

# Протокол Диффи — Хеллмана

Подготовил: Жембловский Алексей

4 курс 9 группа

# Протокол

*Функция:*

Формирование общего секретного ключа при аутентифицируемом канале

*Параметры:*

$G$  - циклическая группа

$g$  – образующий группы,  $G = \langle g \rangle$

$q$  – порядок группы,  $|G| = q$  :

$G = \{g^0 = e, g^1, \dots, g^{q-1}\}$ ,

$g^q = g^0 = e, g^{q+1} = g^1, \dots$

# Протокол

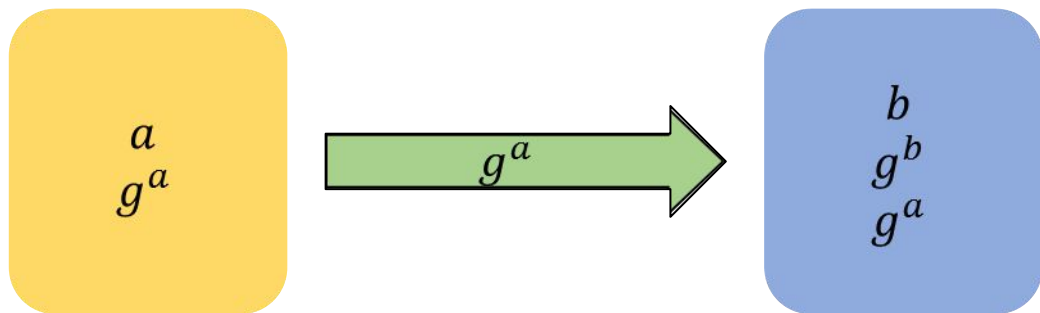
• *Стороны:*  $A$  (Алиса),  $B$  (Боб),  $V$  – злоумышленник Виктор

• *Шаги:*

1.  $A: a \xleftarrow{R} \{1, 2, \dots, q - 1\}, g^a$  ( $a$ - секретный ключ  $A$ ,  $g^a$  – открытый ключ  $A$ )

2.  $B: b \xleftarrow{R} \{1, 2, \dots, q - 1\}, g^b$  ( $b$  - секретный ключ  $B$ ,  $g^b$  – открытый ключ  $B$ )

3.  $A \xrightarrow{\text{АКС}} B: g^a$ .



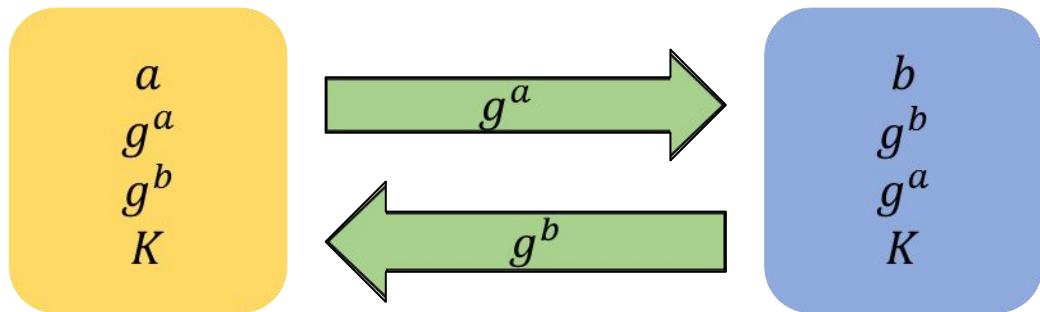
# Протокол

4.  $A \xleftarrow{\text{AKC}} B: g^b.$

5.  $A: K \leftarrow (g^b)^a.$

6.  $B: K \leftarrow (g^a)^b.$

- *Корректность:*  $K = (g^b)^a = (g^a)^b = g^{ab}.$



# ПРОТИВНИК

Знает:

- Описание  $G, g$
- $g^a, g^b$

Должен узнать:

- $K$

$(g, g^a, g^b) \rightarrow g^{ab}$  - вычислительная задача Диффи-Хеллмана

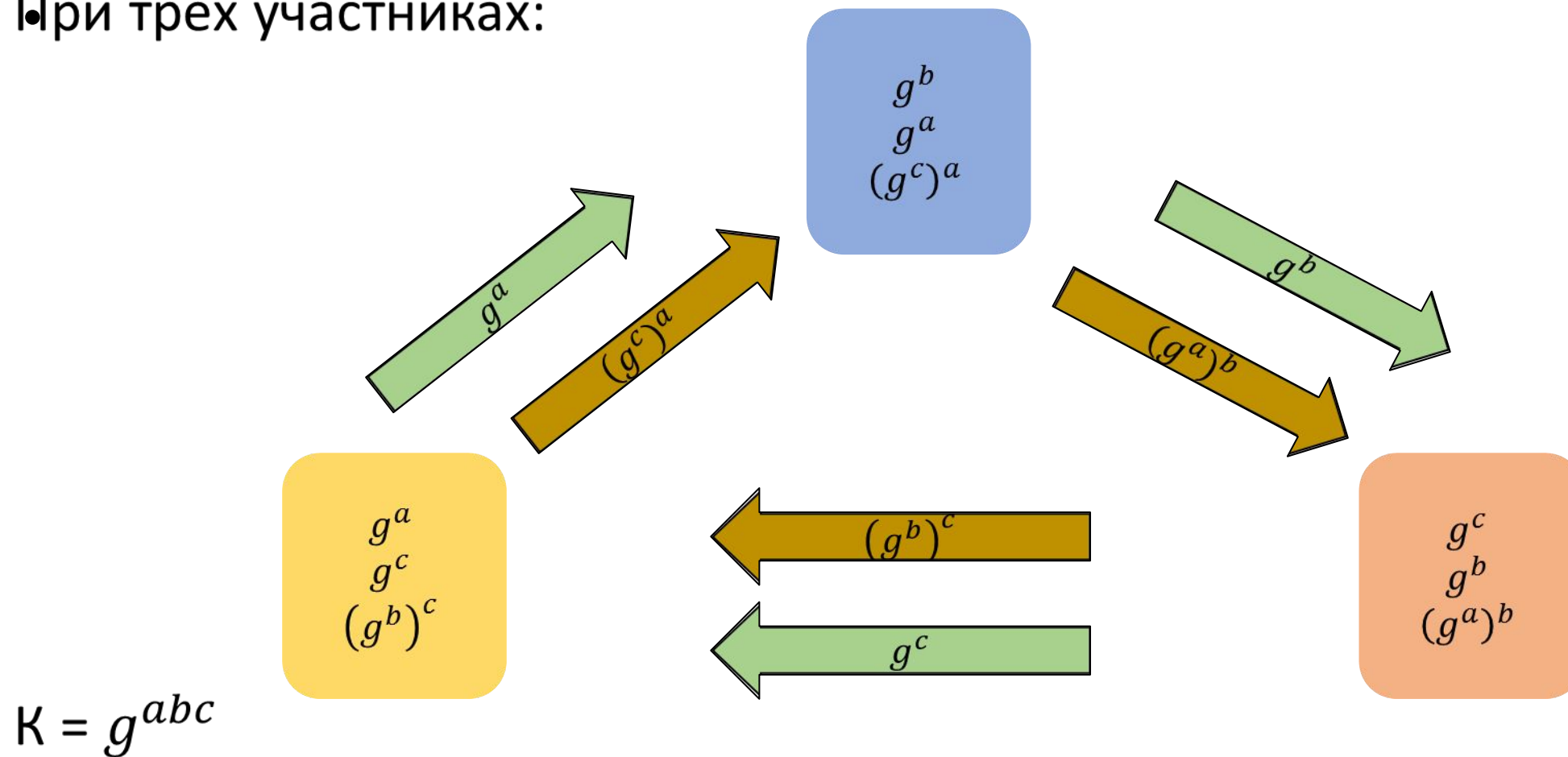
# Сложность

Участники	задача	Сложность*
A, B		
V	вычислительная задача Диффи-Хеллмана	

\* - При криптографически правильном выборе  $G$

# Масштабируемость

При трёх участниках:



# Атака «противник посередине»

Можно ли вместо АКС использовать ОКС? Нет.

Атака :

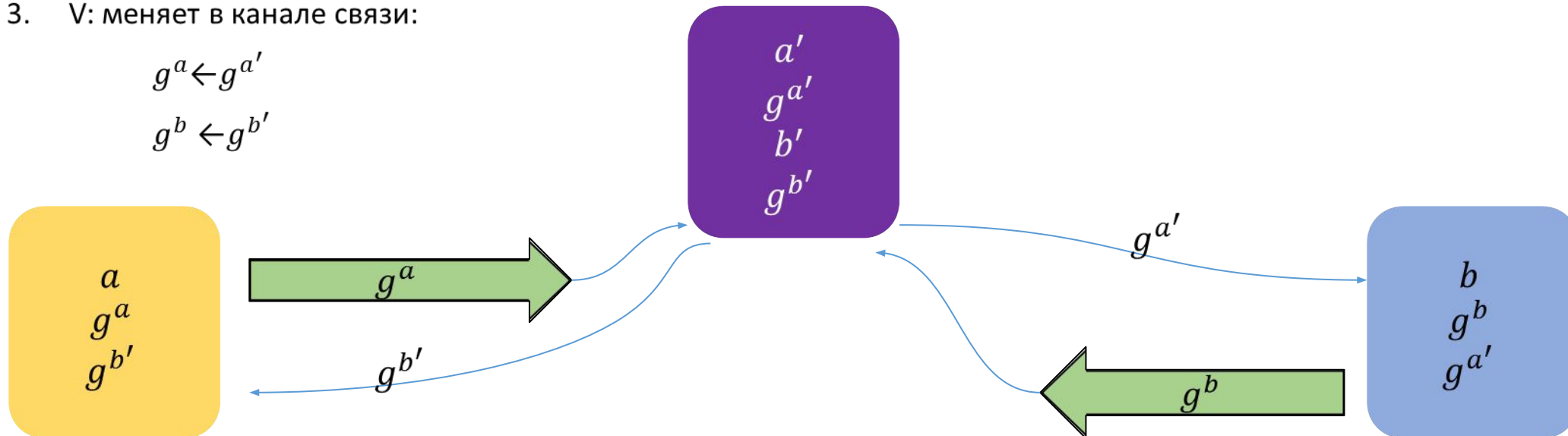
1.  $V: a' \xleftarrow{R} \{1, 2, \dots, q - 1\}, g^{a'}$

2.  $V: b' \xleftack{R} \{1, 2, \dots, q - 1\}, g^{b'}$

3. V: меняет в канале связи:

$$g^a \leftarrow g^{a'}$$

$$g^b \leftarrow g^{b'}$$





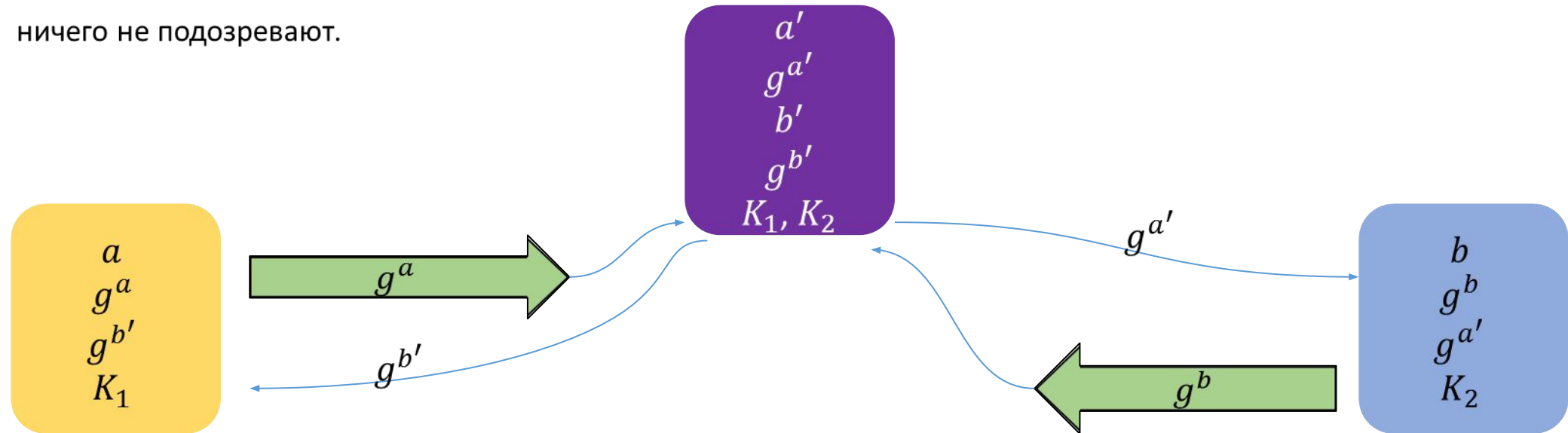
# Атака «противник посередине»

4. A:  $K_1 \leftarrow (g^{b'})^a$

5. B:  $K_2 \leftarrow (g^{a'})^b$

6. V: получает  $K_1 = (g^{b'})^a, K_2 = (g^{a'})^b$

А и В обмениваются сообщениями,  
ничего не подозревают.



# Пример реализации атаки

(система CAPTCHA)

Стороны:  $A$  (Сайт),  $B$  (Пользователь),  $V$  (Сайт злоумышленник).

Шаги:

1.  $A: I_A \leftarrow T_A$  ( $I_A$  – изображение текста,  $T_A$  – ключевой текст)
2.  $V: I_B \leftarrow I_A$
3.  $V \leftarrow B: T_A \leftarrow I_B$
4.  $V \rightarrow A: T_A$

# Реализация протокола

$F_p = \{0, 1, \dots, p - 1\} \text{ mod } p$  – простое поле

$F_p^*$  - мультипликативная группа  $\langle F_p \setminus \{0\}, * \rangle$

*Теорема.*  $F_p^*$  - циклическая группа

# Алгоритм построения примитивного элемента

*Вход:*  $p$  – простое,  $p - 1 = \prod_{i=1}^k p_i^{l_i}$

*Выход:*  $\alpha$  – примитивный элемент  $F_p^*$

*Шаги:*

1.  $\alpha \xleftarrow{R} F_p^*$
2. Для  $i = 1, \dots, k$ :
  1. Если  $\alpha^{\frac{p-1}{p_i}} \equiv 1 \pmod{p}$ , то шаг 1.
3. Возвращаем  $\alpha$

# Алгоритм генерации $G \subseteq F_p^*$

*Вход:*  $p$  – простое,  $\alpha$  – примитивный элемент  $F_p^*$ ,  $q \mid (p - 1)$

*Выход:*  $g \in F_p^*$ ,  $\text{ord}(g) = q$ ,  $G = \langle g \rangle$

*Шаги:*

1.  $g \leftarrow \alpha^{\frac{p-1}{q}} \pmod p$
2. Возвращаем  $g$

# Алгоритм генерации группы простого порядка

*Вход:*  $p$  – простое,  $q$  – простое,  $q \mid (p - 1)$

*Выход:*  $g \in F_p^*$ ,  $\text{ord}(g) = q$ ,  $G = \langle g \rangle$

*Шаги:*

1.  $\alpha \xleftarrow{R} F_p^*$
2.  $g \leftarrow \alpha^{\frac{p-1}{q}} \pmod{p}$
3. Если  $g = 1$ , то возвращаемся к шагу 1.
4. Возвращаем  $g$

**Спасибо за просмотр**