Криптосистема RSA

Выполнил Зайнуллин Богдан ИБ 31-19

- **RSA** (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.
- Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений, включая PGP, S/MIME, TLS/SSL, IPSEC/IKE и других

- Идея асимметричной криптосистемы с открытым и закрытым ключом приписывается Уитфилду Диффи и Мартину Хеллману, которые опубликовали эту концепцию в 1976 году. Они также ввели цифровые подписи и попытались применить теорию чисел. В их формулировке использовался секретный ключ с общим доступом, созданный путем экспоненциализации некоторого числа по модулю простого числа. Однако они оставили открытой проблему реализации односторонней функции, возможно, потому что сложность факторизации в то время не была хорошо изучена.

Криптографические системы с открытым ключом используют так называемые односторонние функции, которые обладают следующим свойством:

- если известно x, то $f(x)$ вычислить относительно просто;
- если известно $y = f(x)$, то для вычисления x нет простого (эффективного) пути.

В основу криптографической системы с открытым ключом RSA положена сложность задачи факторизации произведения двух больших простых чисел. Для шифрования используется операция возведения в степень по модулю большого числа. Для дешифрования (обратной операции) за разумное время необходимо уметь вычислять функцию Эйлера от данного большого числа, для чего необходимо знать разложение числа на простые множители.

- В криптографической системе с открытым ключом каждый участник располагает как открытым ключом (англ. *public key*), так и закрытым ключом (англ. *private key*). В криптографической системе RSA каждый ключ состоит из пары целых чисел. Каждый участник создаёт свой открытый и закрытый ключ самостоятельно. Закрытый ключ каждый из них держит в секрете, а открытые ключи можно сообщать кому угодно или даже публиковать их. Открытый и закрытый ключи каждого участника обмена сообщениями в криптосистеме RSA образуют «согласованную пару» в том смысле, что они являются *взаимно обратными*

открытого и секретного ключей

Алгоритм создания открытого и секретного ключей [править | править код]

RSA-ключи генерируются следующим образом[15]:

1) выбираются два различных случайных простых числа p и q заданного размера (например, 1024 бита каждое);
2) вычисляется их произведение $n = p \cdot q$, которое называется *модулем*;
3) вычисляется значение функции Эйлера от числа n:
   $\varphi(n) = (p-1) \cdot (q-1)$;
4) выбирается целое число e ($1 < e < \varphi(n)$), взаимно простое со значением функции $\varphi(n)$;
   число e 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 e, например 3, потенциально могут ослабить безопасность схемы RSA.[16];
5) вычисляется число d, мультипликативно обратное к числу e по модулю $\varphi(n)$, 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.

Система RSA может использоваться не только для шифрования, но и для цифровой подписи.

Поскольку цифровая подпись обеспечивает как аутентификацию автора сообщения, так и подтверждение целостности содержимого подписанного сообщения, она служит аналогом подписи, сделанной от руки в конце рукописного документа.

Важное свойство цифровой подписи заключается в том, что её может проверить каждый, кто имеет доступ к открытому ключу её автора. Один из участников обмена сообщениями после проверки подлинности цифровой подписи может передать подписанное сообщение ещё кому-то, кто тоже в состоянии проверить эту подпись. Например, сторона A может переслать стороне B электронный чек. После того как сторона B проверит подпись стороны A на чеке, она может передать его в свой банк, служащие которого также имеют возможность проверить подпись и осуществить соответствующую денежную операцию.

Заметим, что подписанное сообщение m не зашифровано. Оно пересылается в исходном виде и его содержимое не защищено от нарушения конфиденциальности. Путём совместного применения представленных выше схем шифрования и цифровой подписи в системе RSA можно создавать сообщения, которые будут и зашифрованы, и содержать цифровую подпись. Для этого автор сначала должен добавить к сообщению свою цифровую подпись, а затем — зашифровать получившуюся в результате пару (состоящую из самого сообщения и подписи к нему) с помощью открытого ключа, принадлежащего получателю. Получатель расшифровывает полученное сообщение с помощью своего секретного ключа[17]. Если проводить аналогию с пересылкой обычных бумажных документов, то этот процесс похож на то, как если бы автор документа поставил под ним свою печать, а затем положил его в бумажный конверт и запечатал, с тем чтобы конверт был распечатан только тем человеком, кому адресовано сообщение.

- Система RSA используется для защиты программного обеспечения и в схемах цифровой подписи.
- Также она используется в открытой системе шифрования PGP и иных системах шифрования (к примеру, DarkCryptTC и формат xdc) в сочетании с симметричными алгоритмами.
- Из-за низкой скорости шифрования, сообщения обычно шифруют с помощью более производительных симметричных алгоритмов со случайным *сеансовым ключом* (например, AES, IDEA, Serpent, Twofish), а с помощью RSA шифруют лишь этот ключ, таким образом реализуется гибридная криптосистема. Такой механизм имеет потенциальные уязвимости ввиду необходимости использовать криптографически стойкий генератор псевдослучайных чисел для формирования случайного сеансового ключа симметричного шифрования.