

Московский авиационный институт
(национальный исследовательский университет)

«Задача дискретного логарифмирования и криптосистемы на ее основе»

Подготовил: Проскурнин Д.В., гр. 3-РО-403Б-15

Преподаватель: Машкин М.Н., каф. 302

Москва 2018 г.

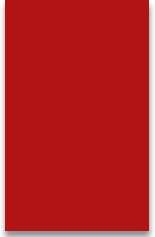
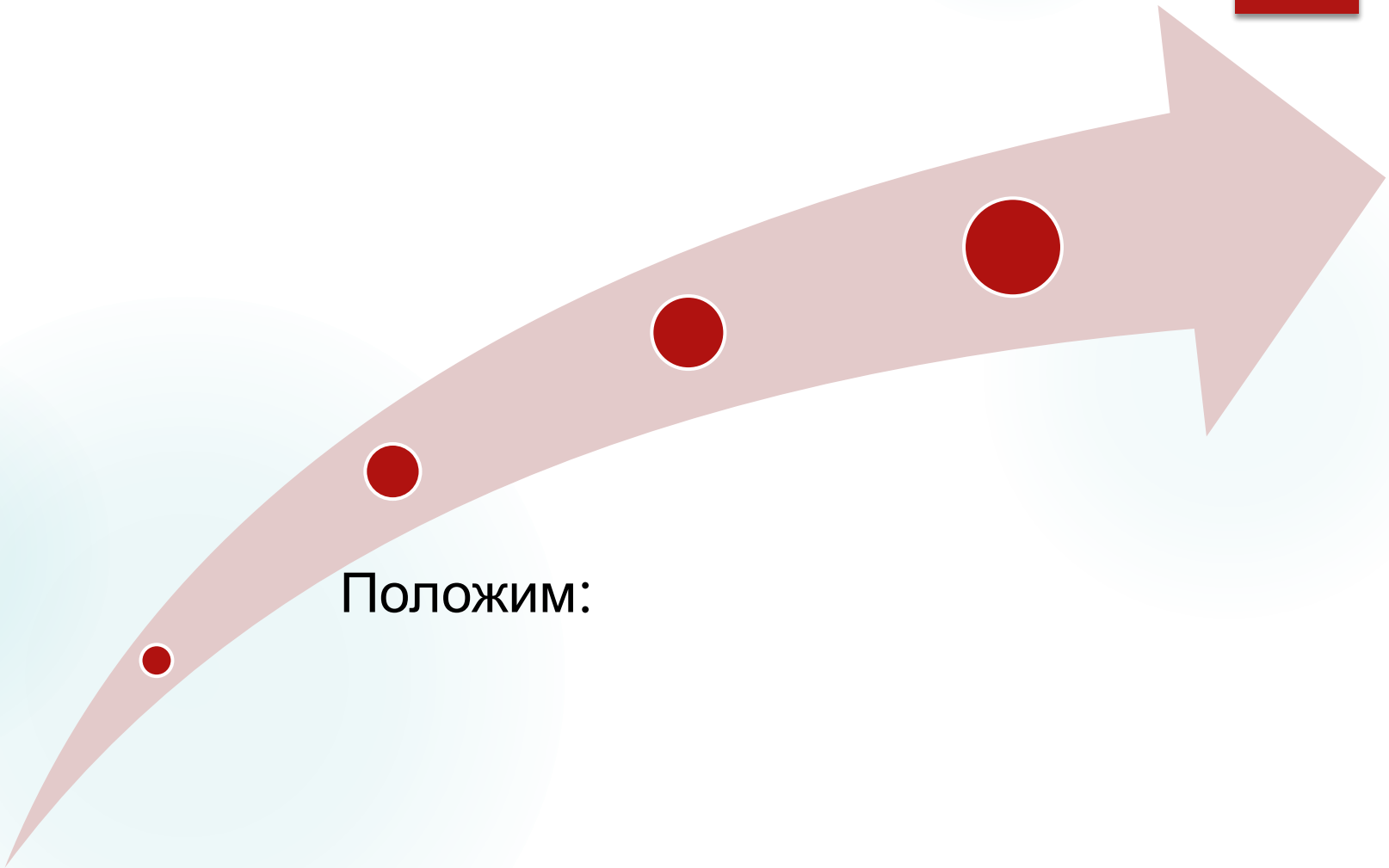


Задача дискретного логарифмирования

$$a^x = b \pmod{m},$$

где a и m известны и взаимно просты (не имеют общих делителей), b также известно.

Рассмотрим алгоритм решения данного уравнения.



Положим:

► Таким образом, имеем уравнение:

$$f_1(p) = f_2(q),$$

при чем, $p \in [1; \lceil \frac{m}{n} \rceil]$ и $q \in [0; n]$

Метод meet-in-the-middle:

$f_1(p) \forall p: p \in [1; \lceil \frac{m}{n} \rceil]$, и отсортировать эти значения.

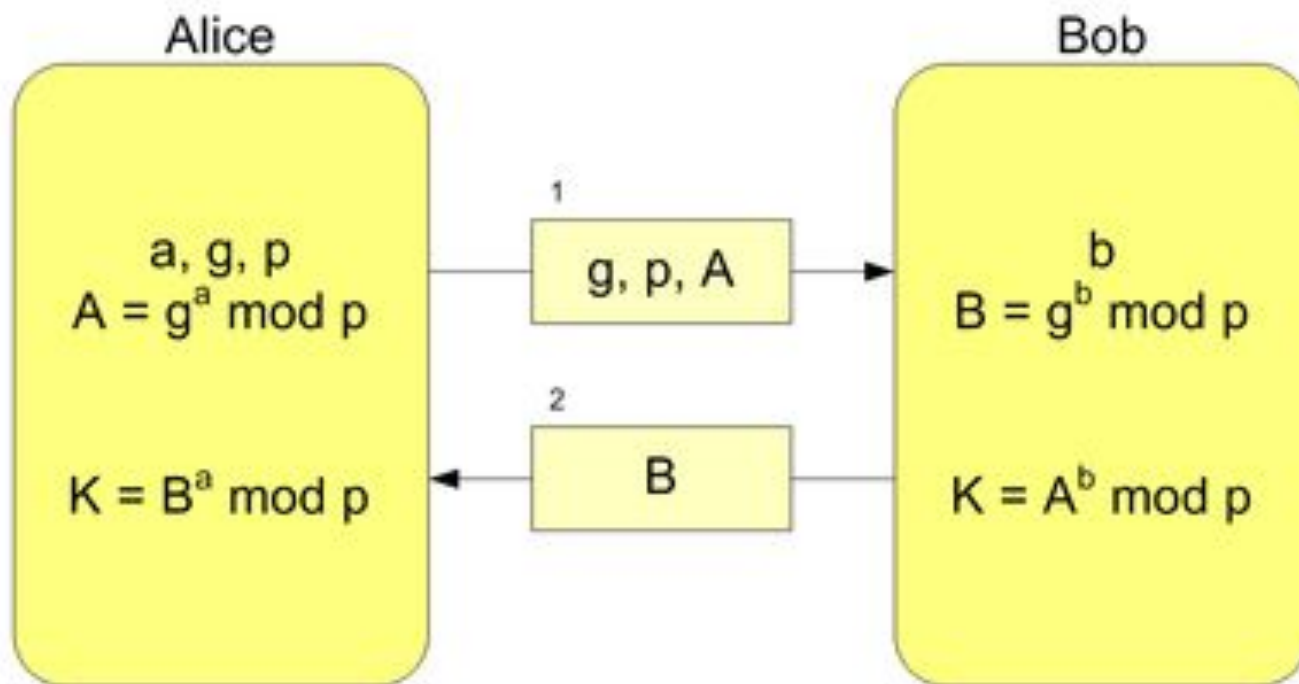
$f_2(q) \forall q: q \in [0; n]$, и искать это значение среди предвычисленных значений f_1 .

Криптосистемы

- ▶ протокол Диффи-Хеллмана;
- ▶ схема Эль-Гамала;
- ▶ криптосистема Мэсси-Омуры.

Протокол Диффи-Хеллмана

Разработан в 1976 году Уитфилдом Диффи и Мартином Хеллманом под влиянием работ Ральфа Меркле (*Ralph Merkle*)



$$K = A^b \text{ mod } p = (g^a \text{ mod } p)^b \text{ mod } p = g^{ab} \text{ mod } p = (g^b \text{ mod } p)^a \text{ mod } p = B^a \text{ mod } p$$

Алгоритм

При работе алгоритма каждая сторона:

1. генерирует случайное натуральное число a — *закрытый ключ*
2. совместно с удалённой стороной устанавливает *открытые параметры* p и g (обычно значения p и g генерируются на одной стороне и передаются другой), где

p является случайным простым числом

$(p-1)/2$ также должно быть случайным простым числом (для повышения безопасности)^[5]

g является первообразным корнем по модулю p (*также является простым числом*)

3. вычисляет *открытый ключ* A , используя преобразование над *закрытым ключом*

$$A = g^a \bmod p$$

4. обменивается *открытыми ключами* с удалённой стороной
5. вычисляет *общий секретный ключ* K , используя открытый ключ удаленной стороны B и свой закрытый ключ a

$$K = B^a \bmod p$$

K получается равным с обеих сторон, потому что:

$$B^a \bmod p = (g^b \bmod p)^a \bmod p = \mathbf{g^{ab} \bmod p} = (g^a \bmod p)^b \bmod p = A^b \bmod p$$

Криптографическая стойкость

- ▶ Основана на предполагаемой сложности проблемы дискретного логарифмирования.
- ▶ Работает только на линиях связи, надёжно защищённых от модификации.
- ▶ Когда в канале возможна модификация данных, появляется очевидная возможность вклинивания в процесс генерации ключей «злоумышленника-посредника» по той же самой схеме, что и для асимметричной криптографии.

Практика

Задание: вычислить открытые ключи A и B , а также общий секретный ключ K , используя открытые параметры g и p и закрытые ключи a и b

- ▶ Исходные данные

$$g = 5; p = 23; a = 6; b = 15$$

- ▶ K = секретный ключ. $K = 2$
- ▶ g = первообразный корень по модулю p . $g = 5$
- ▶ A = открытый ключ. $A = g^a \bmod p = 8$
- ▶ B = открытый ключ. $B = g^b \bmod p = 19$

Спасибо за внимание!