1 Криптосистема Рабина

Рассматриваемая ниже криптосистема Рабина является системой с доказуемо трудной проблемой расшифрования. А именно, дешифрование эквивалентно задаче модульного извлечения квадратного корня и, следовательно, задаче факторизации (См. раздел Квадратичные вычеты и квадратные корни Практикума).

Алгоритм генерации ключей в этой системе следующий.

Абонент A для обеспечения возможности передачи ему секретной информации на открытом ключе выбирает два случайных больших простых числа p и q и вычисляют их произведения $n = p \cdot q$.

Число n есть *открытый ключ шифрования* и публикуются через центр сертификации открытых ключей. Числа p и q составляют секретную *лазейку* и сохраняются как секретный ключ абонента A.[1].

Возможность вычислить и сертифицировать свой открытый ключ имеет каждый абонент сети. Существенно, что простые числа p и q должны выбираться абонентами независимо друг от друга.

Любой отправитель B, получив от центра сертификации сертификат открытого ключа абонента A, имеет возможность зашифровать и безопасно передать абоненту A секретное сообщение в виде числа m, $0 < m < n$. (Более длинные сообщения предварительно разбиваются на блоки, последовательно шифруемые и передаваемые абоненту A). Алгоритм E_A зашифрования абонентом B имеющегося сообщения для абонента A заключаются в возведении числа m в квадрат по модулю n :

$$c = E_A(m) = m^2 \bmod n,$$

где m и c – исходное открытое сообщение (шифрвеличина) и криптотекст (шифробозначение) соответственно.

Абонент A, получив шифртекст c от стороны B для его расшифрования с использованием своего секретного ключа находит четыре квадратных корня m_1, m_2, m_3, m_4 из числа c по модулю n и выбирает по смыслу один из них. (Для определённости выбора в сообщение может быть внесена избыточность).

[1]Абонент A в центре сертификации открытых ключей проходит аутентификацию некриптографического характера, предъявляет открытый ключ и криптографическим методом доказывает, что владеет соответствующим ему секретным ключом. При этом возможно использование протокола доказательства с нулевым разглашением секрета. Центр сертификации публикует открытый ключ данного абонента в составе сертификата открытого ключа за своей цифровой подписью,ключ проверки которой известен всем абонентам компьютерной сети. Использование сертифицированного открытого ключа гарантирует,что зашифрованная на этом ключе информация может быть расшифрована только владельцем соответствующего секретного ключа, имя которого указывается в сертификате открытого ключа

[2]

Пример. Пусть $p = 277$, $q = 331$, тогда $n = pq = 91687$. Открытый ключ есть $n = 91687$, секретный ключ есть $(p = 277,\ q = 331)$. Будем вводить избыточность дублированием шести последних битов 10-битового сообщения. Так из сообщения $m = 1001111001$ получим $\bar{m} = (1001111001111001)_2 = (40569)_{10}$.

При зашифровании вычисляют

$$c = m^2 \bmod n = 40569^2 \bmod 91687 = 62111.$$

при расшифровании с использованием p и q получают

$$m_1 = 69654,\ m_2 = 22033,\ m_3 = 40596,\ m_4 = 51118,$$

или в бинарной форме

$$m_1 = 10001000000010110,\quad m_2 = 101011000010001,$$

$$m_3 = 1001111001111001,\quad m_4 = 1100011110101110.$$

При этом только m_3 соответствует способу введения избыточности.

Как можно заметить, шифрсистема Рабина имеет очень быстрый алгоритм зашифрования. Скорость алгоритма расшифрования сравнима со скоростью расшифрования в RSA.

2 Контрольные вопросы

1. На какой трудной проблеме теории чисел основана безопасность криптосистемы Рабина и почему она называется теоретически безопасной?

2. Какие предосторожности следует соблюдать при выборе параметров криптосистемы Рабина?

3. Какова сложность алгоритмов зашифрования и расшифрования криптосистемы Рабина?

4. Возможно ли шифрование блоков текстов на естественном языке посредством криптосистемы Рабина без введения дополнительной избыточности?

---

[2] Алгоритм вычисления квадратных корней по модулю составного числа n при известной факторизации $n = pq$ следующий (См. раздел Квадратичные вычеты и квадратные корни практикума).

1. Ещё на этапе генерации ключей, используя расширенный алгоритм Евклида, вычислить целые a и b, такие, что $ap + bq = 1$.
2. Вычислить квадратные корни r и $-r$ числа c по модулю p.
3. Вычислить квадратные корни s и $-s$ числа c по модулю q.
4. Вычислить $x = (aps + bqr) \bmod n$.
5. Вычислить $y = (aps - bqr) \bmod n$.
6. Четыре квадратных корня по модулю n образуют следующие числа:

$$x,\ -x \bmod n,\ y\quad -y \bmod n.$$