P_n=m$; $P_i=q_i \cdot P_{i-1}+P_{i-2}$, якщо $1<i<m$.

г) Знаходимо розв'язок x з виразу $\tilde{o} = (-1)^{n-1} \cdot P_{n-1.}$

Приклад:

1. $123 \cdot x \equiv 1 \bmod 369$.

а) $(123,369)=3$ – ров´язку не існує.

2. $16 \cdot x \equiv 1 \bmod 23$

а) $(16,23)=1$ – розв´язок існує і він єдиний;

б) Знаходимо залишки

1. $23 = 16 \cdot 1 + 7, \quad q_1 = 1, r_1 = 7$
2. $16 = 7 \cdot 2 + 2, \quad q_2 = 1, r_2 = 2$
3. $7 = 2 \cdot 3 + 1, \quad q_3 = 3, r_3 = 1$
4. $2 = 1 \cdot 2 + 0, \quad q_4 = 2, r_4 = 0$

в) Будуємо таблицю

i	0	1	2	3	4
q_i		1	2	3	2
P_i	1	1	3	10	23

$P_0=1; P_1=1; \; P_2=q_2 \cdot p_1+p_0=2 \cdot 1+1=3;$

$P_3=q_3 \cdot p_2+p_1=3 \cdot 3+1=10;$

г) Знаходимо розв'язок $\tilde{o} = (-1)^{4-1} \cdot P_{4-1} = (-1)^3 \cdot P_3 = -10$

Перевіряємо:

$16 \cdot (-10) \equiv 1 \bmod 23; \; \frac{-160-1}{23} = -7 + 0,$ значить x=-10 – це вирішення вихідного порівняння.

Знаходження розв'язку порівнянь першого степеня використовується в асиметричній криптографії , зокрема в алгоритмі RSA- при генеруванні відкритого ключа сеансу зв'язку.

Обчислення величини $b = a^k \bmod m$

Тут a – ціле число, a<m, $k \geq 0$.

Для розрахунку величини $b = a^k \bmod m$ звичайно використовують **алгоритм послідовного піднесення до квадрату.** Він складається з 6 етапів.

1.Розкладаємо k по степеням числа 2 та визначаємо максимальний степінь t

$k = k_0 \cdot 2^0 + k_1 \cdot 2^1 + k_2 \cdot 2^2 + ...k_t \cdot 2^t$; $\{k_0, k_1, k_2, ..., k_t\}$;

2. b:= 1. Якщо k=0, повертаємо b;
3. A:=a;
4. Якщо k_0=1, то b:= a;
5. Цикл по і від 1 до t
   5.1 A:=A^2mod m;
   5.2 Якщо k_i =1,то b:=(A·b)mod m;
6. Повертаємо b.

Приклад:

Розрахувати $b = 2^{18} \bmod 13$; тут a=2,k=18, m=13.

1. $k = 0 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4 \rightarrow \{0,1,0,0,1\}; t = 4$;
2. b:=1;
3. A:=2;
4. k_0=0;
5. $i = 1; k_1 = 1; A := 2^2 \bmod 13 = 4; b := 4 \cdot 1 \bmod 13 = 4; b := 4;$

   $i = 2; k_2 = 0; A := 4^2 \bmod 13 = 3;$

   $i = 3; k_3 = 0; A := 3^2 \bmod 13 = 9;$

   $i = 4; k_4 = 1; A := 9^2 \bmod 13 = 3; b := 3 \cdot 4 \bmod 13 = 12; b := 12;$
6. b:=12

Відповідь: b=12, тобто 2^{18} mod13=12.

Обчислення величини $b=a^k \bmod m$ використовуються в асиметричній криптографії; зокрема при шифруванні відкритим ключем отримувача, та дешифруванні закритим ключем відправника при застосуванні криптоалгоритму RSA.

Додаток Б

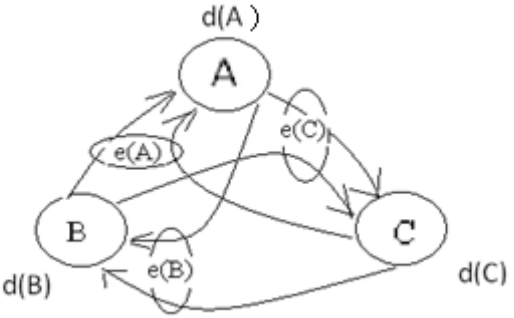
Таблиця простих чисел

1	47	113	197	281	379	463	571								
2	53	127	199	283	383	467	577								
3	59	131	211	293	389	479	587								
5	61	137	223	307	397	487	593								
7	67	139	227	311	401	491	599								
11	71	149	229	313	409	499	601								
13	73	151	233	317	419	503	607								
17	79	157	239	331	421	509	613								
19	83	163	241	337	431	521	617								
23	89	167	251	347	433	523	619								
29	97	173	257	349	439	541	631								
31	101	179	263	353	443	547	641								
37	103	181	269	359	449	557	643								
41	107	191	271	367	457	563	647								
43	109	293	277	373	461	569	.....								

Додаток В

Основні принципи асиметричної криптографії (АК). Алгоритм шифрування RSA

Кожен абонент володіє двома ключами – відкритим e (можна викласти в Інтернеті, або в телефонній книжці) і закритим d (таємний). Ключ *e* отримувача відправник використовує для шифрування, а отримувач дешифрує зашифроване повідомлення (шифртекст) своїм таємним ключем d. Схему ключів АК наведено на рисунку В.1.



A,B,C- абоненти
e(A), e(B),e(C)- відкриті ключі
d(A),d(B),d(C) – закриті (таємні ключі)

Рисунок В.1 – Схема ключів в АК

Принципи функціонування АК розглянемо на прикладі двох абонентів – А та В:

1. Абонент А генерує два ключа – e(A) та d(A) і передає ключ e(A) абоненту В по відкритому каналу;
2. Абонент В шифрує своє повідомлення з використанням ключа e(A);
3. Абонент В посилає свою шифрограму абоненту А по відкритому каналу;
4. Абонент А отримує шифрограму та дешифрує його за допомогою ключа d(A).

Пари e(A), d(A) та e(B), d(B) розраховується за допомогою спеціальних методів теорії чисел (модулярна математика), причому

жоден ключ не може бути (дуже складно) отримано (розраховано) із другого.

Найчастіше використовується криптографічна система RSA, запропонована в 1977р. Р.Ривестом (Rivest.R), А. Шамиром (Shamir A.) та А.Адлеманом (Adleman A.). Надійність шифрування за алгоритмом RSA базується на складності процедури **факторизації** (розкладання на прості множники) **великих** чисел та складності обрахунку дискретних логарифмів (знаходження x при відомих a,в, та m із рівняння $a^x=b(\mathrm{mod}(m))$.

Алгоритм RSA складається з трьох частин:

1.Генерування ключів.

Оберемо два великих простих числа p та q та знайдемо їх добуток n=p·q. Обчислимо функцію Ейлера $j(n)=(p-1)\cdot(q-1)$.

Закритий ключ d обираємо умов d<φ(n), та (d, φ(n))=1. Відкритий ключ *e* обираємо з умов *e*<φ(n) та $d\cdot e\equiv 1\mathrm{mod}\left(\varphi(n)\right)$, тобто треба знайти розв'язок порівняння першого степеня типу(А25),де в якості невідомої величини виступає *e*. З цією метою використовується розширеним алгоритм Евкліда (додаток А).

В алгоритмі RSA

{e,n}- відкритий ключ,

{d,n}- закритий ключ.

2.Шифрування

Вихідний текст розбивається на блоки M_i однакової довжини. Кожен блок представляється у вигляді великого десяткового числа, яке менше n, та шифрується окремо за формулою

$$M^e = C(\mathrm{mod}\ n),$$

де C – шифрблок, що відповідає блоку повідомлення M. Шифрблоки з'єднуються в шифрограму операцією конкатенації.

3.Дешифрування

При дешифруванні отримана шифрограма розбивається на блоки відомої довжини і кожен блок дешифрується окремо за формулою

$$C^d = M\left(\mathrm{mod}\ n\right).$$

Додаток Г

Електронний цифровий підпис (ЕЦП)

Г.1 Задачі та властивості ЕЦП

Схема АК, яка застосована навпаки, коли для шифрування задіяно закритий ключ (з невеликим доповненнями) дала можливість для розробки ще однієї галузі сучасної криптографії – ЕЦП. При створенні ЕЦП (під документом) в нього треба закласти достатньо інформації, щоб **будь-який** отримувач зміг пересвідчитися (за допомогою відкритого ключа відправника), що тільки ним (відправником) підписано (і відповідно, відправлено) підписане повідомлення. Але при цьому в підписі повинно бути недостатньо інформації, щоб **здобути** з неї сам **закритий ключ відправника** , бо після першого підписання будь-який отримувач (або зловмисник) буде мати можливість підписувати від імені відправника свої повідомлення, тобто технологія ЕЦП дуже нагадує асиметричний шифр, тільки навпаки.

Таким чином АК та ЕЦП вирішують цілком різні **задачі:**

АК – забезпечення **конфіденційності** повідомлення;

ЕЦП – забезпечення **аутентичност**і відправника і **цілісності** повідомлення.

По цій причині часто використовується спочатку шифрування повідомлення, а потім його підпис за допомогою ЕЦП.

Можна встановити три **властивості** ЕЦП(як і будь – якого другого):

1. Підписати документ можна тільки «законний » власник підпису;

2. Автор підпису не може від неї відмовитися;

3. В випадку виникнення суперечки можлива участь третіх осіб (наприклад, суду) для встановлення істинності підпису.

Для формування ЕЦП часто застосовують інверсію алгоритму RSA . Для зменшення вразливості ЕЦП до криптоатак застосовують підпис не всього документу, а лише деякої його **контрольної суми** h. При цьому повсюдно прийнято застосовувати тільки криптостійкі (необоротні,вірніше,важкооборотні) контрольні суми-хеш функції, або функції хешування.

Г.2 Функції хешування (ФХ) та вимоги до них

ФХ призначені для скорочення підписуваної частину документу, тому їх можна назвати **скорочувальними функціями**.

ФХ звуть таке перетворення даних, яке переводить рядок бітів M **довільної довжини** в рядок бітів h(M) деякої **фіксованої довжини**.

Вимоги до ФХ h(M):

1.ФХ h(M) повинна бути **чутливою** до будь — яких змін вхідної послідовності M;

2. Для данного значення h(M) повинно бути **неможливим знайти значення M (відновити M)**;

3. Для даного значення h(M) повинно бути **неможливим** знайти таке значення M', що $h((M') = h(M)$.

Г.3 Алгоритм RSA для розрахунку ФХ

Вхідна послідовність M розбивається на блоки M_i (i=1,2,..,k; тут k – кількість блоків) однакової довжини (фіксованої) та обробляються по блокове за формулою.

$$H_i = f(H_{i-1}, M_i), \qquad (Г.1)$$

де $f(H_{i-1}, M_i)$ - задана функція, H_0- довільний початковий вектор (вектор ініціалізації).

За **ФХ всього повідомлення** приймається те **значення ФХ** , **яке отримано** при вводі **останнього блоку M_k**.

В відповідності з рекомендацією МККТТ X.509 застосовується варіант ФХ за виразом

$$H_i = (H_{i-1} + M_i)^2 \bmod n, \qquad (Г.2)$$

де n=p·q, p та q- великі прості числа.

Г.4 Загальна (класична) схема ЕЦП

Для створення ЕЦП **відправник** виконує такі дії:

1. Застосовує до вихідного повідомлення ФХ;

2. Розраховує ЕЦП по хеш-образу повідомлення з використанням таємного (закритого) ключа створення підпису;

3. Формує нове повідомлення, яке складається з вихідного повідомлення (можливо зашифрованого) і приєднаного до нього ЕЦП.

Отримувач, отримавши підписане повідомлення, виконує такі дії:

1. Відокремлює ЕЦП від прийнятого повідомлення, тобто виділяє основне повідомлення та ФХ;

2. Застосовує до основного повідомлення ФХ;

3. З використанням відкритого ключа перевірки підпису здобуває хеш-образ повідомлення з ЕЦП;

4. Перевіряє відповідність обчисленого хеш-образу повідомлення (п.2) та добутого з ЕЦП. Якщо хеш-образи співпадають, то підпис визнається справжнім.

Г.5 Схема підпису RSA

Для отримання ЕЦП повідомлення M відправник виконує такі дії:

1. Розраховує хеш-образ r=h(M) повідомлення M за допомогою деякої ФХ, наприклад за виразом (Г.2);

2. Зашифровує отриманий хеш-образ r на своєму секретному ключі {d,n}, тобто обчислює значення

$$S = r^d \bmod n. \qquad (Г.3)$$

Величина S і є ЕЦП.

Для перевірки ЕЦП отримувач виконує такі дії :

1. **Розшифровує** підпис S на **відкритому** ключі {e,n} відправника, тобто обраховує

$$r' = S^e \bmod n \qquad (Г.4)$$

і таким чином відновлює **імовірний** хеш-образ r′ повідомлення M;

2. Обчислює хеш-образ h(M)=r повідомлення M за допомогою тієї ж ФХ, котру використовував відправник;

3. Порівнює отримані значення r та r'. Якщо вони співпадають, то підпис правильний, відправник дійсно є тим, за кого себе вbдає, і повідомлення не було змінене при передачі. Таким чином **задачі забезпечення аутентичності** відправника та **цілісності** повідомлення виконано.

Додаток Д

Сторінка шифр блокноту (розміром 8×20)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	В	’	Є	Т	Ь	С	Я	,	Н	А	Ч	Е	_	З	М	І	И	К	А	,
2	Н	Е	С	П	О	К	І	И	Н	А	_	Р	І	Ч	К	А	,			
3	Т	У	Л	И	Т	Ь	С	Я	_	Б	Л	И	З	Е	Н	Ь	К	О		
4	Д	О	_	П	І	Д	Н	І	Ж	Ж	Я	_	Г	І	Р					
5	А	_	Н	А	_	Т	О	М	У	_	Б	О	Щ	І						
6	Т	А	М	_	Ж	И	В	Е	_	М	А	Р	І	Ч	К	А				
7	В	_	Х	А	Т	І	,	Щ	О	_	С	Х	О	В	А	Л	А	С	Ь	
8	У	_	З	Е	Л	Е	Н	И	И	_	Б	І	Р	.						

Додаток Е

Таблиця символів алфавіту Z_{36}

Символ	Номер	Символ	Номер	Символ	Номер	Символ	Номер
А	1	З	10	О	19	Ч	28
Б	2	И	11	П	20	Ш	29
В	3	І	12	Р	21	Щ	30
Г	4	Ї	13	С	22	Ь	31
Ґ	5	Й	14	Т	23	Ю	32
Д	6	К	15	У	24	Я	33
Е	7	Л	16	Ф	25	пробіл	34
Є	8	М	17	Х	26	’	35
Ж	9	Н	18	Ц	27	,	36