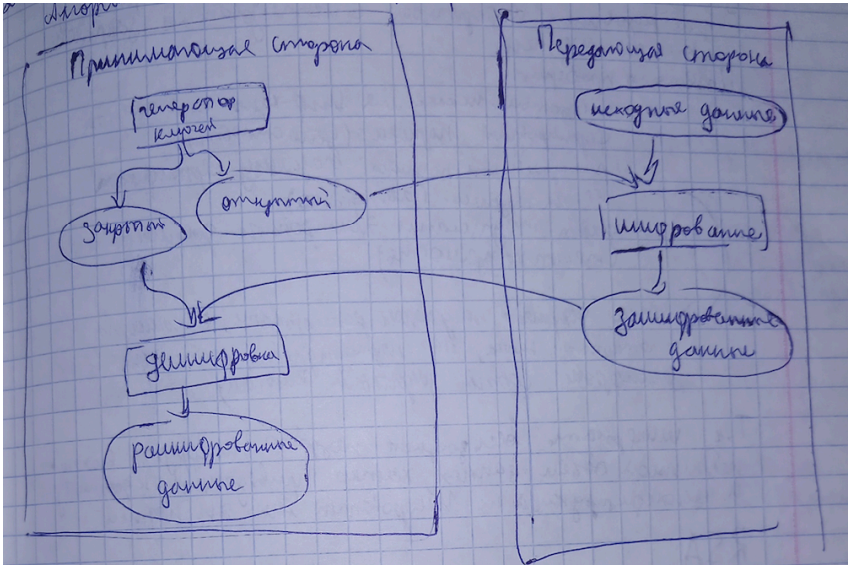
21 Асимметричные криптосистемы, электронная подпись. Алгоритм RSA. Комбинированные системы шифрования



- зная открытый ключ, нельзя вычислить закрытый ключ за разумное время (используются большие простые числа).
- метод шифрования открытым ключом так, чтобы расшифровать можно было только закрытым.
- закрытый ключ секретный, открытый ключ можно распространять свободно.

RSA-ключи

RSA-ключи генерируются следующим образом:

1. выбираются два различных случайных простых числа p и q заданного размера;
2. вычисляется их произведение n = p * q, которое называется модулем;
3. вычисляется значение функции Эйлера от числа n: ϕ(n) = (p-1) * (q-1);
4. выбирается целое число e (1 < e < ϕ(n)), которое называется открытой экспонентой (англ. public exponent).
   Обычно в качестве e берут простые числа, содержащие небольшое количество единичных бит в двоичной записи, например, простые из чисел Ферма: 17, 257 или 65537, так как в этом случае время, необходимое для шифрования с использованием быстрого возведения в степень, будет меньше. Слишком малые значения, например 3, потенциально могут ослабить безопасность схемы RSA.
5. вычисляется число d, мультипликативно обратное к числу e по модулю ϕ(n), то есть число, удовлетворяющее сравнению:
   $d \cdot e \equiv 1 \pmod{\varphi(n)}$
   (число d называется секретной экспонентой; обычно оно вычисляется при помощи расширенного алгоритма Евклида);

6. пара (e, n) публикуется в качестве открытого ключа RSA (англ. RSA public key);
7. пара (d, n) играет роль закрытого ключа RSA (англ. RSA private key) и держится в секрете.

RSA можно использовать для шифрования и расшифрования сообщений, а также для создания цифровой подписи.

шифрование

шифрование происходит с помощью открытого ключа:

1. берется открытый ключ (e, n)
2. берется открытый текст m
3. $c = E(m) = m^e \mod n$

для расшифрования используется закрытый ключ:

1. берется закрытый ключ (d, n)
2. берется зашифрованный текст c
3. $m = D(c) = c^d \mod n$

цифровая подпись

создание цифровой подписи происходит следующим образом:

1. берется открытый текст m
2. берется закрытый ключ (d, n)

3. $s = S_A(m) = m^d \mod n$

проверка цифровой подписи происходит следующим образом:

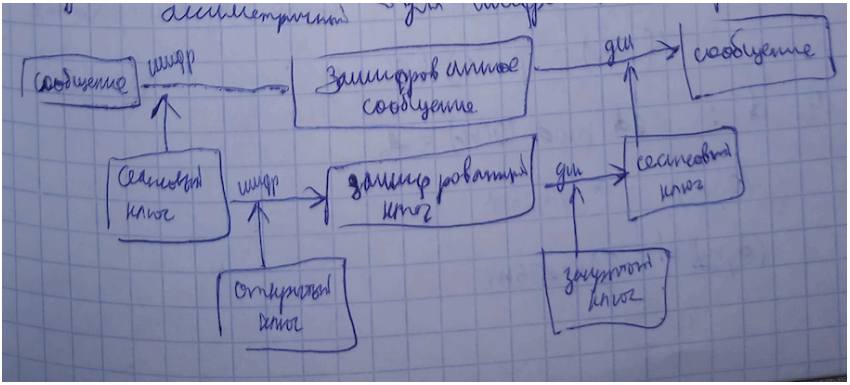
1. берется пара из сообщения и цифровой подписи (m, s)
2. берется открытый ключ (e, n)
3. $m' = P_A(s) = s^e \mod n$
4. проверить: $m = m'$. если равенство верно, то подпись действительна, а сообщение не изменено.

цифровая подпись используется для верификации документов. позволяет проверить:

- отсутствие искажений
- принадлежность подписи владельцу сертификата
- факт подписания документа - подлинность

комбинированные системы

используется симметричное шифрование для зашифровки данных и асимметричное шифрование для зашифровки симметричного ключа.


сообщение
шифр
Зашифрованное сообщение
дш
сообщение
Сеансовый ключ
шифр
Зашифрованный ключ
дш
Сеансовый ключ
Открытый ключ
Закрытый ключ