Задача шифрования. В общем задача выглядит так: есть Алиса и Боб, которые хотят передавать друг другу информацию таким образом, чтобы их сообщение можно было перехватить, но перехвативший человек не понял бы, что в нем написано. Дальше будем считать, что канал между Алисой и Бобом прослушивается Евой. В принципе, Евой может быть кто угодно, потому что каналы публичные. Причем, даже если Ева прочитает и расшифрует сообщение, Алиса с Бобом даже не узнают про это.

Схема RSA. Пусть у Алисы и Боба было по два объекта: публичный и приватный ключ. Ключ — это просто какой-то шифровальный объект. При этом ключи взаимообратимы, но для каждого из них по отдельности найти обратную функцию сложно, то есть $M = private(public(M)) = public(private(M))$. Если все участники знают публичные ключи, то обмен можно провести таким образом: Алиса произносит $public_B(M)$, тогда Боб делает $private_B(public_B(M)) = M$.

Факты для RSA:

- $\forall a, n: \ a^{\phi(n)} \equiv 1 \pmod{n}$
- $(a, b) = 1 \to \phi(ab) = \phi(a)\phi(b)$
- Можно проверить число на простоту за $O(\log^k n)$
- Нельзя посчитать факторизацию n за $O(\log^k n)$. Этот факт не доказан человечеством.

Зафиксируем два простых ключа p_1, p_2. Их произведение равно n. Мы знаем, чему равно $\phi(n)$ — это $(p_1 - 1)(p_2 - 1)$. При этому быстро посчитать $\phi(n)$ нельзя по факту 4.

Нашим публичным ключом будет пара (e, n), приватным ключом будет пара (d, n). e и d — это такие числа, что $ed \equiv 1 \pmod{\phi(n)}$. Тогда $M^{ed} = M$. Тогда Алиса сначала фиксирует какое-то e, взаимно простое с $\phi(n)$. Тогда Алиса может решить диофантово уравнение $ed + \phi(n)m = 1$, получая d.

Теперь пусть все знают e. Тогда Алиса посылает M^e, Боб делает $M^e d = M^{\phi(n)k+1} = M$.

Man in the middle и authority. На самом деле, описанный выше не работает, если у нам есть Мэллори, которая читает и модифицирует канал связи между Алисой и Бобом. Мэллори может выдать им свои публичные ключи в качестве публичного ключа друг друга. Тогда Мэллори будет явно читать весь канал между Алисой и Бобом, причем поскольку она знает публичные ключи Алисы и Боба, она может отправлять им что угодно.

Таким образом, мы хотим решить следующую задачу: получить публичный ключ, которому можно доверять.

Мы предположим, что у нас есть добрый Трент, которому все стороны доверяют, и публичный ключ которого известен всем. Тогда все могут сообщить Тренту свои публичные ключи и спросить у Трента чужие публичные ключи.

Цифровая подпись. Для того, чтобы все точно верили, что сообщение отправляет именно Трент, он может отправить пару $(M, private(M))$. Это называется цифровой подписью Трента. Теперь наши участники запрашивают сертификат у Трента, а Трент в качестве сертификата выдает Алисе свою цифровую подпись для этого ключа. То есть теперь Алиса может отправлять свой публичный ключ, представляясь Алисой, которую одобрил Трент.