# Распределение ключей

## 2. Протоколы открытого распределения ключей

### Алгоритм Диффи-Хеллмана с тремя и более участниками

Алиса, Боб и Кэрол вместе генерируют секретный ключ. Общие параметры имеют тот же смысл. Графическая схема показана на рис. 6.

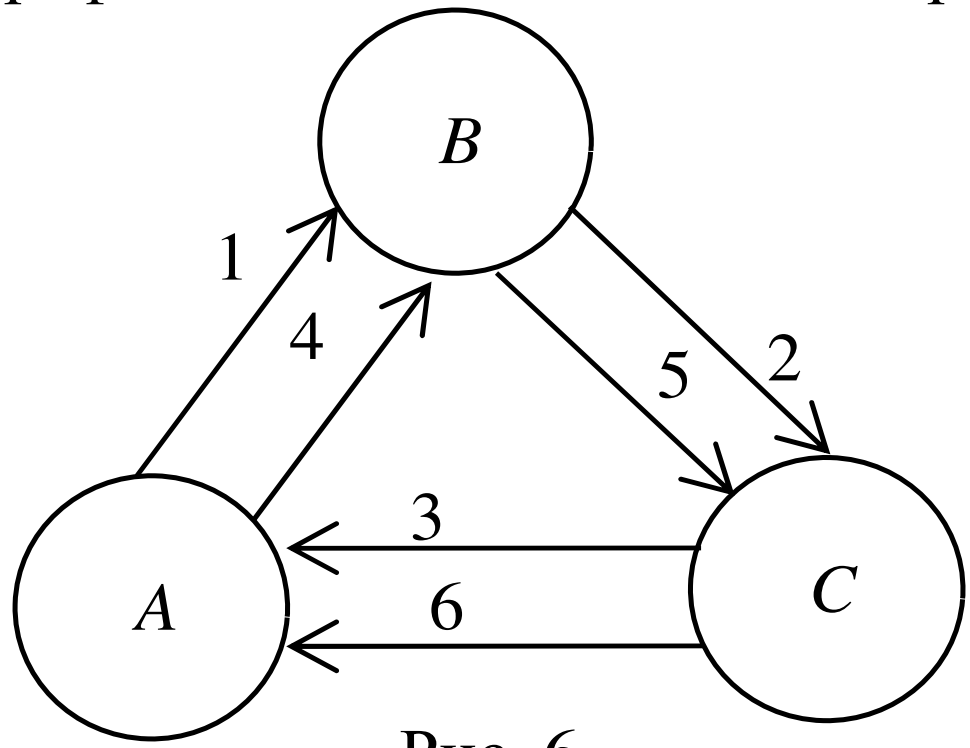


Рис. 6

# Распределение ключей

## 2. Протоколы открытого распределения ключей

## Алгоритм Диффи-Хеллмана с тремя и более участниками

1. Первый цикл проходов:
   - 1.1. $A \rightarrow B$: $\{X = g^x \bmod p\}$, где $x$ — случайное секретное целое число Алисы из интервала $1 < x < p$.
   - 1.2. $B \rightarrow C$: $\{Y = g^y \bmod p\}$, где $y$ — случайное секретное целое число Боба из интервала $1 < y < p$.
   - 1.3. $C \rightarrow A$: $\{Z = g^z \bmod p\}$, где $z$ — случайное секретное целое число Кэрол из интервала $1 < z < p$.

# Распределение ключей

## 2. Протоколы открытого распределения ключей

### Алгоритм Диффи-Хеллмана с тремя и более участниками

2. Второй цикл проходов:
   - 2.1. $A \to B$: $\{Z' = Z^x \bmod p\}$.
   - 2.2. $B \to C$: $\{X' = X^y \bmod p\}$.
   - 2.3. $C \to A$: $\{Y' = Y^z \bmod p\}$.
3. Этап вычисление секретного ключа каждым участником:
   - 3.1. $A$: $K = Y'^x \bmod p$.
   - 3.2. $B$: $K = Z'^y \bmod p$.
   - 3.3. $C$: $K = X'^z \bmod p$.

Закрытый ключ $K$ равен $g^{xyz} \bmod p$. При расширении протокола на $n$ участников, очевидно, будет $n - 1$ циклов из $n$ проходов.

# Распределение ключей

## 2. Протоколы открытого распределения ключей

### Алгоритм Хьюза

В протоколе Диффи-Хеллмана по сути секретный ключ генерируется по ходу его проведения и никто не знает на сколько хорошими характеристиками он будет обладать. Что является одним из заметных недостатков этого протокола.

Иной вариант алгоритма Диффи-Хеллмана, предложенный Хьюзом (Hughes), позволяет Алисе сначала генерировать ключ, проверить его надёжность, и уже потом послать его Бобу. Общие параметры те же. Он так же двухпроходный, графическая схема изображена на рис. 7.

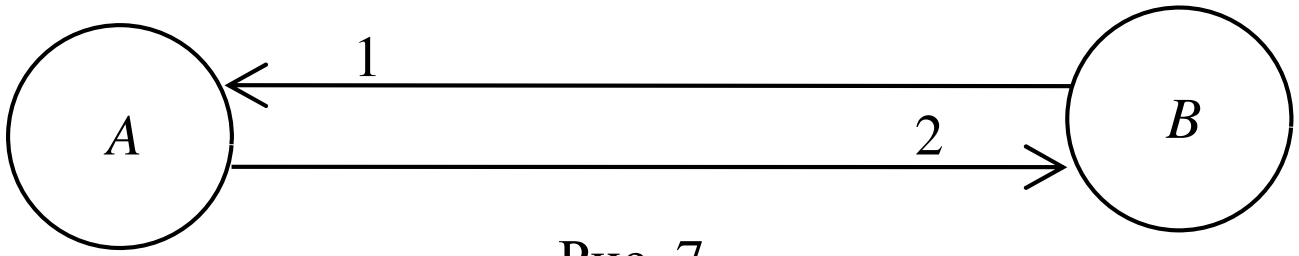


Рис. 7

# Распределение ключей

## 2. Протоколы открытого распределения ключей

### Алгоритм Хьюза

1. $A$: $K = g^x \bmod p$, где $x$ — случайное секретное целое число Алисы из интервала $1 < x < p$, (Алиса генерирует сеансовый ключ $K$).
2. $B \to A$: $\{Y = g^y \bmod p\}$, где $y$ — случайное секретное целое число Боба из интервала $1 < y < p$ с условием $(y, p - 1) = 1$. Если $p$ – сильное простое число, например, вида $p = 2^k q + 1$, тогда $y$ может быть любым большим случайным нечетным числом, кроме $q$.
3. $A \to B$: $\{X = Y^x \bmod p\}$.
4. $B$: $z = y^{-1} \bmod (p - 1)$, $K' = X^z \bmod p$.

Если все выполнено правильно, то $K = K'$. Действительно, учитывая свойства индексов: $X^z = X^{y^{-1}} = g^{yxy^{-1}} \equiv g^x \bmod p \Leftrightarrow yxy^{-1} \equiv x \bmod (p - 1)$.

# Распределение ключей

## 2. Протоколы открытого распределения ключей

### Алгоритм Хьюза

Преимуществом описанного выше протокола над протоколом Диффи-Хеллмана состоит в том, что $K$ можно вычислить заранее, до какого-либо взаимодействия, и Алиса может зашифровать сообщения с помощью $K$ задолго до установления соединения с Бобом. При этом Алиса может послать сообщение сразу множеству людей, а передать ключ позднее каждому по отдельности.