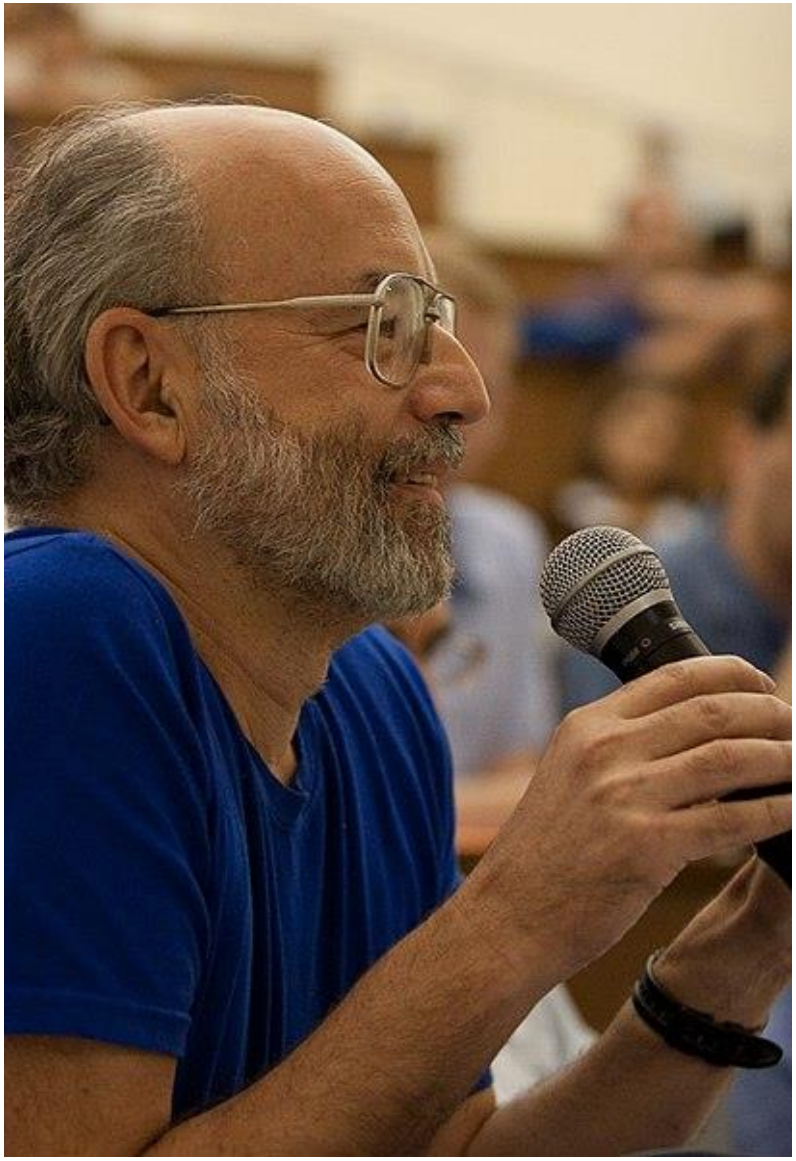
Шифр Шамира



~ 1980 г.

Ади Шамир (Adi Shamir)

описал трехэтапный протокол обмена зашифрованными сообщениями.

Описание алгоритма

Перейдем к описанию системы. Пусть есть два абонента A и B, соединенные линией связи. A хочет передать сообщение m абоненту B так, чтобы никто не узнал его содержание. A выбирает случайное большое простое число p и открыто передает его B. Затем A выбирает два числа c_A и d_A, такие, что

$$c_A d_A \bmod (p-1) = 1. \tag{2.17}$$

Эти числа A держит в секрете и передавать не будет. B тоже выбирает два числа c_B и d_B, такие, что

$$c_B d_B \bmod (p-1) = 1, \tag{2.18}$$

и держит их в секрете.

После этого A передает свое сообщение m, используя трехступенчатый протокол. Если $m < p$ (m рассматривается как число), то сообщение m передается сразу , если же $m \geq p$, то сообщение предствляется в виде $m_1, m_2, \ldots, m_t$, где все $m_i < p$, и затем передаются последовательно $m_1, m_2, \ldots, m_t$. При этом для кодирования каждого m_i лучше выбирать случайно новые пары (c_A, d_A) и (c_B, d_B) — в противном случае надежность системы понижается.

В настоящее время такой шифр, как правило, используется для передачи чисел, например, секретных ключей, значения которых меньше p. Таким образом, мы будем рассматривать только случай $m < p$. Дадим описание протокола.

Шаг 1. A вычисляет число

$$x_1 = m^{c_A} \bmod p, \tag{2.19}$$

где m — исходное сообщение, и пересылает x_1 к B.

Шаг 2. B, получив x_1, вычисляет число

$$x_2 = x_1^{c_B} \bmod p \tag{2.20}$$

и передает x_2 к A.

Шаг 3. A вычисляет число

$$x_3 = x_2^{d_A} \bmod p \tag{2.21}$$

и передает его B.

Шаг 4. B, получив x_3, вычисляет число

$$x_4 = x_3^{d_B} \bmod p. \tag{2.22}$$

Утверждение 2.10 (свойства протокола Шамира).

1) *$x_4 = m$, т.е. в результате реализации протокола от A к B действительно передается исходное сообщение;*

2) *злоумышленник не может узнать, какое сообщение было передано.*

Доказательство. Вначале заметим, что любое целое число $e \geq 0$ может быть представлено в виде $e = k(p-1) + r$, где $r = e \bmod (p-1)$. Поэтому на основании теоремы Ферма

$$x^e \bmod p = x^{k(p-1)+r} \bmod p = \\ = (1^k \cdot x^r) \bmod p = x^{e \bmod (p-1)} \bmod p. \quad (2.23)$$

Справедливость первого пункта утверждения вытекает из следующей цепочки равенств:

$$\begin{aligned} x_4 &= x_3^{d_B} \bmod p = (x_2^{d_A})^{d_B} \bmod p = \\ &= (x_1^{c_B})^{d_A d_B} \bmod p = (m^{c_A})^{c_B d_A d_B} \bmod p = \\ &= m^{c_A d_A c_B d_B} \bmod p = m^{(c_A d_A c_B d_B) \bmod (p-1)} \bmod p = m \end{aligned}$$

(предпоследнее равенство следует из (2.23), а последнее выполняется в силу (2.17) и (2.18)).

Доказательство второго пункта утверждения основано на предположении, что для злоумышленника, пытающегося определить m, не существует стратегии более эффективной, чем следующая. Вначале он вычисляет c_B из (2.20), затем находит d_B и, наконец, вычисляет $x_4 = m$ по (2.22). Но для осуществления этой стратегии злоумышленник должен решить задачу дискретного логарифмирования (2.20), что практически невозможно при больших p.

Опишем метод нахождения пар c_A, d_A и c_B, d_B, удовлетворяющих (2.17) и (2.18). Достаточно описать только действия для абонента A, так как действия для B совершенно аналогичны. Число c_A выбираем случайно так, чтобы оно было взаимно простым с $p-1$ (поиск целесообразно вести среди нечетных чисел, так как $p-1$ четно). Затем вычисляем d_A с помощью обобщенного алгоритма Евклида, как это было объяснено в разд. 2.3.

Пример 2.15. Пусть A хочет передать B сообщение $m = 10$. A выбирает $p = 23$, $c_A = 7$ $(\gcd(7, 22) = 1)$ и вычисляет $d_A = 19$. Аналогично, B выбирает параметры $c_B = 5$ (взаимно простое с 22) и $d_B = 9$. Переходим к протоколу Шамира.

Шаг 1. $x_1 = 10^7 \bmod 23 = 14$.

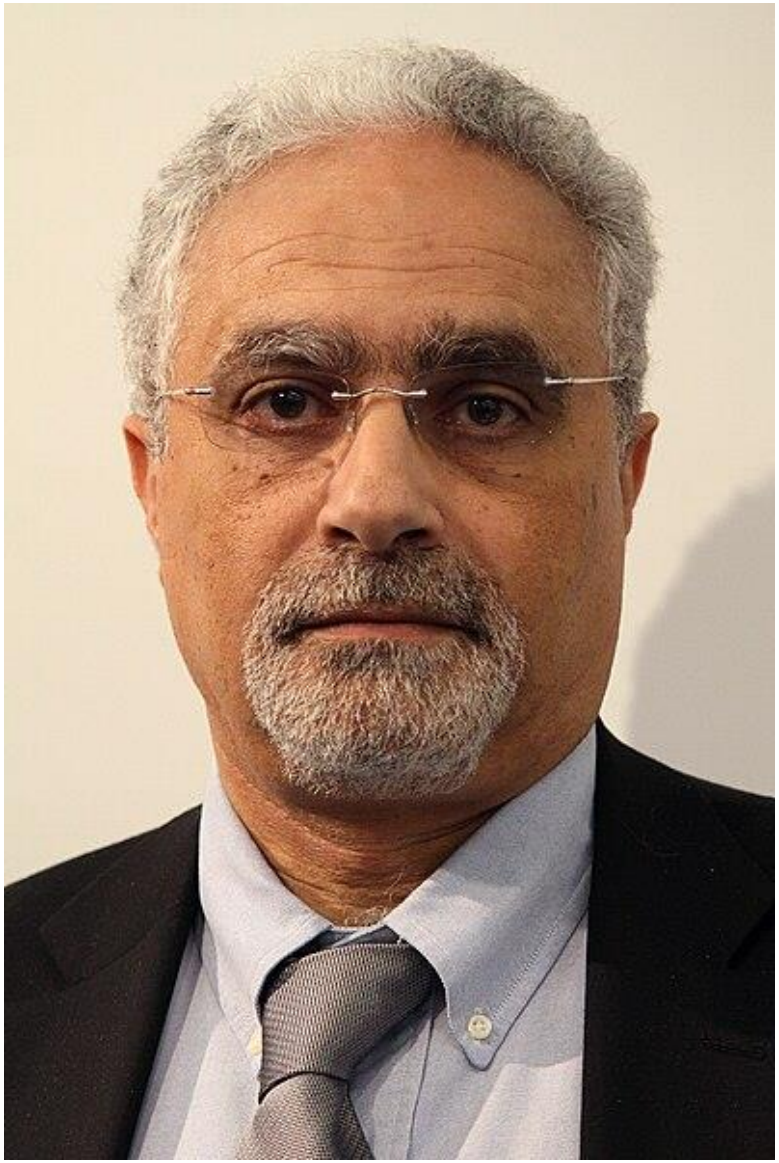
Шаг 2. $x_2 = 14^5 \bmod 23 = 15$.

Шаг 3. $x_3 = 15^{19} \bmod 23 = 19$.

Шаг 4. $x_4 = 19^9 \bmod 23 = 10$.

Таким образом, B получил передаваемое сообщение $m = 10$.

Шифр Эль-Гамаля



1985 г.

Тахер Эль-Гамаль

(Taher ElGamal)

предложил криптосистему с открытым ключом

Описание алгоритма

Абоненты A, B , C , . . . , хотят передавать друг другу зашифрованные сообщения, не имея никаких защищенных каналов связи

Шифр, предложенный Эль-Гамалем, решает эту задачу, используя, в отличие от шифра Шамира, только одну пересылку сообщения.

Фактически здесь **используется схема Диффи–Хеллмана**, чтобы сформировать общий секретный ключ для двух абонентов, передающих друг другу сообщение, и затем сообщение шифруется путем умножения его на этот ключ.

Для каждого следующего сообщения секретный ключ вычисляется заново.

Для всей группы абонентов выбираются некоторое большое простое число **p** и число **g**, такие, что различные степени **g** суть различные числа по модулю **p**.

Числа **p** и **g** передаются абонентам в открытом виде (они могут использоваться всеми абонентами сети).

Затем каждый абонент группы выбирает свое секретное число c_i, $1 < c_i < p-1$, и вычисляет соответствующее ему открытое число d_i,

$$d_i = g^{c_i} \bmod p. \qquad (2.24)$$

Абонент	Секретный ключ	Открытый ключ
A	c_A	d_A
B	c_B	d_B
C	c_C	d_C

Покажем теперь, как A передает сообщение m абоненту B. Будем предполагать, как и при описании шифра Шамира, что сообщение представлено в виде числа $m < p$.

Шаг 1. A формирует случайное число k, $1 \le k \le p-2$, вычисляет числа

$$r = g^k \bmod p, \tag{2.25}$$

$$e = m \cdot {d_B}^k \bmod p \tag{2.26}$$

и передает пару чисел (r, e) абоненту B.

Шаг 2. B, получив (r, e), вычисляет

$$m' = e \cdot r^{p-1-c_B} \bmod p. \tag{2.27}$$

Утверждение 2.11 (свойства шифра Эль-Гамаля).

1) *Абонент B получил сообщение, т.е. $m' = m$;*

2) *противник, зная p, g, d_B, r и e, не может вычислить m.*

Доказательство. Подставим в (2.27) значение e из (2.26):

$$m' = m \cdot {d_B}^k \cdot r^{p-1-c_B} \bmod p.$$

Теперь вместо r подставим (2.25), а вместо d_B — (2.24):

$$m' = m \cdot (g^{c_B})^k \cdot (g^k)^{p-1-c_B} \bmod p =$$
$$= m \cdot g^{c_B k + k(p-1) - k c_B} \bmod p = m \cdot g^{k(p-1)} \bmod p.$$

По теореме Ферма

$$g^{k(p-1)} \bmod p = 1^k \bmod p = 1,$$

и, таким образом, мы получаем первую часть утверждения.

Для доказательства второй части заметим, что противник не может вычислить k в равенстве (2.25), так как это задача дискретного логарифмирования.

Следовательно, он не может вычислить m в равенстве (2.26), так как m было умножено на неизвестное ему число.

Противник также не может воспроизвести действия законного получателя сообщения (абонента B), так как ему не известно секретное число c_B (вычисление c_B на основании (2.24) — также задача дискретного логарифмирования).

Пример 2.16. Передадим сообщение $m = 15$ от A к B. Выберем параметры аналогично тому, как это было сделано в примере 2.2 стр. 20. Возьмем $p = 23$, $g = 5$. Пусть абонент B выбрал для себя секретное число $c_B = 13$ и вычислил по (2.24)

$$d_B = 5^{13} \bmod 23 = 21.$$

Абонент A выбирает случайно число k, например $k = 7$, и вычисляет по (2.25), (2.26):

$$r = 5^7 \bmod 23 = 17, \quad e = 15 \cdot 21^7 \bmod 23 = 15 \cdot 10 \bmod 23 = 12.$$

Теперь A посылает к B зашифрованное сообщение в виде пары чисел $(17, 12)$. B вычисляет по (2.27)

$$m' = 12 \cdot 17^{23-1-13} \bmod 23 = 12 \cdot 17^9 \bmod 23 = 12 \cdot 7 \bmod 23 = 15.$$

Мы видим, что B смог расшифровать переданное сообщение.