Лекция 1

Введение в дисциплину. Основы теории чисел. Теория сравнений и ее приложения.

Методы защиты информации

- Физический
- криптографический
- стеганографический

Что такое криптология?

Криптоло́гия — наука, занимающаяся методами шифрования и дешифрования. Криптология состоит из двух частей — криптографии и криптоанализа.

Криптография занимается разработкой методов шифрования данных.

Криптоанализ занимается оценкой сильных и слабых сторон методов шифрования, а также разработкой методов, позволяющих взламывать криптосистемы.

Криптография обеспечивает

- **секретность данных**, т.е. защиту от несанкционированного знакомства с содержанием;
- **аутентификацию сообщений**, т.е. подтверждение их подлинности и времени создания;
- **невозможность отказа от авторства**, т.е. электронную подпись;
- **целостность данных**, т.е. защиту от несанкционированного изменения содержания.

Области применения криптографии

- Электронная Цифровая Подпись (ЭЦП);
- электронные деньги;
- электронное голосование;
- защита ценных бумаг и документов от подделок.

Периоды развития криптографии

Донаучный

Научный

Современный

- В 1978г. на основе концепции, которая была изложена в этой работе, три математика Ривест, Шамир, Адлеман предложили принципиально новый криптографический метод шифрования, который называется RSA.

Шифры и ключи

Основное понятие в криптографии – **шифр**. **Шифр** – это преобразование исходного, секретного сообщения с целью его защиты.

Выбор конкретного преобразования открытого текста определяется наиболее секретной частью криптографической защиты – так называемым **ключом защиты**.

При построении криптографической системы исходят из того, что противнику известен алгоритм шифрования, а стойкость шифра зависит только от ключа шифрования.

Классы шифров

Шифры простой замены	• шифр Цезаря, квадрат Полибия, шифр Плейфера, двойной квадрат
Шифры перестановки	• квадрат Лесандра, табличные способы перестановки, таблица с усложненным и элементами
Многоалфавитные шифры замены	• квадрат Виженера, шифр Грансфельда.

Криптография базируется на следующих разделах математики:

- теория чисел
- линейная алгебра
- алгебраические структуры

Арифметика целых чисел использует

множество целых чисел
Z={ …, -3,-2,-1,0,1,2,3,…}

бинарные операции: +, -, x

В арифметике целых чисел результатом деления **a** на **n** являются два числа **q** и **r**.

Отношения между этими четырьмя целыми числами задается *уравнением деления:*

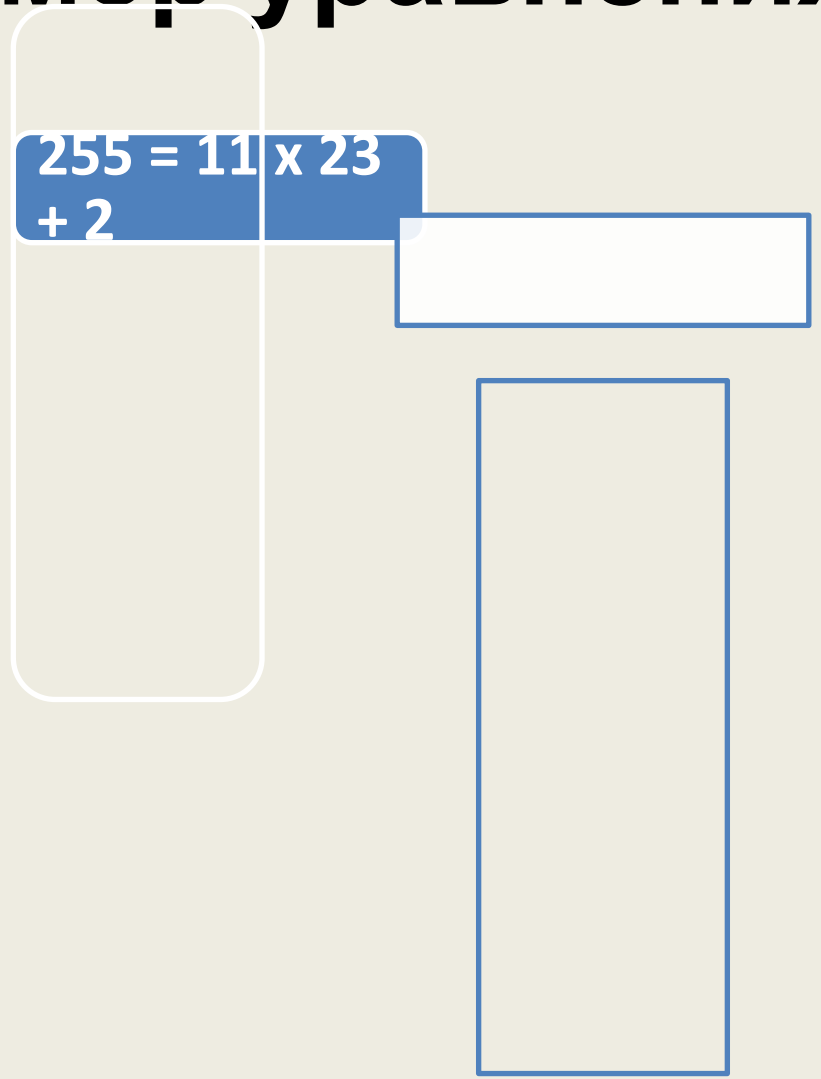
a = q x n + r, где

a - *делимое* ; q — *частное* ;

n — *делитель;* r — *остаток*.

Обратите внимание, что деление — это не операция, поскольку результат деления a на n — это два целых числа q и r.

Пример уравнения деления



Ограничения на уравнения деления в криптографии

Ограничение 1	• делитель должен быть положительным целым числом (n > 0) • Остаток должен быть неотрицательным целым числом (r >= 0)
Ограничение 2	
Например	• 255 = 11 x (-23) +(- 2)= 11 x (-24) + 9

Обозначение делимости

Если в уравнении деления r = 0, то есть a = q x n, то говорят, что a делится на n без остатка, или что n делит a и пишут

n | a.

Если остаток не является нулевым, то n не делит a, и пишут

n † a.

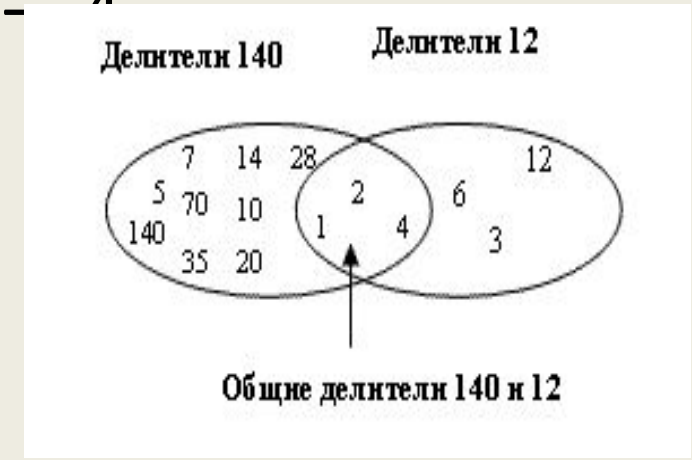
Например:

Отображение делимости: 13|78, 7|98, –6|24, 4|44.

Отображение неделимости 13†27, 7†50, –6|23, 4†41.

Наибольший общий делитель

- Два положительных целых числа могут иметь много общих делителей, но только один наибольший общий делитель.
- Например, общие делители чисел 12 и 140 есть 1, 2 и 4. Однако наибольший общий делитель - 4



Алгоритм Евклида нахождения НОД(a,b)

Алгоритм Евклида основан на следующих двух фактах:

Факт 1: **НОД (a, 0) = a**

Факт 2: **НОД (a, b) = НОД (b, r)**,

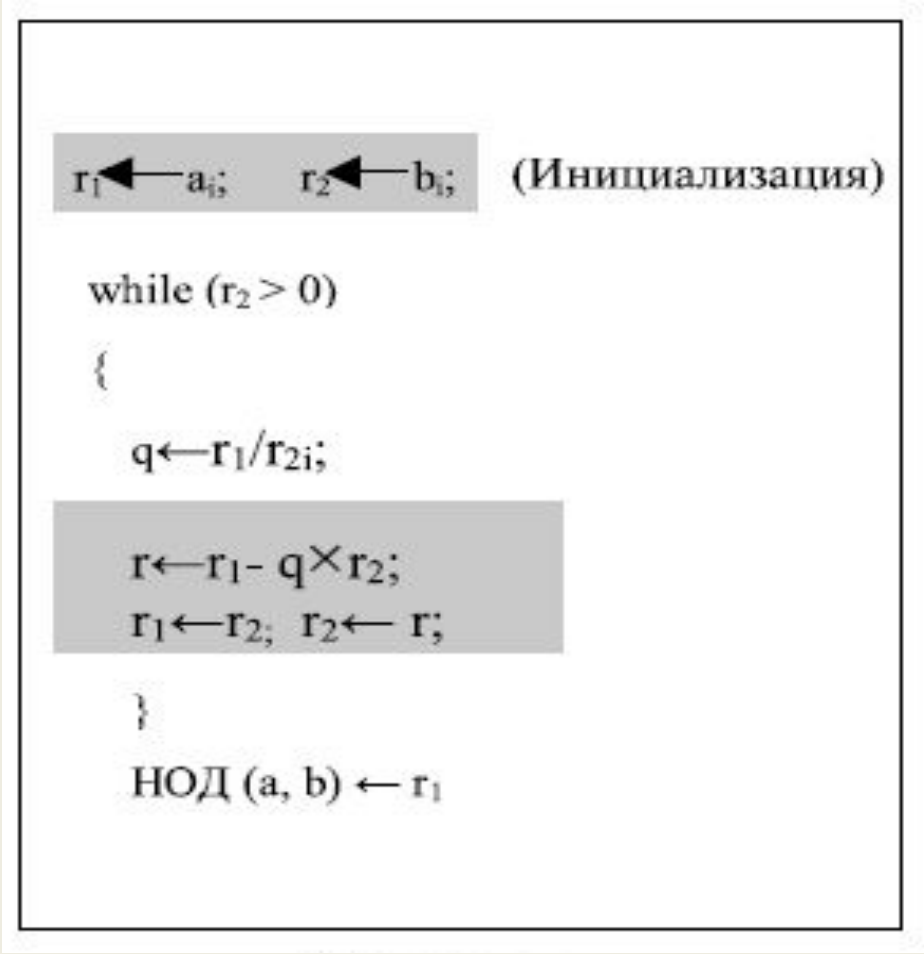
где **r** — остаток от деления **a** на **b**

Например,

НОД(36,10) = НОД(10,6) = НОД(6,4) =

= НОД(4,2) = НОД(2,0) = 2

Алгоритм Евклида на языке псевдокода



Пример применения алгоритма Евклида

Найти наибольший общий делитель чисел 25 и 60.

q	r_1	r_2	r
0	25	60	25
2	60	25	10
2	25	10	5
2	10	5	0
	5	0	

НОД(25,60) = 5

Расширенный алгоритм Евклида

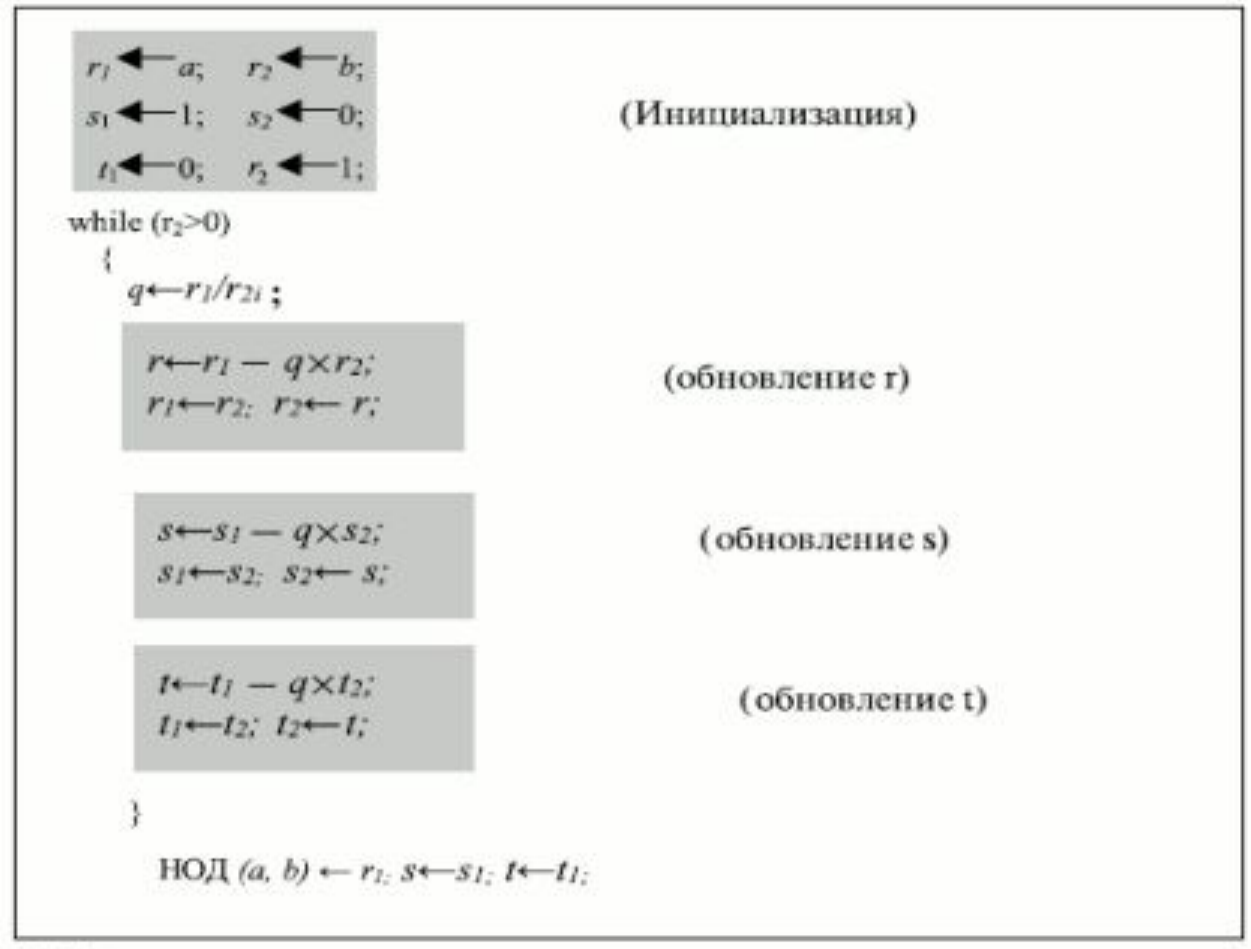
Позволяет найти для целых чисел **a** и **b** такие два целых числа **s** и **t**, что

s x a + t x b = НОД(a,b)

Например,

НОД (161, 28) = (–1) x 161 + 6 x 28 = 7

Расширенный алгоритм Евклида на языке псевдокода



Пример применения расширенного алгоритма Евклида

Дано a = 161 и b = 28, надо найти НОД (a, b), s и t.

$r = r_1 - q \times r_2$ $s = s_1 - qs_2$ $t = t_1 - q \times t_2$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	7	0		-1	4		6	-23	

НОД (161, 28) = (–1) x 161 + 6 x 28 = 7

Линейные диофантовы уравнения

Определение

- *Линейное диофантово уравнение* — это уравнение двух переменных вида:
- **ax + by = c** .
- Мы должны найти целые числа **x** и **y**, которые удовлетворяют этому уравнению.

Утверждение

- Этот тип уравнения либо не имеет решений, либо имеет бесконечное число решений.
- Пусть d = НОД (a, b).
- Если d†c, то уравнение не имеет решения.
- Если d|c, то уравнение имеет бесконечное число решений.
- Одно из них называется *частным*, остальные — *общими*.

Решение линейных диофантовых уравнений

Шаг 1

- Найти s и t в равенстве $a_1 s + b_1 t = 1$, используя расширенный алгоритм Евклида.

Шаг 2

- Частное решение: $x_0 = (c / d) s$ и $y_0 = (c / d) t$.

Шаг 3

- Общие решения: $x = x_0 + k (b / d)$ и $y = y_0 – k (a / d)$, где k

Шаг 4

Пример решения линейных

Найти частные и общие решения уравнения $21x + 14y = 35$.

Мы имеем d = НОД (21, 14) = 7. Так как 7|35, уравнение имеет бесконечное число решений.

Разделив обе стороны уравнения на 7, получим уравнение $3x + 2y = 5$.

Используя расширенный алгоритм Евклида, мы находим s = 1 и t = –1, такие, что 3s + 2t = 1.

Частное решение:

$x_0 = (c / d)\, s = 5 \times 1 = 5$ и $y_0 = (c / d)\, t = 5 \times (-1) = -5$.

Общие: $x = x_0 + k\,(b / d) = 5 + k \times 2$; $y = y_0 - k\,(a / d) = -5 - k \times 3$, где k — целое.

Поэтому решения будут следующие (5, –5), (7, –8), (9, –11),..

Мы хотим обменять денежный чек 100$ на некоторое число банкнот 20$ и несколько банкнот по 5$.

Пример приложения

Имеется много вариантов, которые мы можем найти, решая соответствующее диофантово уравнение $20x + 5y = 100$. Обозначим $d = НОД(20, 5) = 5$. Так как $5|100$, уравнение имеет бесконечное число решений, но приемлемы только несколько из них (неотрицательные целые числа).

Мы делим обе части уравнения на 5, чтобы получить

$4x + y = 20$, и решаем уравнение $4s + t = 1$. Находим $s = 0$ и $t = 1$, используя расширенный алгоритм Эвклида.

Частное решение: $x_0 = 0 \times 20 = 0$ и $y_0 = 1 \times 20 = 20$.

Общие решения с неотрицательными x и y — (0, 20), (1, 16), (2, 12), (3, 8), (4, 4), (5, 0). Первое число в скобках обозначает число банкнот по 20$; второе число обозначает число банкнот по 5$.

Пусть **a = q x n + r.**

Тогда говорят, что **a** равно **r** по модулю **n** и пишут:

a mod n = r

r называют ***вычетом***.

Множество $Z_n = \{0, 1, 2, \ldots, n-1\}$ образует ***систему вычетов по модулю n***

Например,

27 mod 5 = 2; **–18 mod 14 = - 4 + 14= 10**

$Z_6 = \{0, 1, 2, \ldots, 5\}$ - система вычетов по модулю 6

В криптографии часто используется понятие **сравнения** вместо равенства.

Говорят, что числа **a** и **b** *сравнимы по модулю **n***, если

a mod n = b mod n.

Обозначение: **a ≡ b (mod n)**

Например, **27 mod 5 = 2; 7 mod 5 = 2; -3 mod 5 = 2**

Следовательно, **27 = 7 = -3 (mod 5)**

Оператор сравнения по модулю **n** каждому целому числу ставит в соответствие число из Z_n.

Свойства оператора mod

Первое свойство:

- $(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

Второе свойство:

- $(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$

Третье свойство:

- $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

В криптографии мы имеем дело с очень большими целыми числами. Данные свойства позволяют работать с меньшими числами.

Примеры применения свойств оператора mod

(1723345 + 2124945) mod 11 = (8 + 9) mod 11 = 6

(1723345 - 2124945) mod 11 = (8 - 9) mod 11 = 10

(1723345 x 2124945) mod 11 = (8 x 9) mod 11 = 6

Следствие из третьего свойства оператора mod

$10^n \bmod x = (10 \bmod x)^n$

$10 \bmod 3 = 1 \rightarrow 10^n \bmod 3 = (10 \bmod 3)^n = 1$

$10 \bmod 7 = 3 \rightarrow 10^n \bmod 7 = (10 \bmod 7)^n = 3^n \bmod 7$

Применение свойств оператора mod

В арифметике остаток от целого числа, разделенного на 3, такой же, как остаток от деления суммы его десятичных цифр. Мы можем доказать это утверждение, используя свойства модульного оператора.
Запишем целое число как сумму его цифр, умноженных на степени 10.

$$a = a_n 10^n + \ldots\ldots\ldots + a_1 10^1 + a_0 10^0$$

Применим модульную операцию к двум сторонам равенства и используем факт, что остаток $10^n \bmod 3 = 1$.

$$a \bmod 3 = (a_n \times 10^n + \ldots + a_1 \times 10^1 + a_0 \times 10^0) \bmod 3 =$$
$$= (a_n \times 10^n) \bmod 3 + \ldots + (a_1 \times 10^1) \bmod 3 +$$
$$+ (a_0 \times 10^0 \bmod 3) \bmod 3 = (a_n \bmod 3) \times (10^n \bmod 3) + \ldots +$$
$$+ (a_1 \bmod 3) \times (10^1 \bmod 3) + (a_0 \bmod 3) \times (10^0 \bmod 3) \bmod 3 =$$
$$= ((a_n \bmod 3) + \ldots + (a_1 \bmod 3) + (a_0 \bmod 3)) \bmod 3$$

Аддитивная инверсия

Определение	• Говорят, что в Z_n два числа a и b **аддитивно инверсны** друг другу, если их сумма по модулю n равна 0.
Пример	• Аддитивной инверсией числа **4** в Z_{10} является **6**.
Утверждение	• Каждое целое число имеет одну и только одну аддитивную инверсию.
Пары аддитивных инверсий в Z_{10}	• (0, 0), (1, 9), (2, 8), (3, 7), (4, 6) и (5, 5).

Мультипликативная инверсия

Определение

- Говорят, что в Z_n два числа **a** и **b** **мультипликативно инверсны** друг другу, если $a \times b \equiv 1 \pmod{n}$
- Обозначение: $a^{-1} = b$

Пример

- Мультипликативная инверсия числа **3** в Z_{10} равна **7,** так как
- $3 \times 7 \equiv 1 \pmod{10}$, т.е.

$$3^{-1} = 7$$

Существование мультипликативной инверсии

Утверждение

В модульной арифметике не каждое целое число имеет мультипликативной инверсии.

Например

- В Z_{10} числа 0, 2, 4, 5, 6 и 8 не имеют мультипликативной инверсии.
- Пары мультипликативных

Утверждение

- Целое число **a** в Z_n имеет мультиплика-тивную инверсию тогда и только тогда, когда **НОД (n, a) = 1 ,**
- т.е. числа **n** и **a** взаимно

Таблицы сложения и умножения в Z_{10}

	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Таблица сложения в Z_{10}

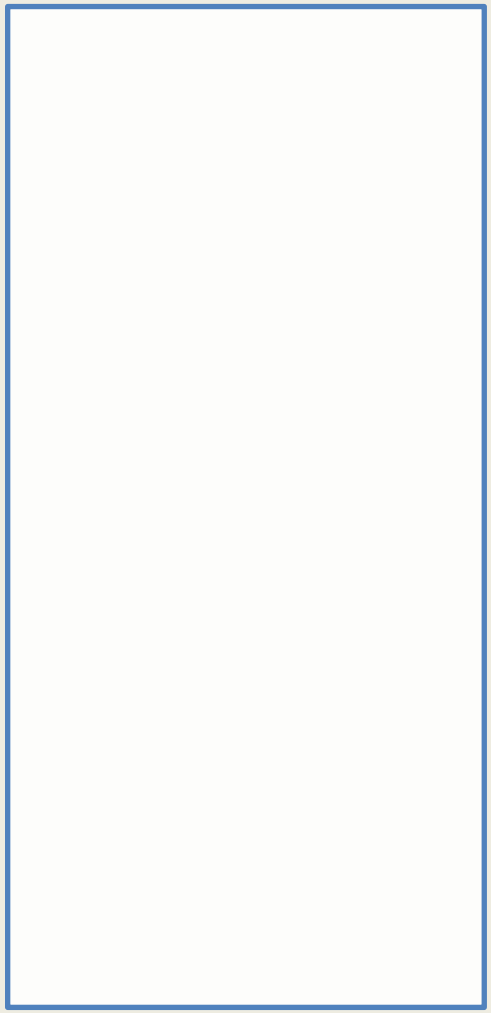
	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Таблица умножения в Z_{10}

зличные множества сложения и умножения

множество Z_n может быть использовано как множество возможных ключей, потому что каждое целое число в этом множестве имеет аддитивную инверсию.

Если алгоритм шифрования / декодирования — **умножение**, Z_n не может быть множеством возможных ключей, потому что только некоторые члены этого множества имеют мультипликативную инверсию. В данном случае ключ выбирают из множества Z_{n*}, которое является



Множества Z_n и Z_{n^*}

Утверждение	• Каждый член Z_n имеет аддитивную инверсию, но только некоторые члены имеют мультипликативную инверсию. • Каждый член Z_{n^*} имеет мультипликативную инверсию, но некоторые
Рекомендации	• Мы должны использовать Z_n, когда необходимы аддитивные инверсии; • мы должны использовать Z_{n^*}, когда необходимы мультипликативные инверсии.

Примеры множеств Z_n и Z_n^*

$Z_6 = \{0,1,2,3,4,5\}$

$Z_7 = \{0,1,2,3,4,5,6\}$

$Z_{10} = \{0,1,2,3,4,5,6,7,8,9\}$

$Z_{6^*} = \{1,5\}$

$Z_{7^*} = \{1,2,3,4,5,6\}$

$Z_{10^*} = \{1,3,7,9\}$

Множества Z_p и Z_{p^*}

Определение

- Z_n, за исключением того, что n — *простое число*.
- $Z_p = \{0, 1, \ldots, p-1\}$.
- Каждый элемент в Z_p имеет аддитивную инверсию;
- каждый элемент в Z_p

Примеры

- Z_{p^*} - очень хороший кандидат, когда мы

- $Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.
- $Z_{11^*} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

Рекомендации

нуждаемся во множестве, которое поддерживает аддитивную и мультиплика

Нахождение

Расширенный алгоритм Евклида может найти мультипликативную инверсию **b** в $\mathbf{Z_n}$, когда инверсия существует, т.е НОД (n, b) = 1.

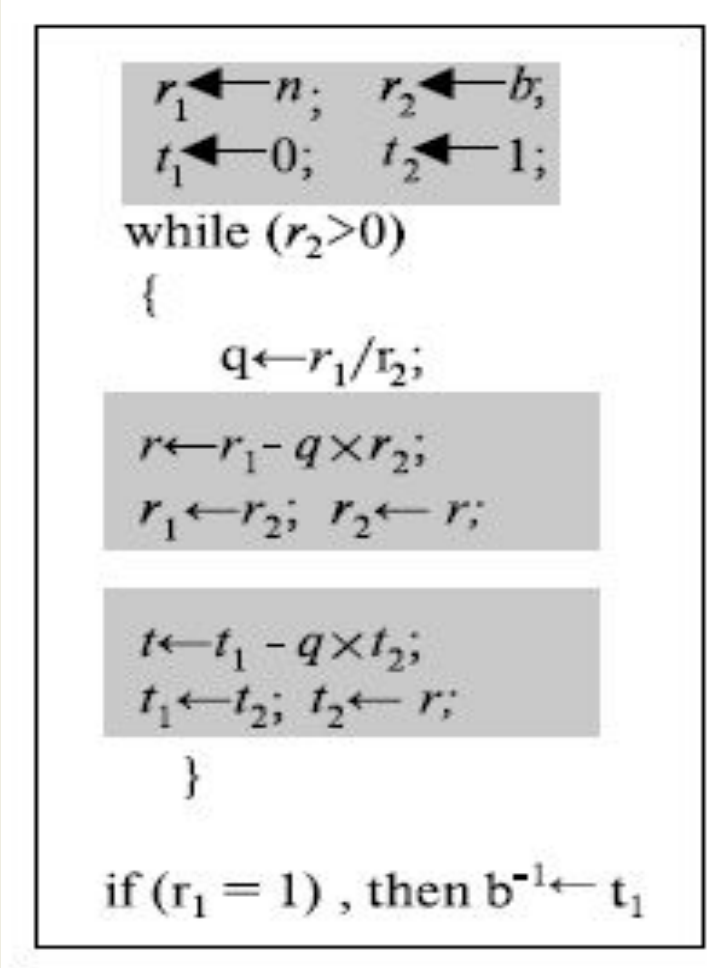
Для этого нам надо решить уравнение

s x n + t x b = НОД (n, b) = 1

Мультипликативная инверсия **b** — это значение **t**, отображенное в $\mathbf{Z_n}$, т.е.

$$b^{-1} = t$$

Расширенный алгоритм Евклида для нахождения мультипликативной инверсии



Пример нахождения мультипликативной инверсии

Найти мультипликативную инверсию числа 11 в Z_{26}.

НОД (11, 26) = 1 $r = r_1 - q \times r_2$ $t = t_1 - q \times t_2$

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
	1	0		-7	26	

$11^{-1} = -7$ (–7) mod 26 = 19 11 x 19 = 209 ≡ 1 (mod 26)

Линейные уравнения с одним неизвестным, содержащие сравнения

Криптография часто использует решение уравнения или множества уравнений с одной или более переменными с коэффициентами в Z_n.

Уравнение вида **$ax \equiv b \pmod n$**

может не иметь ни одного решения или иметь ограниченное число решений.

Предположим, что **НОД (a, n) = d**.

Если **d † b**, решение не существует.

Если **d | b**, то имеется ровно **d** решений.

Решение линейных сравнений с одним неизвестным

$ax \equiv b \pmod n$

Если **d|b**, то используем следующую стратегию:

1. сократить уравнение, разделив обе стороны уравнения (включая модуль) на d;
2. умножить обе стороны сокращенного уравнения на мультипликативную инверсию числа **a**, чтобы найти конкретное решение $\mathbf{x_0}$.
3. общие решения находятся по формуле

$\mathbf{x = x_0 + k\,(n/d)}$, где k = 0, 1..., (d – 1).

Примеры решения линейных сравнений с одним неизвестным

Пример 1.

- Решить уравнение $14x \equiv 12 \pmod{18}$.
- НОД(14, 18) = 2.
- 2 делит 12, значит, имеется 2 решения.
- Сократим обе части уравнения на 2: $7x \equiv 6 \pmod{9}$.

$$7x \equiv 6(\mathrm{mod}\,9) \Rightarrow x \equiv 6 \cdot 7^{-1}(\mathrm{mod}\,9) \Rightarrow x_0 \equiv 6 \cdot 4(\mathrm{mod}\,9) = 6$$

$$x_1 = x_0 + 1 \cdot n/d = 6 + 9 = 15.$$

Пример 2.

- НОД(10,15) = 5.
- 5 не делит 2, значит, решений нет.

Матрицы вычетов

Криптография использует **матрицы вычетов** – матрицы, которые содержат элементы из $Z_n = \{0, 1, \ldots, n-1\}$

Все операции на матрицах вычетов выполняются так же, как и на матрицах целых чисел, за исключением того, что операции производятся в модульной арифметике.

Сравнение матриц

Две матрицы называются **сравнимыми по модулю n**, если они имеют одинаковое число строк и столбцов, и все соответствующие элементы — сравнимы по модулю n, т.е.

A ≡ B (mod n), если $a_{ij} \equiv b_{ij} \pmod{n}$ для всех i и j.

$$\begin{pmatrix} 5 & 2 \\ 3 & 14 \end{pmatrix} \equiv \begin{pmatrix} 15 & 22 \\ 13 & 4 \end{pmatrix} (\mathrm{mod}\, 10)$$

Операции над матрицами вычетов

Сложение и вычитание можно делать только для матриц равного размера.

Мы можем **умножить** друг на друга две матрицы различных размеров, если число столбцов первой матрицы совпадает с числом строк второй матрицы.

Матрица вычета имеет **инверсию**, если детерминант матрицы имеет инверсию.

Примеры операций над матрицами вычетов

$$\begin{pmatrix} 8 & 2 & 9 \\ 6 & 5 & 7 \end{pmatrix} + \begin{pmatrix} 5 & 7 & 3 \\ 4 & 6 & 8 \end{pmatrix} \equiv \begin{pmatrix} 3 & 9 & 2 \\ 0 & 1 & 5 \end{pmatrix} (\mathrm{mod}\, 10)$$

A - матрица вычетов в Z_{26} . det (A) = 21 имеет мультипликативную инверсию 5 в Z_{26}, поэтому существует A^{-1} - мультипликативная инверсия матрицы A.

Когда умножают эти две матрицы, то результат — единичная матрица в Z_{26}:

$$A = \begin{pmatrix} 3 & 5 & 7 & 2 \\ 1 & 4 & 7 & 2 \\ 6 & 3 & 9 & 17 \\ 13 & 5 & 4 & 16 \end{pmatrix} \quad A^{-1} = \begin{pmatrix} 15 & 21 & 0 & 15 \\ 23 & 9 & 0 & 22 \\ 15 & 16 & 18 & 3 \\ 24 & 7 & 15 & 3 \end{pmatrix} \quad A \cdot A^{-1} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} (\mathrm{mod}\, 26)$$

$$3 \cdot 15 + 5 \cdot 23 + 7 \cdot 15 + 2 \cdot 24 = 313 \equiv 1 (\mathrm{mod}\, 26)$$

Системы линейных уравнений, содержащих сравнения

Мы можем решить систему линейных уравнений с одним и тем же модулем, если матрица, сформированная из коэффициентов системы уравнений, имеет инверсию (обратную матрицу).

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2 \\ \cdots\quad \cdots\quad \cdots &\quad \cdots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n &= b_n \end{aligned}$$

а) Система уравнений

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \equiv \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \qquad \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \equiv \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}^{-1} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

б) интерпретация системы уравнений в) решение

Обзорные вопросы по лекции 1

1. Покажите различие между Z и Z_n. Какое из этих множеств может содержать отрицательные целые числа? Как мы можем отобразить целое число из Z в целое число из Z_n?
2. Приведите пример целого числа с единственным делителем. Приведите пример целого числа только с двумя делителями. Приведите пример целого числа с более чем двумя делителями.
3. Определите наибольший общий делитель двух целых чисел. Какой алгоритм может эффективно найти наибольший общий делитель?
4. Что такое линейное диофантово уравнение двух переменных? Сколько решений может иметь такое уравнение? Как может быть найдено решение(я)?
5. Что такое оператор по модулю? Перечислите все свойства, которые мы упоминали в этой лекции для операций по модулю.
6. Определите сравнение и перечислите его свойства .

Обзорные вопросы по лекции 1

7. Определите систему вычетов.
8. Какова разница между множеством Z_n и множеством Z_{n*}? В каком множестве каждый элемент имеет аддитивную инверсию? В каком множестве каждый элемент имеет мультипликативную инверсию? Какой алгоритм используется, чтобы найти мультипликативную инверсию целого числа в Z_n?
9. Какой алгоритм может использоваться, чтобы решить линейное сравнение?
10. Когда матрица вычета имеет инверсию?
11. При каком условии можно решить систему линейных уравнений с одним и тем же модулем?