

Числосе 2 алгоритма A и B

1) Выбор m, q и переговор

$$A \xrightarrow{m, q} B$$

2) Выбирается gear. большее число α и gear. x .

$$x \equiv q^\alpha \pmod{m} \text{ и } x \text{ передается } B$$

$$\xrightarrow{x}$$

3) Адемент B gear.

$$y \equiv q^\beta \pmod{m} \text{ gear. } y \text{ и передается}$$

$$\xrightarrow{y}$$

Четвертая четв. (m, q, x, y) - открытый квест.

4) Каждый из них формирует секретный квест

$$A: k_1 = y^\alpha \pmod{m} \quad B: k_2 = x^\beta \pmod{m} \\ \equiv q^{\alpha\beta} \pmod{m} \quad = q^{\alpha\beta} \pmod{m}$$

$k = k_1 = k_2$ - секретный квест.

Zagara 3. $m = 67, q = 11$

$$\alpha = 47, \beta = 51$$

$k - ?$

Задача открытой лекции. Выявление циклических

18.09

$$(M, q, x, y) = (4397, 2381, 2567, 4709)$$

k?

for alpha in (2, 10000):

$$t = q**alpha$$

$$t \bmod m = (t \% m)$$

print(alpha)

break

Замечание Криптостойкость системы, если на
автоматическую диаграмму - Киммского сужения
и блоков из таблицы направлена вниз

$$g \in \mathbb{Z}_p^*$$

$$\langle g \rangle = \mathbb{Z}_p \setminus \{0\} \quad g \text{- генератор группы } \mathbb{Z}_p^*$$

$$\gamma, \gamma^2 = \delta_1, \gamma^3 = \delta_2, \gamma^4 = \delta_3, \dots$$

$$F(\gamma) = 2 \Rightarrow \text{нельзя расшифровать}$$

$$\gamma^t = e, \gamma^t \cdot \gamma^{-1} = \gamma^{t-1} = e$$

$$\mathbb{Z}_p \rightsquigarrow \mathbb{Z}_{31}$$

$$\mathbb{Z}_p \setminus \{0\} = A \cup B$$

$$y = \gamma^i, i = 1, \dots, p-1$$

$$A = \{i : \gcd(i, p-1) = 1\}$$

$$B = \{i : \gcd(i, p-1) > 1\}$$

$$q^1, q^2, q^3, \dots, q^{p-1}$$

\downarrow 1, 2, 3, ..., $(p-1)$ - neu. Folget
 1 2, ..., $p-1$

$$y = q^i, i = 1, \dots, p-1$$

$$p-1 = km_1,$$

$$j = k m_2$$

$$(q^j)^{m_1} = (q^{km_1})^{m_2} = (q^{p-1})^{m_2} = e$$

$$q^{j_1}, q^{j_2}, q^{j_3}, \dots, q^{j_{m_2}} = e$$

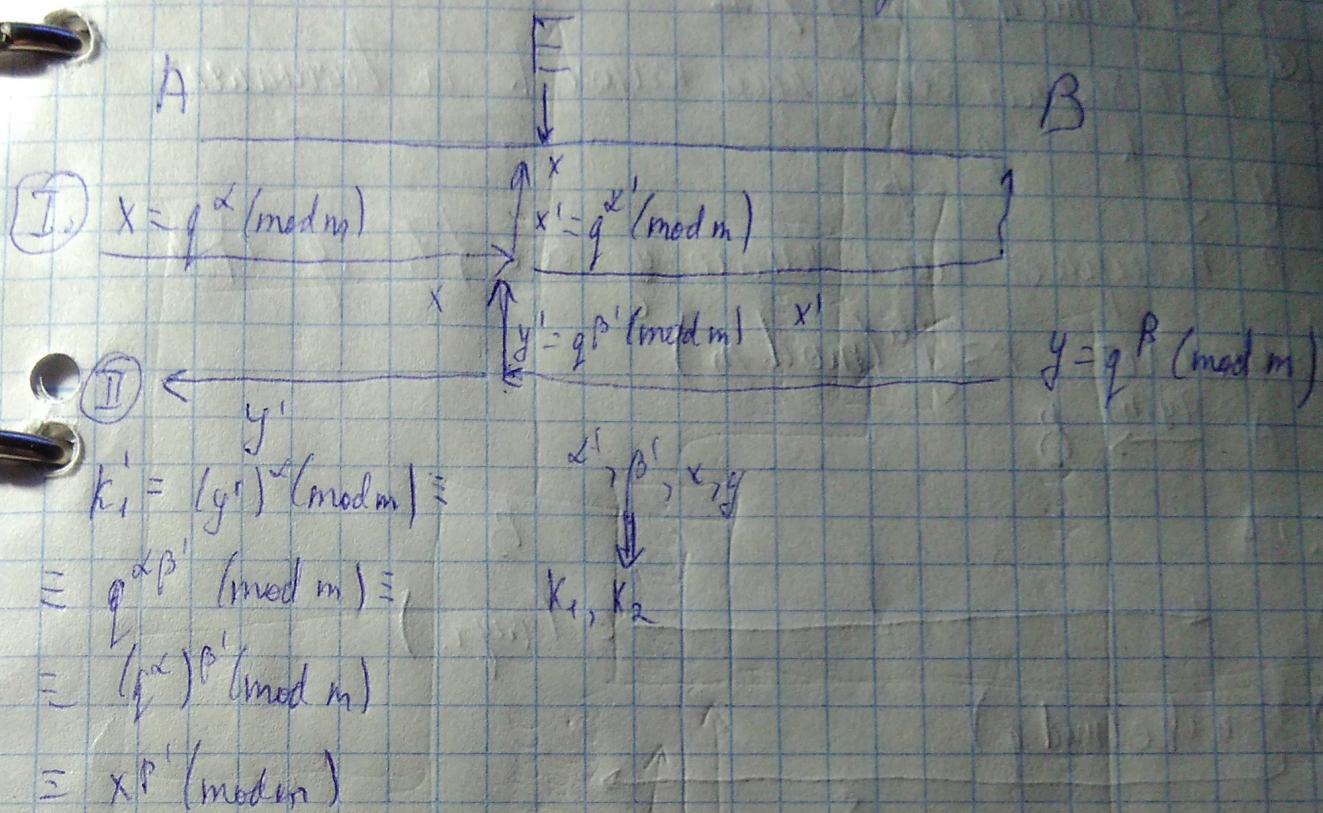
Planeieren wir, dass alle. mit k -potenzen

Multiplizieren $\delta \mathcal{Z}_p$

- 1) 19. April, $\delta \mathcal{Z}_{31}$
- 2) 17. April, $\delta \mathcal{Z}_{31}$
- 3) Nach. neg. Kriterium

Пример работы на алгоритме
Диффи-Хелмана: члены погрешности

12.10



Продолжение начатое с помощью сертификации
ключей (алгоритмы цифровой подписи)

Протокол

Протокол аутентификации

на основе скрытых ключей

Цель протоколов - проверка подлинности информации

A

B (проверяет A)

- Выбор параметров протокола (один раз предполагается заблаговременно) выбираем $p, q : (p-1)/2$

Выбирается $g \in \mathbb{Z}_p$

$$g^q \equiv 1 \pmod{p}, g \neq 1$$

2) А выбирает секретный ключ k и берет

$$y = g^{-k} \in \mathbb{Z}_p$$

А выбирает агр. рандом $a \in \{1, \dots, q-1\}$

берет $r = g^a \pmod{m}$

$$A \xrightarrow{(y, r)} B$$

II. A

B

1) $\xleftarrow{\quad} e \text{ (агр.)}$

2) $s = a + ke \pmod{q}$

s

3)

$$r \equiv g^s y^e \pmod{p}$$

b приглашает B не присыпать r \downarrow
гдк. A.

Задача 1 Основная $r = g^s y^e$

$$g^{s+ke} y^e = g^{(a+k)e} y^e = g^a (g^e)^k y^e = g^a g^{ke} y^e$$

(i) $s \equiv a + ke \pmod{q}$

$$s \equiv a + ke + lq$$

$$g^s = g^{a+ke+lq} = g^a g^{ke} (g^q)^l = r g^{ke} \in \mathbb{Z}_p$$

(ii) $y = g^{-k}$

$$g^k y = 1$$

$$(iii) g^{s \cdot e} \stackrel{?}{=} r g^{k \cdot e} = r(g^k y)^e \stackrel{?}{=} r$$

Zadacha 2 Глобальное программу. Я - Боб. Обмениваю с Алисой
Переводит цифр. e , она $\rightarrow s$. Программа, которая
из s всех параллельных независимых определений, Алиса ищет

$$p = 33107 \quad 1) \quad e = 15776$$

$$g = 165535 \quad s = 9856$$

$$g = 2902 \quad 2) \quad e = 490 \quad s = 8108$$

$$y = 9107 \quad 3) \quad e = 9987$$

$$r = 32607 \quad s = 7309$$

$$4) \quad e = 155 \quad s = 1267$$

Найден циф. r_{Bob} к. (Prop.)

RSA

16.10

Rivest, Shamir, Adleman

I	A	B
	—————	
p_1, p_2		q_1, q_2
$r_A = p_1 p_2$		$r_B = q_1 q_2$
$\varphi(r_A) = r_A \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) =$		$\varphi(r_B) = r_B \left(1 - \frac{1}{q_1}\right) \left(1 - \frac{1}{q_2}\right) =$
$= (p_1 - 1)(p_2 - 1)$		$= (q_1 - 1)(q_2 - 1)$

II $1 < \alpha < \varphi(r_A)$
 $\gcd(\alpha, \varphi(r_A)) = 1$

III $A \{ r_A, \alpha \}$

$$\alpha \cdot x \equiv 1 \pmod{\varphi(r_A)}$$

откуда x

также known

B $\boxed{r_B, b}$

$$b \cdot \beta \equiv 1 \pmod{\varphi(r_B)}$$

откуда β

Как это работает:

A зам. б та же known B и бер. $m_1 = m^b \pmod{r_B}$

и проверяет известное B

$$m_2 \equiv m_1^b \pmod{r_B}$$

$$m_2 = m$$

Задача 1. Имеем $m_2 = m$?

$$1. m_2 = m_1^b \equiv (m^b)^{\beta} \equiv m^{b\beta} \quad b \geq r_B$$

$$2. b\beta \equiv 1 \pmod{\varphi(r_B)}$$

$$b\beta \equiv 1 + \tilde{l} \varphi(r_B), \quad \tilde{l} \in \mathbb{Z}$$

$$3. m^{b\beta} \equiv m^{1+\tilde{l}\varphi(r_B)} = m \left(m^{\varphi(r_B)} \right)^{\tilde{l}} = m \quad b \geq r_B$$

т.к. $\gcd(m, r_B) = 1$

Задача 2.

A

$$m_1 = 25963634$$

$m - ?$

B

$$r_B = 71361259$$

$$b = 74674$$

$$\beta = 33289211$$

$\frac{\beta-1}{10} = k$, $\beta = 10k+1$, удаляем степень

$$m_1^k \pmod{r_B} \quad C^{10} \cdot m_1 \pmod{r_B}$$

my-files.ru/um2x63

Задача 3 // опубликован открытое кольцо

$$r_A = 66899179$$

$$\alpha = 9467$$

Взяться за λ .

$$1/dq \text{ gg } L_p$$

Примеры шагов на алгоритме RSA

30.10

Чтобы бессмысленного цикла.

$$r_A \quad . \quad \alpha \quad c$$

Криптосистема зашифровывается с открытого
открытое кольцо α . Еще несколько раз, пока не будет
не получать шифротекст c

$$c, c_1, c_2, \dots, c_n = c.$$

Число k фиксируется

$$(c^a)^k \equiv c \pmod{r_A}$$

$$\gcd(c, r_A) = 1$$

$$C^{\varphi(r_A)} \equiv 1 \pmod{N_A} \text{ ибо } Th \text{ зиера}$$

$$C^{\varphi(r_A)+1} \equiv C \pmod{N_A}$$

$$\alpha k = \varphi(r_A) + 1 - ?$$

$$C^k = (m^\alpha)^k = m^{\alpha k} = m^{\varphi(r_A)+1} = m$$

$\beta \in \mathbb{Z}_{r_A}$

Задача 1 Найти m, k

$$r_A = 212887, \alpha = 8061, C = 35947$$

$$131406$$

Атака на базе общего модуля
Генератора свидетельств о геометрическом
уравнении.

$$P: \underbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}_{k \text{ раз}} \rightarrow \mathbb{Z}$$

$P(x_1, x_2, \dots, x_k) = 0$ наз. геометрическим

$$ax + by = c \quad \text{отн. } x, y. \quad (*)$$

a, b, c — целые

$$\gcd(a, b) = 1.$$

Упс Имеется пары (x_0, y_0) — решения ур-я (*). Тогда
общее решение ур-я (*) можно записать в виде

$$(x, y) = (x_0 + bk, y_0 - ak), \quad k \in \mathbb{Z}$$

Dek

$$ax_0 + by_0 = c$$

Возможна спосіб. розв'язк. (x, y)

$$ax + by = c$$

$$ax - ax_0 + by - by_0 = 0$$

$$a(x - x_0) + b(y - y_0) = 0 \Rightarrow a(x - x_0) = -b(y - y_0) =$$

$$\Rightarrow a(x - x_0) : b = (x - x_0) : b \Rightarrow$$

$$\Rightarrow x = x_0 + kb$$

$$akb = -b(y - y_0)$$

$$ak = y - y_0 \Rightarrow y = y_0 - ak$$

T.B. 2] 1) (x_0, y_0) - розв'язк.

тоді $ax \equiv c \pmod{b}$ (!)

2) Йдеть x_0 - розв. (!), тоді $\exists y_0$ така, що

(x_0, y_0) - розв'язк (!).

~~Доведіть~~

$$\gcd(a, b) = 1$$

$$a^{\varphi(b)-1} \equiv 1 \pmod{b} \quad |+c$$

$$c \cdot a^{\varphi(b)} \equiv c \pmod{b}$$

$$\text{or } \underbrace{(c a^{\varphi(b)-1})}_x \equiv c \pmod{b}$$

$$\boxed{1999b} g_x + 273y = 6$$

$$23x + 91y = 2$$

$$23x \equiv 2 \pmod{91} \Rightarrow$$

$$23x \equiv 184 \pmod{91}$$

$$x \equiv 3 \pmod{91}$$

$$x = 3,$$

$$y = -2.$$

$$(x, y) = (8 + 91k, -2 - 23k), k \in \mathbb{Z}$$

A,

B,

C

r_A

r_B

r_C

a

b

c

} exp. koeffiz.

λ

β

f

exp.-ausw.

m

$$m_1 \equiv m^\alpha \pmod{r_A}$$

$$m_2 \equiv m^\beta \pmod{r_A}$$

Zagaro]: Koeffizienz m.

r_A, a, b, m₁, m₂

m - ?

$$\alpha x + \beta y = 1$$

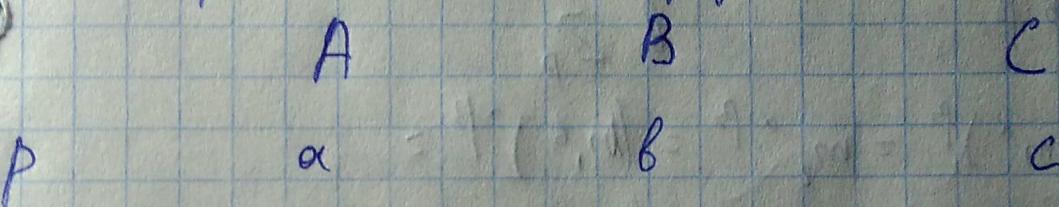
(x_0, y_0)

$$\alpha x_0 + \beta y_0 = 1$$

$$m_1^{x_0} \cdot m_2^{y_0} = (m^\alpha)^{x_0} (m^\beta)^{y_0} = m^{\alpha x_0 + \beta y_0} = m^1 = m$$

Kryptosystemet følger følgende kurser

13.19



$$1) \quad \gcd(\alpha, p-1) = 1, \quad \gcd(\beta, p-1) = 1, \quad \gcd(\gamma, p-1) = 1$$

$$2) \quad \alpha \cdot \alpha^{-1} \equiv 1 \pmod{p-1}, \quad \beta \cdot \beta^{-1} \equiv 1 \pmod{p-1}, \quad \gamma \cdot \gamma^{-1} \equiv 1 \pmod{p-1}$$

$$\alpha \cdot \alpha^{-1} \equiv 1 \pmod{p-1} \quad \beta \cdot \beta^{-1} \equiv 1 \pmod{p-1} \quad \gamma \cdot \gamma^{-1} \equiv 1 \pmod{p-1}$$

cekp
vech

(α, α)	(β, β)	(γ, γ)
--------------------	------------------	--------------------

$$m_1 = m_1^\alpha \pmod{p}$$

$$m_2 = m_2^\alpha \pmod{p}$$

$$m_3 = m_3^\alpha \pmod{p}$$

$$m_4 = m_4^\alpha \pmod{p}$$

$$D \rightarrow G, \text{med } m = m_4 \in \mathbb{Z}_p$$

$$\alpha \alpha = 1 + \varphi(p) h$$

$$m_4 = (m^{\alpha})^\beta = (m^{1 + \varphi(p) h})^{1 + \varphi(p) l} =$$

$$= (m m^{\varphi(p) h}) (m m^{\varphi(p) h})^{\varphi(p) l}$$

$$m \underset{\text{``1''}}{(m^{\varphi(p)})^h} \underset{\text{``1''}}{(m^{\varphi(p)})^l} \underset{\text{``1''}}{(m^{\varphi(p)})^h} \underset{\text{``1''}}{(m^{\varphi(p)})^l} = m_4$$

α, β - per.

$$\gcd(\alpha, p-1) = 1$$

$$m_4 = m^{\alpha \cdot \alpha \cdot \beta \cdot \beta} \quad \beta \geq p$$

$$m_4 = m_3^\beta = (m^\alpha)^\beta = m_2^{\alpha \cdot \beta} = (m_1^{\alpha})^{\alpha \beta} =$$

$$= m_1^{\alpha \cdot \beta} \underset{\text{``2''}}{=} (m^{\alpha})^{\alpha \beta} = m^{\alpha \cdot \alpha \beta} \quad \textcircled{2}$$

$$a \cdot \alpha \equiv 1 \pmod{\varphi(p)}$$

$$b \cdot \beta \equiv 1 \pmod{\varphi(p)}$$

$$a \cdot \alpha \cdot b \cdot \beta \equiv 1 \pmod{\varphi(p)}$$

$$a \cdot \alpha \cdot b \cdot \beta = 1 + l \varphi(p)$$

$$\textcircled{2} \quad m^{1 + l \varphi(p)} = m \underset{\text{``1''}}{(m^{\varphi(p)})^l} = m$$

Следовательно
Доказано

(1935)

A

B

1. p
2. g - generator, $\text{ord}_p(g) = p-1$
3. $x \in \{1, \dots, p-1\}$
4. $y = g^x \pmod{p}$

(p, g, y) - öffentl. Klasse

$\mathcal{Q} \subseteq \{1, \dots, p-1\}$

k -teile. Klasse

$$Q \equiv b/a^x \pmod{p}$$

$$a^x \equiv g^k \pmod{p}$$

$$b \equiv Q \cdot y^k \pmod{p}$$

(Q, b) - unbestimmt

Zagaro

$$\mathcal{D}-76 \quad Q \equiv b/a^x \pmod{p}$$

$$Q \in \mathcal{Q} \cdot y^k \cdot g^{-kx} = \mathcal{Q} \cdot g^{kx} \cdot g^{-kx} = \mathcal{Q}$$

$$a \equiv g^k \pmod{p} \Rightarrow a^x \equiv g^{kx} \pmod{p}$$

$$\equiv (a^x)^k \pmod{p} \equiv y^k \pmod{p} \Rightarrow$$

$$\Rightarrow a^x \equiv y^k \pmod{p}$$

$$b \equiv Q \cdot y^k \pmod{p} = \mathcal{Q} \cdot a^x \pmod{p} \Rightarrow a^{-1}$$

$$\mathcal{Q} \equiv a^{-x} \cdot b \pmod{p}$$

Задача Криптодокумент горячего, PGP о асм. 1

и не имеющий секрета k .

1-е коорд. $(a_1, b_1) = (27572, 50973)$

$a_1 = 123$ (рек. характерист.)

$(a_2, b_2) = (27572, 4246)$

$Q_2 = ?$

$p = 54751$

$$Q_1 \equiv Q_1 (a_1^*)^{-1} \pmod{p}$$

$$Q_2 = Q_2 (a_2^*)^{-1} \pmod{p} \stackrel{\text{log}_a}{=} b_2 (a_2 \log_a)$$

$$b_1 \equiv y^k Q_1 \pmod{p}$$

$$b_2 \equiv y^k Q_2 \pmod{p}$$

$$b_2^{-1} \equiv (y^k)^{-1} Q_2^{-1} \pmod{p}$$

$$b_1 b_2^{-1} \equiv y^k Q_1 (y^k)^{-1} Q_2^{-1} \pmod{p}$$

$$b_1 b_2^{-1} \equiv Q_1 Q_2^{-1} \pmod{p} \Rightarrow Q_2 \equiv Q_1 b_1^{-1} b_2 \pmod{p}$$

/g2j5gq

Задача $(p, g, y) = (23, 5, 14)$

$k = 16$

$Q = ?$

Вывеска: $x \rightarrow$

$$\frac{15}{16} = \frac{258}{256} \equiv 1 \pmod{16}$$

$$28 = 4^4 = 16^2 \equiv 0 \pmod{16}$$

$$81^4 \equiv 1 \pmod{16}$$

$$6 \equiv 20 \cdot 14^{16} \pmod{16}$$

$$6 \equiv 4 \cdot (2)^{16} \pmod{16}$$

$$(a, b) = (3, 22)$$

$$x = 21$$

Шифрование ногнус
на основе схемы Ганнеле

A



B

- I.
- 1) p
 - 2) g - нрвнл. эл. в \mathbb{Z}_p
 - 3) $x \in \{1, \dots, p-1\}$
 - 4) $y \equiv g^x \pmod{p}$ - сек. кннк

(p, g, y) - от. кннк.

$$1) k \quad \text{gcd}(k, p-1) = 1$$

$$2) r \equiv g^k \pmod{p}$$

$$3) s \equiv (Q - x \cdot r) k^{-1} \pmod{p-1}$$

Q $[r, s]$
однок. ногнус

$$1) 0 \leq r < p, \quad 0 \leq s < p-1$$

$$2) y^{r+s} \equiv g^Q \pmod{p}$$

нрвн. ногн.
нрвн. ногн.

Zagaro | $\theta = 76$, now easy

$$y^r r^s \equiv g^{\theta} \pmod{p}$$

Decr-e:

$$g^{\theta} \equiv y^r r^s \pmod{p} \Leftrightarrow$$

$$g^{\theta} \equiv x^{xr+ks} \pmod{p}$$

$$1) y \equiv g^x \pmod{p}$$

$$y^r \equiv g^{xr} \pmod{p}$$

$$2) r \equiv g^k \pmod{p}$$

$$r^s \equiv g^{ks} \pmod{p}$$

$$y^r r^s \equiv g^{xr+ks} \pmod{p}$$

$$3) sk \equiv \theta - xr \pmod{p-1}$$

$$\exists l \in \mathbb{Z} \quad sk = \theta - xr + l(p-1)$$

$$\begin{aligned} & \theta \not\equiv p \quad y^r r^s \equiv g^{xr+ks} = g^{\theta + l(p-1)} \\ & = g^{\theta} (g^{p-1})^l = g^{\theta} \end{aligned}$$

$$g^0 = 1, g^1, \dots, g^{p-2}, g^{p-1}$$

Zagaro | $\theta = 3, p = 23, g = 5, x = 7, k = 5$
 $(r, s) = ?$

~~$23 \not\equiv 1 \pmod{22}$~~
 $(20, 21)$

Zagara (p, q, y) = (337, 15, 303)

	ϱ	r	s
1)	309	31	232
2)	19	31	74
3)	106	31	324
4)	106	185	81
5)	99	187	88

Криптосистема Меркеля-Каллидано (1978)

Оп. Использование низкочастотных символов

$$x_i > \sum_{j=1}^{i-1} x_j \quad \forall i$$

A

1. $wv = (w_1, \dots, w_n) \leftarrow$ супервозр.

2. q, r

$$\gcd(q, r) = 1$$

$$q > \sum_{i=1}^n w_i$$

$$\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$$

$$\alpha_i = \# w_i \pmod{q}$$

(w, q, r) -
супр. кимр.

Мног - e

A

B

$$m = (m_1, \dots, m_n)$$

$$m_i \in \{0, 1\}$$

$$S = \sum_{i=1}^n a_i m_i$$

Равнодействие

$$1. r^{-1} : \mathbb{Z}_q$$

$$2. s' \equiv sr^{-1} \pmod{q}$$

равнодействие на основе s'

Задача I $g - \pi_b$.

$$S = a_1 m_1 + a_2 m_2 + \dots + a_n m_n$$

$$S' = S q^{-1} \pmod{q} = \sum_{i=1}^n a_i m_i q^{-1} \pmod{q} \quad (\textcircled{1})$$

$$a_i \neq w_i \pmod{q}$$

$$\textcircled{2} \quad \sum_{i=1}^n q a_i m_i q^{-1} \pmod{q}$$

$$S' = \sum_{i=1}^n w_i m_i \pmod{q}$$

$$w_n > S' \Rightarrow m_n \geq 0$$

$$w_n \leq S' \Rightarrow m_n = 1$$

$$S'' = S' - m_n w_n = w_{n-1}$$

Задача II $A \sim O = (0, 0, 0, 0, 0)_2$

$$B \sim 25 = (1, 1, 0, 0, 1)_2$$

$$W = (2, 3, 7, 15, 31)$$

$q = 61$, $n = 17$, $a = ?$ "why"

$$17 \cdot 2 \equiv 34 \pmod{61}$$

$$17 \cdot 3 \equiv 51 \pmod{61}$$

$$17 \cdot 7 \equiv 119 \equiv 58 \pmod{61}$$

$$17 \cdot 15 \equiv 255 \equiv 11 \pmod{61}$$

$$17 \cdot 31 \equiv 527 \equiv 39 \pmod{61}$$

(34, 51, 58, 11, 39)

$$w = 34 + 58 + 11 = 92 + 41 = 103 \quad (103)$$

$$h = 58 + 39 + 11 = 108 \quad (108)$$

$$y = 34 + 51 = 85 \quad (85)$$

Задача Рассмотрим задачу о соотношении

$$A = 1 = (0, 0, 0, 0, 0, 1)$$

$$B = 32 = (1, 0, 0, 0, 0, 0)$$

$$W = (1, 2, 4, 9, 18, 35)$$

$$q = 80, n = 29$$

$$X = (100, 58, 21, 79, 100, 155)$$

$$\alpha(9, 18, 16, 4, 2, 15)$$

$$\beta(1, 0, 1, 1, 1)$$
$$X = (55, 97, 21, 79, 100, 155)$$

126 to 04