4.3. Основные способы использования алгоритмов с открытым ключом

Основными способами использования алгоритмов с *открытым ключом* являются шифрование/дешифрование, создание и проверка подписи и обмен ключа.

Шифрование с *открытым ключом* состоит из следующих шагов:

1. Пользователь B создает пару ключей KU_b и KR_b, используемых для шифрования и дешифрования передаваемых сообщений.
2. Пользователь B делает доступным некоторым надежным способом свой ключ шифрования, т.е. *открытый ключ* KU_b. Составляющий пару *закрытый ключ* KR_b держится в секрете.
3. Если A хочет послать сообщение B, он шифрует сообщение, используя *открытый ключ* B KU_b .
4. Когда B получает сообщение, он дешифрует его, используя свой *закрытый ключ* KR_b. Никто другой не сможет дешифровать сообщение, так как этот *закрытый ключ* знает только B.

Создание и проверка подписи состоит из следующих шагов:

1. Пользователь A создает пару ключей KR_A и KU_A, используемых для создания и проверки подписи передаваемых сообщений.
2. Пользователь A делает доступным некоторым надежным способом свой ключ проверки, т.е. *открытый ключ* KU_A. Составляющий пару *закрытый ключ* KR_A держится в секрете.
3. Если A хочет послать подписанное сообщение B, он создает подпись $E_{KRa}[M]$ для этого сообщения, используя свой *закрытый ключ* KR_A.
4. Когда B получает подписанное сообщение, он проверяет подпись $D_{KUa}[M]$, используя *открытый ключ* A KU_A. Никто другой не может подписать сообщение, так как этот *закрытый ключ* знает только A.

*Обмен ключей***:** две стороны взаимодействуют для обмена ключом сессии, который в дальнейшем можно использовать в алгоритме симметричного шифрования.

Некоторые алгоритмы можно задействовать тремя способами, в то время как другие могут использоваться одним или двумя способами.