Лекция 1

КРИПТОГРАФИЯ

Способы защиты информации

1. Физическая защита НЕРЕАЛЬНО

   Создать абсолютно надежный, недоступный для других канал связи между абонентами.

2. Стеганографическая защита

   Этот способ защиты основан на попытке скрыть от противника сам факт наличия интересующей его информации.

3. Криптографическая защита

   Криптография в переводе с греческого означает “тайнопись”.

   Этот метод защиты информации предполагает преобразование информации для сокрытия ее смысла от противника.

Стеганография

1. Текст, видимый только при определенных условиях
   Симпатические чернила

2. Физическое сокрытие информации:
   В корешках книг
   Под маркой конверта с письмом
   Древне римский вариант: на голове раба

3. Информационное сокрытие информации
   В файле с изображением

Цели криптографии

1. Конфиденциальность
   Шифрование данных с целью защиты от несанкционированного доступа.
2. Целостность
   Получатель может проверить, не было ли сообщение изменено или подменено в процессе пересылки;
3. Подлинность
   Получатель сообщения может проверить его источник.
4. Невозможность отказа от авторства
   Невозможность как для получателя, так и для отправителя отказаться от факта передачи.
5. Доступность информации

Основные определения

* **Шифр** (cipher) – совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты.

* Исходные сообщения обычно называют **открытыми текстами (plaintext)**.

* **Алфавит** - конечное множество используемых для кодирования информации символов.

* Сообщение, полученное после преобразования с использованием любого шифра, называется **шифрованным сообщением (ciphertext).**

* Ш**ифрование (зашифрование)** — преобразование открытого текста в зашифрованный текст

* **Расшифрование —** действие обратное зашифрованию с использованием ключа шифрования

* **Дешифрование —** действие обратное зашифрованию без использования ключа шифрования

* **Ключ** – информация, необходимая для зашифрования и расшифрования сообщений.

* **Система шифрования**, или **шифрсистема**, – это любая система, которую можно использовать для обратимого изменения текста сообщения с целью сделать его непонятным для всех, кроме тех, кому оно предназначено.

Криптоанализ

– условно выделяемая часть криптографии (криптологии), предоставляющая противнику подходы, средства и методы для взлома криптографических средств защиты информации.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. способность противостоять криптоанализу).

Криптология

Иногда криптографию и криптоанализ объединяют в одну науку, ***криптологию***, занимающуюся вопросами обратимого преобразования информации с целью защиты от несанкционированного доступа, оценкой надежности систем шифрования и анализом стойкости шифров.

Требования к шифрсистемам

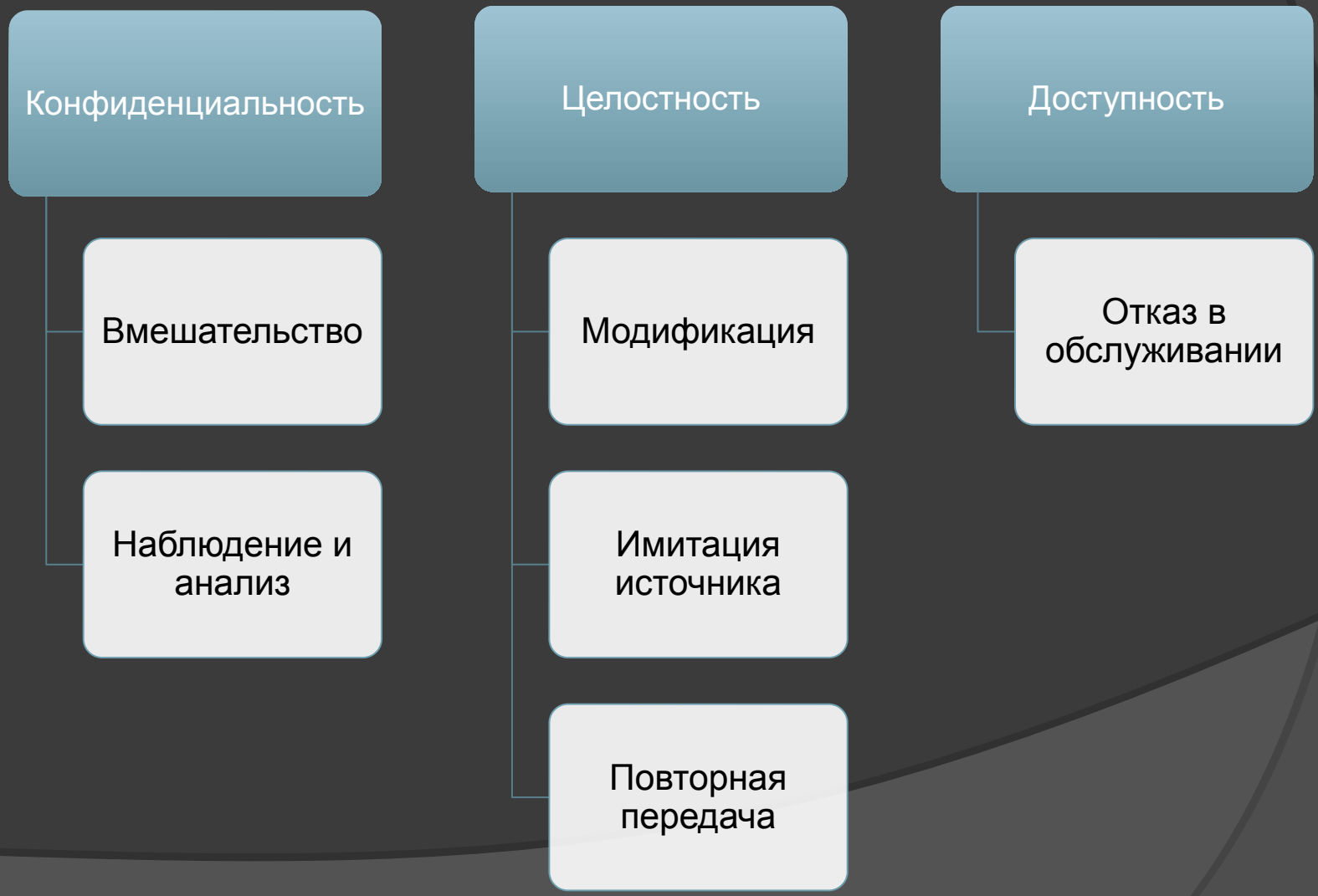
1. Зашифрованное сообщение должно поддаваться чтению только при наличии ключа.

2. Знание алгоритма шифрования не должно влиять на надежность защиты. (принцип Керкгоффса)

3. Любой ключ из множества возможных должен обеспечивать надежную защиту информации.

4. Алгоритм шифрования должен допускать как программную, так и аппаратную реализацию.

Атаки на шифрсистемы



Атаки на шифрсистемы

Атаки	Пассивные/Активные	Угроза
Вмешательство	Пассивные	Конфиденциальности
Наблюдение и анализ		
Модификация	Активные	Целостности
Имитация источника		
Повторная передача		
Отказ в обслуживании		Доступности

Арифметика целых чисел

Множество целых чисел - Z = { … -2 -1 0 1 2 …}

Бинарные операции имеют два входа и один выход. Для целых чисел определены три общих бинарных операции — сложение, вычитание и умножение.

Деление целых чисел имеет 2 входа и ДВА выхода: **a = q*n + r**

Если a не равно нулю, а r = 0, тогда мы можем записать вышеупомянутые отношения как n|a, иначе как n†a.

Наибольший общий делитель (НОД) — наибольшее целое число, которое делит оба целых числа.

Линейное диофантово уравнение — это уравнение двух переменных: a*x + b*y = c .

Линейные диофантовы уравнения

Пусть $d = НОД (a, b)$. Если $d \dagger c$, то уравнение не имеет решения.

Если же $d|c$, то мы имеем бесконечное число решений. Одно из них называется частным, остальные — общими.

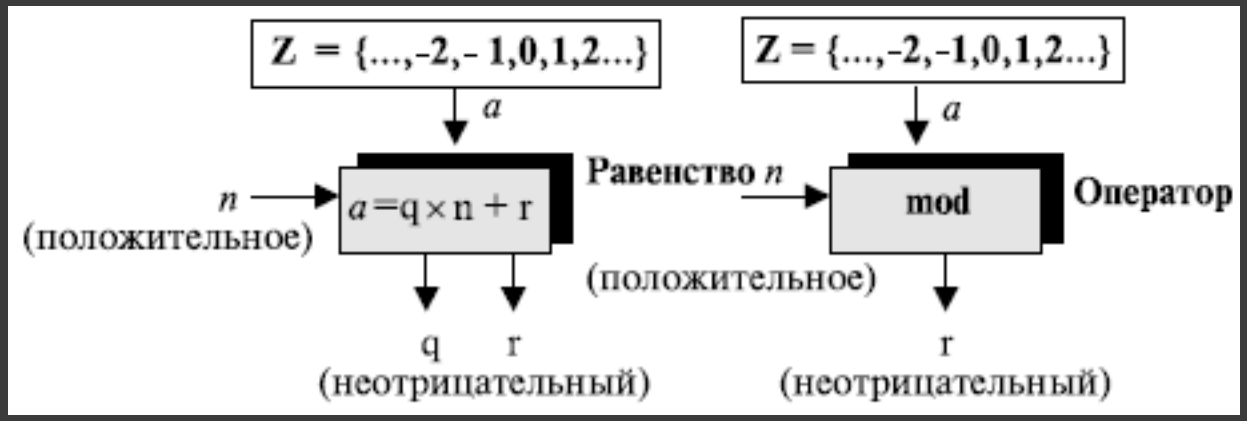
Можно найти частное решение, используя следующие шаги:

1. Преобразуем уравнение к $a_1x + b_1y = c_1$, разделив обе части уравнения на d.
2. Найти s и t в равенстве $a_1s + b_1t = 1$, используя расширенный алгоритм Евклида.
3. Частное решение может быть найдено: $X_0 = (c/d)s$ и $y_0 = (c/d)t$

После нахождения частного решения общие решения могут быть найдены следующим образом: $x = x_0 + k(b/d)$ и $y = y_0 – k(a/d)$, где k — целое число

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

Модульная арифметика



Мы можем представить изображение уравнения деления (a = q*n + r) как бинарный оператор с двумя входами a и n и одним выходом r. Этот бинарный оператор назван **оператором по модулю** и обозначается как mod. Второй вход (n) назван **модулем**. Вывод r назван **вычетом**. Мы можем записать это так: a mod n = r

Система вычетов: Zn

Результат операции по модулю n — всегда целое число между 0 и n – 1.Другими словами, результат a mod n — всегда неотрицательное целое число, меньшее, чем n.

Мы можем сказать, что операция по модулю создает набор, который в модульной арифметике можно понимать как **системувычетов по модулю n**, или Z_n.

Однако мы должны помнить, что хотя существует только одно множество целых чисел (Z), мы имеем бесконечное число множеств вычетов (Z_n), но лишь одно для каждого значения n.

ПРИМЕР: Z_2 = { 0, 1 }
ПРИМЕР: Z_6 = { 0, 1, 2, 3, 4, 5 }
ПРИМЕР: Z_{11} = { 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 }

Сравнения

В криптографии мы часто используем понятие **сравнения** вместо равенства. Отображение Z в Z_n не отображаются "один в один". Бесконечные элементы множества Z могут быть отображены одним элементом Z_n.

Например, результат 2 mod 10 = 2, 12 mod 10 = 2, 22 mod 10 = 2, и так далее. В модульной арифметике целые числа, подобные 2, 12, и 22, называются сравнимыми по модулю 10 (mod 10).

Для того чтобы указать, что два целых числа сравнимы, мы используем **оператор сравнения** (≅). Мы добавляем mod n к правой стороне сравнения, чтобы определить значение модуля и сделать равенство правильным.

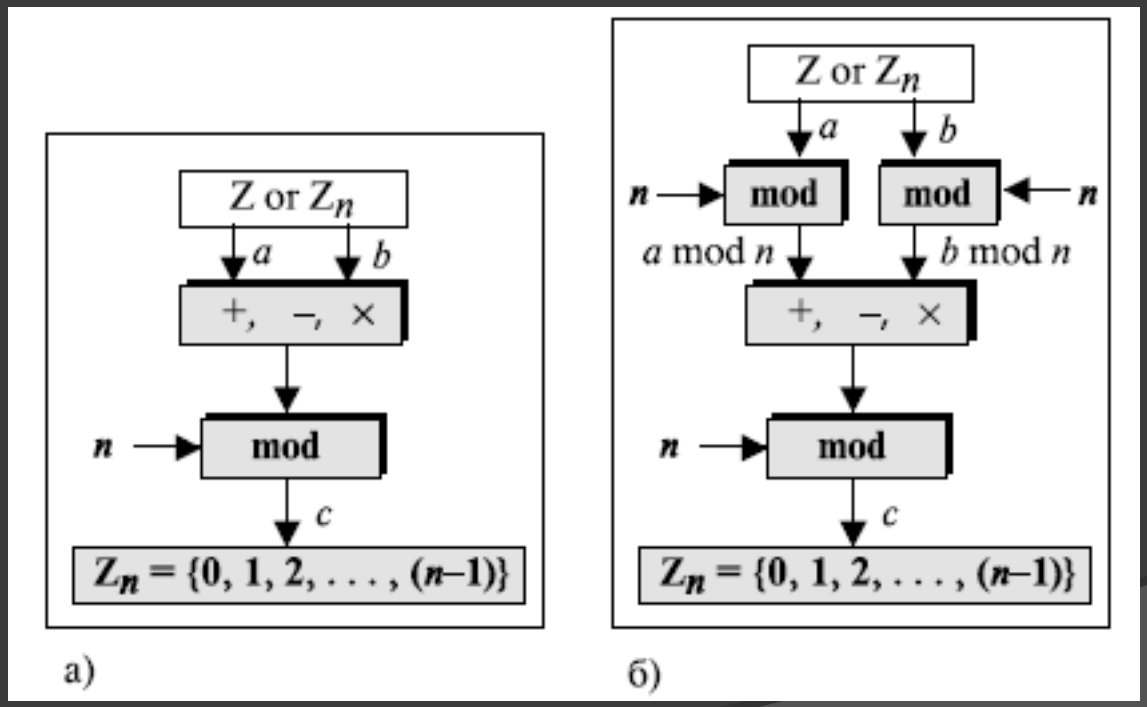
$$2 \equiv 12 (mod\ 10) \quad 13 \equiv 23 (mod\ 10) \quad 34 \equiv 24 (mod\ 10) \quad -8 \equiv 12 (mod\ 10)$$
$$3 \equiv 8 (mod\ 5) \quad 8 \equiv 13 (mod\ 5) \quad 23 \equiv 33 (mod\ 5) \quad -8 \equiv 2 (mod\ 5)$$

Свойства оператора mod

Первое свойство: (a + b) mod n = [(a mod n) + (b mod n)] mod n

Второе свойство: (a – b) mod n = [(a mod n) - (b mod n)] mod n

Третье свойство: (a x b) mod n = [(a mod n) x (b mod n)] mod n



Инверсии

Когда мы работаем в модульной арифметике, нам часто нужно найти операцию, которая позволяет вычислить величину, обратную заданному числу.

Мы обычно ищем **аддитивную инверсию** (оператор, обратный сложению) или **мультипликативную инверсию** (оператор, обратный умножению).

В модульной арифметике каждое целое число имеет аддитивную инверсию. Сумма целого числа и его аддитивной инверсии сравнима с 0 по модулю n .

В модульной арифметике целое число может или не может иметь мультипликативную инверсию. Целое число и его мультипликативная инверсия сравнимы с 1 по модулю n.

Нужно доказать, что целое число a имеет мультипликативную инверсию в Z_n, тогда и только тогда, когда НОД(n, a) = 1.