$$a \equiv bmodm \iff \begin{matrix} a = km + r, \\ b = tk + r \end{matrix} \iff a - b : m$$

Сравнение.

0.0.1 Свойства сравнения

Рассмотрим свойства сравнения:

$$a \equiv bmodm \tag{1}$$
$$c \equiv dmodm \tag{2}$$

$a + c \equiv b + dmodm$

$ka \equiv kbmodm$ - обе части можно умножить на некоторое число.

Почленное перемножение

$$a \equiv bmodm \tag{3}$$
$$c \equiv dmodm \tag{4}$$

-> $ac \equiv bdmodm$

Доказательство

$$ac = (km + r)(cm + r_1) = ()m + rr_1 \tag{5}$$
$$bd = (tm + r)(hm + r_1) = ()m + rr_1 \tag{6}$$

Из этого можно получить, что:

$$a^k \equiv b^k mod m, \qquad k \in N_0 \tag{7}$$

Такие свойства достаточно упрощают всякие штуки, например:

$$\sum_i A_i b^i mod m = \sum_i (A_i mod m)(b mod m)^i; \tag{8}$$

Пример:

$$17^{17} mod 13 \equiv 4^{17} = (4^2)^8 \cdot 4 \equiv 3^8 \dot{4} \equiv (3^3)^2 \cdot 9 \cdot 4 \equiv 36 \equiv 10 mod 13 \tag{9}$$

Еще пример:

$$d|mLa \equiv b mod m => \tag{10}$$

Пусть числа m, n взаимнопростые, т.е. $(m, n) = 1$ и $a \equiv b mod m$ и $a \equiv b mod n => a \equiv b mod mn$

(Тут рисуночек) $_0 = [0] = \{0, +-m, +-2m...\}$ $C_1 = [1] = \{1, +-m+1, +-2m+1\}$ ... $C_{m-1} = [m-1] = \{m-1, +-m+(m-1), +-2m$ - это полная система вычетов по модулю m. Причем, классы можно складывать умножать и все такое. Для примера: $C_i + C_j = C_{i+j}$ например : $(7+12) mod 5 = 19 mod 5 = 4$ $2 + (-3) = (-1 mod 5) = 4$

И умножать: $c_i \cdot c_j = c_{ij}$

Обратные по умножению: $a^{-1} : a^{-1} \cdot a = 1 mod m$ $Z_m = \{[0], [1], ..., [m-1]\} = \{0, 1, ..., m-1\}$

$Z_5 = \{0, 1, 2, 3, 4\}$ $1^{-1} = 1$ $2^{-1} = 3$ $3^{-1} = 2$ $4^{-1} = 4$

$Z_6 = 0, 1, 2, 3, 4, 5$ $1^-1 = 1$ $2^-1 = null$ $3^-1 = null$ $4^-1 = null$ $5^-1 = 5$

$\exists a^{-1} mod m \Leftrightarrow (a, m) = 1$ -взаимнопростые;

Алгоритм для нахождения обратного по модулю - расширенный алгоритм Эвклида. $(a, m) = 1, \qquad m > a\ m = q_1 a + r_1\ a = q_2 r_1 + r_2$ $r1 = q_3 r_2 + r_3$ ... $r_{n-3} = q_n r_{n-2} + r_{n-1}\ r_{n-2} = a_{n-2} + r_n\ r_{n-1}$ - нод $r_n = 0$

$1 = um + va$ Возьмем по модулю $m : 1 \equiv vamodm$ -> v будет обратным к a Пример: $23^{-1}mod135$ $135 = 5 \cdot 23 + 20$ $23 = 1 \cdot 20 + 3$ $20 = 6 \cdot 3 + 2$ $3 = 1 \cdot 2 + 1$ 1 -> нод 23 и 135. $1 = 3 - 1 * 2 = 3-1*(20-6*3) = -20+7*3 = -20+7*(23-20) = 7*23-8*20 = 7 * 23 - 8(135 - 5 * 23) = -8 * 135 + 47 * 23$

$$\begin{array}{cccccc} & & q_1 & q_2 & \dots & q_n \\ 0 & 1 & p_1 & p_2 & & p_n \end{array} \tag{11}$$

$p_i = q_i p_{i-1} + p_{i-2}$

$a^{-1}modm = (-1)^m p_n$

Пример:

$$\begin{array}{cccccc} & & 5 & 1 & 6 & 1 \\ 0 & 1 & 5 & 6 & 41 & 47 \end{array} \tag{12}$$

Домашнее задание:

0.1 Основные направления, аспекты защиты информаци

0.1.1 Цели, задачи ЗИ

1. Конфидициальность
2. Целостность
3. Аутентичность - подтверждение подлинности сообщения (подвид целостности)
4. Доступность
5. Наблюдаемость - отслеживание доступа
6. Юридическая значимость

0.1.2 Направления и методы ЗИ

1. Правовые
2. Нормативно-методические
3. Организационные
4. Непосредственные (физические)
5. Технические - защита от утечки через каналы информации
    - электромагнитная
    - аккустический

- виброаккустический
- оптический
- криптографические
- стеганографический (стегано - крыша) - скрывается сам файт передачи сообщения
- методы квантовой криптографии (1983)
- морально-психологические

0.1.3 Основные понятия криптологии

Криптология делится на криптографию и криптоанализ
Открытый текст - сообщение, подлежащее шифрованию.

$$X = x_1, ...x_n M = m_1 m_2 ... m_n x_i, m_j \in Z_r \tag{13}$$

Z_r - алфавит из r букв

$$Z_r = \{0, 1, ..., r-1\} \tag{14}$$

Шифрованный текст (криптограмма) (ШТ) - ;

Зашифрование - процедура ОТ->ШТ с использованием открытых или секретных ключей Расшифрование - процедура ШТ->ОТ законным пользователем с использованием секретных ключей Секретный ключ - параметр, управляющий процессом шифрования.

$$K = k_1 k_2 ... k_s, \qquad k_i \in Z_q \tag{15}$$

- пространство ключей. $||$ - мощность

0.1.4 Классификация криптографии

1. Классическая криптография (до начала 20 века) - шифры перестановки и шифры перестановки
2. Механические шифровальные машины (конец 19-го - начало 20-го века)
3. Электромеханические (пример. Энигма)
4. Современные криптосистемы (вторая половина 20го века) - аппаратные, программные и аппаратно-программные
   (а) Симметричные (с закрытым ключем) - блочные, потоковые;
   (б) Ассиметричные (с открытым ключем) - с 1976 года;
   (в) Квантовые - с 1983 года.

Савчук Михаил Николаевич

0.1.5 Литература

...