**Вариант 1**

Два легальных пользователя - Алиса и Боб. Перед передачей данных Алиса и Боб проходят процедуру согласования, используя публичный ключ Боба.

$$А \rightarrow Б: E\_{pk\_{b}}(r)$$

Затем Боб шлет Алисе сообщение $hello$ зашифрованное симметричным алгоритмом на ключе, выработанным с помощью случайного числа *r.*

$$Б \rightarrow А: E\_{K\_{r}}(hello)$$

Алиса расшифровывает сообщение и проверяет, что передано сообщение $hello$. После этого Алиса и Боб начинают передачу зашифрованных данных на ключе $ E\_{K\_{r}}$.

**Вариант 2**

Два легальных пользователя - Алиса и Боб. Перед передачей данных Алиса и Боб проходят процедуру согласования, используя публичный ключ Боба.

$$А \rightarrow Б: E\_{pk\_{b}}(r, counter)$$

Боб проверяет, что значение $counter$ не повторялось на предыдущих согласованиях. Затем Боб шлет Алисе сообщение $hello$ зашифрованное симметричным алгоритмом на ключе, выработанным с помощью случайного числа *r.*

$$Б \rightarrow А: E\_{K\_{r}}(hello)$$

Алиса расшифровывает сообщение и проверяет, что передано сообщение $hello$. После этого Алиса и Боб начинают передачу зашифрованных данных на ключе $ E\_{K\_{r}}$.

**Вариант 3**

Два легальных пользователя - Алиса и Боб. Перед передачей данных Алиса и Боб проходят процедуру согласования, используя общий секретный ключ.

$$А \rightarrow Б: counter, E\_{K}\left(r\right), MAC\_{K}(r)$$

Боб проверяет, что значение $counter$ не повторялось на предыдущих согласованиях. Затем Боб шлет Алисе сообщение $hello$ зашифрованное симметричным алгоритмом на ключе, выработанным с помощью случайного числа *r.*

$$Б \rightarrow А: E\_{K\_{r}}(hello)$$

Алиса расшифровывает сообщение и проверяет, что передано сообщение $hello$. После этого Алиса и Боб начинают передачу зашифрованных данных на ключе $ E\_{K\_{r}}$.