Рассмотрим примеры криптосистем, безопасность которых определяется задачей разложения числа на множители.

## Криптосистема Рабина (Rabin)

Как и для RSA, рассмотрим протокол шифрования с открытым ключом. Отличие состоит в том, что показатель зашифрования ($e$ в RSA) равен 2, а расшифрование выполняется неоднозначно. Открытым ключом является пара $(n, B)$, где $n = pq$ – составное число, $B \in \{0, \dots, n-1\}$ – случайное, а секретным – разложение этого числа на множители. В основу криптосистемы положена следующая теорема.

**Теорема 1.** Задача нахождения всех четырех решений сравнения $y^2 \equiv \alpha \pmod{n}$ эквивалентна задаче разложения на множители $n = pq$.

Доказательство. Если известно разложение числа $n$, то сравнение может быть решено вычислением квадратных корней из $\alpha$ по модулям $p$ и $q$ и восстановлением результата по китайской теореме об остатках. Сложность вычислений оценивается полиномом от $\log n$ степени не выше 3. Обратно, если известны четыре корня, то они по китайской теореме могут быть представлены в виде

$$(\sqrt{\alpha}(mod\, p), \sqrt{\alpha}(mod\, q)),\ (\sqrt{\alpha}(mod\, p), -\sqrt{\alpha}(mod\, q)),$$

$$(-\sqrt{\alpha}(mod\, p), \sqrt{\alpha}(mod\, q)),\ (-\sqrt{\alpha}(mod\, p), -\sqrt{\alpha}(mod\, q)).$$

Тогда, если сумма по модулю $n$ двух корней не равна 0, то она имеет нетривиальный наибольший общий делитель с $n$, который может быть вычислен двоичным алгоритмом Евклида с квадратичной сложностью от $\log n$. ■

В качестве секретного ключа часто выбирают $p \equiv q \equiv 3(mod\ 4)$, поскольку решать сравнения вида $y^2 \equiv \alpha \pmod{n}$ в данном случае проще всего.

**Протокол 1.** Схема шифрования Рабина.
Вход отправителя. Открытый ключ $(n, B)$, сообщение $m \in \mathbb{Z}/n\mathbb{Z}$.
Вход получателя. Числа $p, q$, шифртекст $c$.
Зашифрование: $c \leftarrow m(m + B) \ (mod\ n)$.

Расшифрование:

1. $\begin{cases} m_p \equiv \pm\sqrt{c}\ (mod\ p), \\ m_q \equiv \pm\sqrt{c}\ (mod\ q). \end{cases}$

2. Объединяем решения по КТО: $m \equiv \sqrt{\frac{B^2}{4} + c} - \frac{B}{2} (mod\ n) \equiv \begin{cases} m_p (mod\ p), \\ m_q\ (mod\ q). \end{cases}$

Получим четыре возможных значения квадратного корня из $c$. Поскольку расшифрование неоднозначно, то для выбора правильного квадратного корня необходима дополнительная информация, т.е. открытый текст должен содержать избыточные биты, например, нули в нескольких старших или младших разрядах.

Открытый показатель необратим по модулю $\varphi(n)$, поэтому протокол шифрования Рабина оказывается уязвимым по отношению к криптоанализу на основе известных открытых текстов. Например, вероятность того, что открытый текст $m$ будет расшифрован неправильно, ненулевая. Нарушитель может зашифровать некоторое сообщение $m$, а потом подать соответствующий шифртекст на расшифровывающее устройство. Если при этом результатом расшифрования будет сообщение $m'$, такое что $m^2 \equiv m'^2\ (mod\ n)$, то, вычислив НОД$(m + m', n)$, можно найти делитель числа $n$.

Задача дешифрования в протоколе Рабина эквивалентна задаче разложения на множители. Если разложение числа $n$ известно, то расшифровать шифртекст можно по определению. Обратно, возможность расшифровать любое сообщение равносильна возможности извлечь квадратный корень (найти любое из четырех значений

квадратного корня). Вычислив наибольший общий делитель суммы (или разности) двух корней и числа $n$, получим нетривиальный делитель $n$.

**Протокол 2.** Схема подписи Рабина.

Вход отправителя. Простые делители $p$ и $q$ числа $n$.

Вход получателя. Составное число $n$.

Для формирования подписи для сообщения $m$ отправитель выполняет следующие действия.

1. Вырабатывает случайное число $r$ и вычисляет $t \equiv h(m||r)(mod\ n)$, где $h$ – хэш-функция.
2. Проверяет, является ли $t$ квадратичным вычетом по модулю $n$, для чего вычисляет символы Лежандра $\left(\frac{t}{p}\right), \left(\frac{t}{q}\right)$. Если $t$ — квадратичный невычет по модулю $n$, то возвращается на шаг 1 (генерирует новое значение $r$ и вычисляет новое $t$). В противном случае вычисляет значение $s \in (\mathbb{Z}/n\mathbb{Z})^*$ такое, что $s^2 \equiv t(mod\ n)$, а именно:
   - находит $s_p \leftarrow \sqrt{t} (\mathrm{mod}\ p)$;
   - находит $s_q \leftarrow \sqrt{t} (\mathrm{mod}\ q)$;
   - восстанавливает $s$ по китайской теореме об остатках:

$$s \leftarrow s_p q(q^{-1}\ mod\ p) + s_q p(p^{-1}\ mod\ q)\ (mod\ n).$$

Подписью для сообщения $m$ является пара $(r, s)$.

Для проверки подписи получатель выполняет следующие действия.

1. Вычисляет значение $t \leftarrow s^2\ (mod\ n)$ и $t' \equiv h(m||r)$
2. Если $t = t'$ то результат: подпись подлинная, иначе результат: подпись неверна. ■

Схема цифровой подписи Рабина подвержена атаке на основе подобранных сообщений (например, извлечение квадратного корня из 4 не требует разложения числа $n$).

## Протокол Фиата–Шамира (Fiat, Shamir)

Рассмотрим протокол аутентификации Фиата–Шамира. Доверенный центр генерирует простые числа $p \equiv q \equiv 3(mod\ 4)$, вычисляет их произведение $n$ и отправляет полученное составное число всем участникам. Разложение $n$ не должно быть известно никому, кроме доверенного центра. Затем каждый участник выбирает $k$ чисел $s_1, s_2, \dots, s_k \in (\mathbb{Z}/n\mathbb{Z})^*$ и вычисляет $v_j \equiv s_j^{-2}\ (mod\ n), \forall j = 1, \dots, k$. Тогда набор $v_i$ – открытый ключ, набор $s_i$ – закрытый ключ участника.

Пусть участник *A* хочет подтвердить личность участнику *B*. Опишем *i*-й цикл протокола аутентификации.

**Протокол 3.** Аутентификация.

| A | B |
|---|---|
| 1. $r_i \in (\mathbb{Z}/n\mathbb{Z})^*$ - случайное | 1. $\tilde{e} = (e_1, e_2, \dots, e_k), e_j \in \{0,1\}$. |
| 2. $x_i \equiv r_i^2\ (mod\ n)$. | 2. Отправляет $e_i$ участнику A. |
| 3. Отправляет $x_i$ участнику B | |
| 4. $y_i \equiv r_i (s_1^A)^{e_1} (s_2^A)^{e_2} \dots (s_k^A)^{e_k} (mod\ n)$ | |
| 5. Отправляет $y_i$ участнику B. | |
| | 3. $z_i \equiv y_i^2 v_1^{e_1} v_2^{e_2} \dots v_k^{e_k}\ (mod\ n)$. |
| | 4. Проверяет $z_i \equiv x_i\ (mod\ n)$. Если выполняется – переход на следующий шаг. |

Если равенство выполняется для $\forall i = 1,2, \dots, k$, то участник *A* проходит аутентификацию.

Общим открытым ключом здесь является составное число $n = pq$; личным секретным ключом — набор элементов $s_0, \dots, s_{k-1}$ кольца $\mathbb{Z}/n\mathbb{Z}$; личным открытым ключом — набор элементов $v_0, \dots, v_{k-1}$ кольца $\mathbb{Z}/n\mathbb{Z}$ таких, что $v_i \equiv s_i^{-2} (mod\ n)$. В отличие от RSA здесь можно использовать общий модуль $n$, при этом ни один из участников не должен знать разложение числа $n$.

**Протокол 4.** Схема подписи Фиата–Шамира.

Вход отправителя. Составное число $n$; $s_1, \ldots, s_k \in (\mathbb{Z}/n\mathbb{Z})^*$.

Вход получателя. Составное число $n$; $v_1, \ldots, v_k \in (\mathbb{Z}/n\mathbb{Z})^*$, где $v_i \equiv s_i^{-2} (mod\ n)$.

Для формирования подписи для сообщения $m$ отправитель выполняет следующие действия.

1. Выбирает произвольное целое число $r$, $1 < r < n - 1$.
2. Полагает $x \leftarrow r^2 \pmod n$.
3. Вычисляет хэш-функцию от аргумента, представляющего собой конкатенацию чисел $m$ и $x$: $\tilde{e} \leftarrow h(m||x)$, и представляет полученное значение в виде двоичного вектора $(e_1, \ldots, e_k)$.
4. Вычисляет $y \leftarrow r \prod_{i=1}^{k} s_i^{e_i} (mod\ n)$.

Подписью для сообщения $m$ является пара $(\tilde{e}, y)$.

Для проверки подписи получатель выполняет следующие действия.

1. Представляет число $\tilde{e}$ в виде двоичного вектора $(e_1, \ldots, e_k)$.
2. Вычисляет $z \leftarrow y^2 \prod_{i=1}^{k} v_i^{e_i} (mod\ n)$.
3. Полагает $e \leftarrow h(m||z)$.
4. Проверяет равенство $e = \tilde{e}$. Если оно выполняется, то результат: подпись подлинная, иначе результат: подпись недействительна. ■

Безопасность этой схемы подписи основана на сложности извлечения корня в кольце $\mathbb{Z}/n\mathbb{Z}$. При этом число $n$ должно вырабатываться доверенной стороной. Для того чтобы каждый пользователь системы мог убедиться в том, что число $n$ выбрано правильно, в криптосистеме необходимо предусмотреть процедуру доказательства того, что число $n$ является произведением двух различных простых чисел.

## Контрольные вопросы

1. В схеме подписи Рабина оцените вероятность выбора $r$ такого, что $t$ является квадратичным вычетом по модулю $n$.

2. Объясните, почему для некоторых криптосистем удобно выбирать $n = pq$, где $p \equiv q \equiv 3(mod\ 4)$.

3. Почему в схеме Фиата–Шамира разные участники могут использовать один и тот же модуль?

## Литература

1. Menezes A., van Oorschot P., Vanstone S. Handbook of applied cryptography. — CRC Press, 1996. http://cacr.uwaterloo.ca/hac/

2. Мао В. Шифрование — асимметричные методы // Современная криптография: Теория и практика — М.: Вильямс, 2005. — 768 с. — ISBN 978-5-8459-0847-6

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — 816 с. — 3000 экз. — ISBN 5-89392-055-4.