Московский физико-технический институт

Улучшения алгоритма Эль-Гамаля

выполнила студентка Б01-907 группы ФРКТ

Широкова Ксения

Аннотация : *С широким применением алгоритма Эль-Гамаля его безопасность обычно подвергается сомнению, и проблема становится все более серьезной. В данной статье будут рассмотрены исследования связанные с повышением устойчивости алгоритма Эль-Гамаля к выбранным атакам. А именно: улучшение для защиты от атаки подобранного шифротекста, устранение уязвимости схемы подписи Эль-Гамаля, в которой используется только одно случайное число и схема подписи Эль-Гамаля на конических кривых.*

Долгопрудный, 2022 г.

Базовый алгоритм

Для начала рассмотрим схему базового алгоритма Эль-Гамаля для работы в режиме шифрования и дешифрования и в режиме подписи и проверки подписи.

Алгоритм генерации ключей

- Выбирается случайное простое число p.
- Выбирается целое число g такое, что $g^{\phi\ (p)} \equiv 1 \pmod{p}$.
- Вычисляется $y = g^x \pmod{p}$.
- Открытым ключом является (y, g, p), закрытым ключом является число x.

Работа в режиме шифрования

M - сообщение, M меньше числа p

Шифрование :

- Выбирается случайное целое число k - сессионный ключ, взаимно простое с (p - 1), такое, что 1 < k < p - 1.
- Вычисляются числа $a = g^k \pmod{p}$ и $b = y^k M \pmod{p}$.
- Шифротекстом является пара чисел (a, b).

Расшифрование :

- Зная закрытый ключ x, получатель может вычислить исходное сообщение из шифротекста (a, b) по формуле: $M = b * (a^x)^{-1} \pmod{p}$.

- При этом можно проверить, что: $(a^x)^{-1} = g^{-kx} \pmod{p}$
  Тогда верно, что
  $b * (a^x)^{-1} = (y^k * M) * g^{-xk} \equiv (g^{xk} * M)g^{-xk} \equiv M \pmod{p}$.

Работа в режиме цифровой подписи

При работе в режиме цифровой подписи предполагается, что используется хэш-функция h(), значения которой лежат в интервале от 1 до p - 1.

Подпись:

- Вычисляется дайджест сообщения M: m = h(M).
- Выбирается случайное число 1 < k < p - 1 взаимно простое с p - 1 и вычисляется $r = g^k \pmod{p}$
- Вычисляется число $s = (m - x * r)k^{-1} \pmod{p-1}$, где k^{-1} это обратное k по модулю p - 1.
- Пара чисел (r, s) является подписью.

Проверка:

- Если не выполняется 0 < r < p и 0 < s < p - 1, то подпись недействительна
- Подпись считается верной, если выполняется сравнение: $y^r r^s \equiv g^m \pmod{p}$.

Корректность проверки

- Из определения s имеем $m \equiv xr + sk \pmod{p-1}$.
- Из малой теоремы Ферма: $g^m \equiv g^{xr} * g^{ks} \equiv (g^x)^r * (g^k)^s \equiv (y)^r * (r)^s \pmod{p}$.

Улучшение алгоритма Эль-Гамаля в режиме шифрования и дешифрования для защиты от атаки на основе подобранного шифротекста

Криптосистема Эль-Гамаля - это криптосистема с открытым ключом, поэтому злоумышленник может использовать атаку подобранного шифротекста на криптосистему Эль-Гамаля без знания закрытого ключа.

Атака на основе подобранного шифротекста

Для начала рассмотрим алгоритм данной атаки.

- Шифротекст, перехваченный злоумышленником - $C = (a, b) = (g^k, M * y^k)$
- Злоумышленник выбирает k' и M' случайным образом и вычисляет
  $C' = (g^k * g^{k'}, b^k * M * b^{k'} * M') = (g^{k+k'}, (M * M') * b^(k + k'))$
- В функцию расшифрования подается C', и возвращается M"
- Теперь из M" можно получить M :
  $C'' = (M * M') * b^{k+k'}$
  $M'' = M * M'$
  $M = M'' * M'^{-1}$

Предложенное улучшение схемы Эль-Гамаля

Допустим, нам нужно зашифровать сообщение M. Закрытый и открытый ключ аналогичны ключам базового алгоритма. Структура зашифрованного текста C изменилась в улучшенной системе.

Шифрование:

- Запишем M как $M = p_1 p_2 ... p_i$, где p_i - простые числа, (0 < i < p).
- Вычислим $n = i * y^k \pmod p$ и $b = M^i$
- Отправляем (a, b, n)

Расшифрование:

- Вычисляем $a^x \pmod p = y^k$
- Вычислим $i = \frac{n}{a^x \pmod p}$
- $M = b^{1/i}$

Корректность:
$c^{\frac{a^x modp}{n}} = c^{\frac{g^{k*x} modp}{i*y^k modp}} = c^{\frac{g^{k*x} modp}{i*g^{x*k} modp}} = c^{1/i}$

Устойчивость к выбранной атаке

Теперь злоумышленник получает зашифрованный текст C = (a, b, n). Злоумышленник выбирает значения k', M' и t случайным образом. (Согласно предыдущей атакой на криптосистему с открытым ключом Эль-Гамаля, злоумышленник выбирает только два случайных значения. С двумя значенями он никогда не сможет атаковать эту расширенную систему. Итак, атакующий выбирает 3 значения для атаки на эту расширенную систему).
$C = (a, b, n) = (g^{k\prime}, M^i, i * y^k modp)$
Теперь $C' = (g^{k\prime} * g^t, M^i * M'^t, y^k modp * t * y^{k\prime} modp)$
$C' = (g^{k+k'}, M^i * M'^{k\prime}, (i * t) * (y^k modp) * (y^{k\prime} modp))$
Теперь из функции расшифрования возвращается M".
$M'' = M^i * M'^t$
$M = (\frac{M''}{M'^t})^{1/i}$
Значение i злоумышленнику неизвестно, следовательно, он не может вычислить M из M".

Схема цифровой подписи Эль-Гамаля на эллиптической кривой над кольцом Z_n

Схема Эль-Гамаля основана на задаче дискретного логарифмирования (DLP). Безопасность RSA основана на проблеме факторизации больших целых чисел (IFP). Рассмотрим улучшение схемы цифровой подписи типа Эль-Гамаля, основанное на конической кривой над кольцом Zn, которая превращает исходную схему цифровой подписи, основанную на одной сложной математической задаче, в основанную на двух сложных математических задачах. Следовательно, улучшенная схема более безопасна, чем исходная схема.

Выбор параметров

Выберем эллиптическую кривую с уравнением $C_n(a, b) : y^2 \equiv ax^2 - bx(\mathrm{mod}\ n)$,
где n = p * q, a и b $\in Z_n$,такие, что (a, n) = (b, n) = 1, p и q - два больших простых числа, такие, что $\frac{a}{p} = \frac{a}{p} = -1$ и p + 1 = 2r, q + 1 = 2s. По определению порядок кривой: $N_n = 2rs$ Начальная точка кривой: $G = (G_x, G_y)$. Случайным образом выбираем d $\in Z_{Nn}*$. Считаем $Q = dG(modn) \neq (0, 0)$. H(m) - хэш сообщения m. Публичный ключ n, a, b, Q, g. Приватный ключ - d и N_n

Алгоритмы подписи и проверки

Подпись:

- Случайным образом выбираем k и считаем
  $kG(\mathrm{mod}\ n) \equiv (x_1, y_1), \gamma \equiv x_1(\mathrm{mod}\ N_n)$(если $\gamma = 0$, то выбираем другое k)
- Вычисляем $R \equiv k\gamma G(\mathrm{mod}\ n)$
- Вычисляем $\delta \equiv (dH(\mathrm{m}) - k\gamma^2)(\mathrm{mod}\ N_n)$
- Отправляем (m, R, γ, δ) в качестве подписи сообщения m

Проверка подписи:

- После получения подписи (m, R, γ, δ) получатель вычисляет $U \equiv H(m)Q(\mathrm{mod}\ n), X \equiv \delta G(\mathrm{mod}\ n), Y \equiv R(\mathrm{mod}\ n)$
- Если среди этих значений есть (0, 0), то подпись недействительна
- Если верно, что $X \oplus Y = U$, то подпись действительна, иначе - недействительна

Корректность проверки :
$X \oplus Y(\mathrm{mod}n) \equiv \delta G \oplus R(\mathrm{mod}n) \equiv (dH(\mathrm{m}) - \gamma)G \oplus R(\mathrm{mod}n) \equiv$
$\equiv (dH(\mathrm{m}) - \gamma)G \oplus \gamma G(\mathrm{mod}n) \equiv dH(\mathrm{m})G(\mathrm{mod}n) \equiv H(\mathrm{m})Q(\mathrm{mod}n) \equiv U$

Симуляция атак

- Если злоумышленник хочет подделать подпись сообщения $\delta = (dH(\mathrm{m}) - \gamma)(\mathrm{mod}\ N_n)$, он должен получить N_n. Предположим, что злоумышленник способен решить проблему целочисленной факторизации, значит он может разложить n на p и q, а следовательно, узнает параметр N_n. Однако, так как мы знаем сложность вычисления дискретного логарифма конической кривой, злоумышленник все еще не может получить приватный ключ d, зная публичный ключ $Q \equiv dG(\mathrm{mod}\ n)$.
- Если злоумышленник умеет вычислять дискретный логарифм конической кривой, предполагаем, что у него есть приватный ключ d из публичного ключа $Q \equiv dG(\mathrm{mod}\ n)$. Чтобы подделать подпись, ему нужно вычислить значение $\delta = (dH(\mathrm{m}) - \gamma)(\mathrm{mod}\ N_n)$. Так как ему не известен параметр N_n, злоумышленнику нужно разложить n на p и q, то есть решить проблему целочисленной факторизации.

Приведенные выше смоделированные атаки показывают, что новая схема цифровой подписи очень безопасна в случае невозможности решения двух сложных математических задач одновременно.

Улучшенный алгоритм Эль-Гамаля на основе добавления случайного числа

С точки зрения схемы цифровой подписи Эль-Гамаля безопасность алгоритма зависит от безопасности закрытого ключа x. Как только закрытый ключ x перехвачен хакером, весь алгоритм цифровой подписи становится доступным для всех, и никакой защиты не существует. Хакер может легко использовать связь между случайными числами, и он получит значение закрытого ключа x без сложных вычислений.

Таким образом, в алгоритме цифровой подписи Эль-Гамаля незащищенное случайное число представляет собой очень большую угрозу его безопасности. Рассмотрим улучшение алгоритма цифровой подписи Эль-Гамаля путем добавления случайного числа и усложнения связи между случайным числом и закрытым ключом для затруднения расшифровки.

Алгоритмы подписи и проверки подписи

Подпись :

- Выбирается большое число p, α - генератор $\mathrm{Zp}^*, \mathrm{x}(1 < x < \varphi(p))$ - приватный ключ, соответствующий публичный ключ может быть вычислен как $\beta = \alpha^x \bmod p$
- Выбираются два случайных числа t и k, где t и k взаимно простые и существуют обратные к ним числа. Вычисляем $\gamma = \alpha^k \bmod p, \lambda = \alpha^t \bmod p$
- M, δ вычисляются с использованием результатов первых двух шагов, а также расширенного алгоритма Евклида и алгоритма модулярной инверсии $M = (x\gamma + k\lambda + t\delta) \bmod (p-1)$
- Отбрасываются случайные числа k и t, после чего получаются требуемые открытые ключи p, β и α. Закрытый ключ — x. Подпись открытого текста M — $(\gamma, \lambda, \delta)$.

Проверка :

- $(\gamma, \lambda, \delta)$ отправляется системой соответствующим клиентам.
- Клиенты используют следующее уравнение для проверки правильности цифровых подписей открытого текста M:
  $\alpha^M = \beta^\gamma \gamma^\lambda \lambda^\delta \bmod p$
- Если равенство верно, то подпись считается корректной, в противном случае подпись неверна или была ошибка передачи.

Симуляции атак на улучшенный алогоритм

- Если для подписи используется схема цифровой подписи Эль-Гамаля с добавлением случайного числа, то на начальном этапе хакер может вычислить множество значений закрытого ключа x, как описано выше, и определить закрытый ключ, но он не может вычислить два случайных числа k и t путем шифрования уравнения на следующем шаге. Уравнение шифрования выглядит следующим образом: $M = (x\gamma + k\lambda + t\delta) \bmod (p-1)$. Точно так же хакер не сможет использовать $\gamma = \alpha^k \bmod p, \lambda = \alpha^t \bmod p$ для проверки правильности закрытого ключа x, который был известен. Поэтому в улучшенной схеме цифровой подписи Эль-Гамаля хакер не может атаковать следующую формулу: $M = (x\gamma + k\lambda + t\delta) \bmod (p-1)$
- Таким образом, основная атака будет сосредоточена на уравнении проверки цифровой подписи. Однако уравнение проверки алгоритма после добавления случайного числа выглядит следующим образом: $\alpha^M = \beta^\gamma \gamma^\lambda \lambda^\delta \bmod p$. δ рассчитывается следующим образом: $\lambda^\delta = \alpha^m \beta^{-\gamma} \gamma^{-\lambda} \pmod p$. Сравнивая выражения выше, вычисление последнего явно сложнее, так как у последнего на одну инверсию больше, чем у первого. И даже при успешном взломе значение выбранных файлов или сообщений M является известной величиной в процессе расчета, поэтому результаты расчета могут быть использованы только для подписи этого документа или сообщения. Ценность этих атак явно снижена.
- Для улучшенных алгоритмов, по сравнению со многими традиционными алгоритмами цифровой подписи, хакер все еще может легко получить доступ к подписи подписавшего (γ, δ) сообщения или документа M, а затем подделать ряд законных цифровых подписей.

Поскольку для улучшенного алгоритма введено больше параметров, вероятность того, что мы захотим адаптировать файл M', может быть уменьшена естественным образом. Даже если способ подделки подписи будет найден, атака на него будет более сложной, чем на алгоритм цифровой подписи Эль-Гамаля. Действительная подпись, полученная таким образом, по-прежнему соответствует значению M.

Методы атаки с добавлением подписанных данных сложнее построить. Его вычисление намного больше, даже если оно удастся. Но настоящие трудности для хакера по-прежнему представляют собой действующую подпись, которая была подделана в то же время, а также производила соответствующее значение M'. Злоумышленник может успешно найти соответствующее значение M'. Хакер, атакующий таким образом, должен иметь очень большую вычислительную способность.

Вывод

Таким образом, были рассмотрены возможные атаки на алгоритм подписи и шифрования Эль-Гамаля и улучшения, повышающие защищенность системы от выбранных атак. Рассмотренные алгоритмы с точки зрения безопасности были значительно улучшены, что делает их область применения достаточно широкой.

Источники

- Статья "Схема Эль-Гамаля"на https://ru.wikipedia.org/wiki/
- Dissanayake W. An Improvement of the Basic El-Gamal Public Key Cryptosystem //International Journal of Computer Applications Technology and Research. – 2018. – Т. 7. – №. 02. – С. 40-44.
- Bai C. X. et al. A new digital signature scheme of ElGamal type on conic curve over the ring Z n //2010 International Conference on Computer Application and System Modeling (ICCASM 2010). – IEEE, 2010. – Т. 11. – С. V11-378-V11-381.
- Xiao-fei L., Xuan-jing S., Hai-peng C. An improved ElGamal digital signature algorithm based on adding a random number //2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing. – IEEE, 2010. – Т. 2. – С. 236-240.