КРИПТОСИСТЕМА ЭЛЬ-ГАМАЛЯ

ПОДГОТОВИЛ СТУДЕНТ 2 КУРСА НИУ ВШЭ

СИДОРЕНКОВ ОЛЕГ, БПИ204

ПЛАН ПРЕЗЕНТАЦИИ

- Дискретное логарифмирование с примерами
- Протокол Диффи — Хеллмана с примерами
- История создания схемы Эль-Гамаля
- Алгоритм Эль-Гамаля
- Примеры шифрования / расшифрования
- Интересные факты

ДИСКРЕТНОЕ ЛОГАРИФМИРОВАНИЕ

Пусть есть конечная абелева группа G
Пусть есть элемент $b \in G$
Пусть есть $y \in G$
Рассмотрим уравнение $y = b^x$
Если оно разрешимо, то $\exists x < ord(G), x \in N$
Пример:
Рассмотрим группу Z_5
$b = 3$
$y = 2$
$2 = 3^x \bmod 5$
$b^3 = 27 \bmod 5 = 2$
$x = 3$

ПРОТОКОЛ ДИФФИ-ХЕЛЛМАНА

Протокол Диффи-Хеллмана — криптографический протокол (набор крипто-алгоритмов), позволяющий двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи. Полученный ключ используется для шифрования дальнейшего обмена с помощью алгоритмов симметричного шифрования.

Алгоритм:

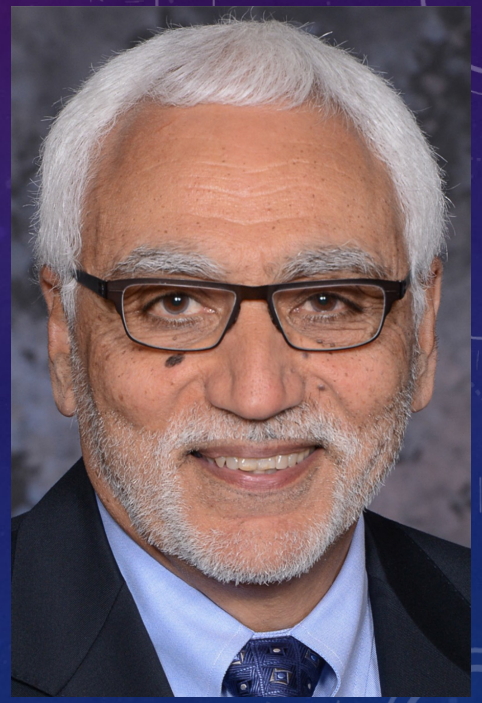
Пусть есть 2 пользователя: Алиса и Боб
Возьмём 2 общеизвестных числа g и p
Оба человека генерируют 2 больших неизвестных никому случайных числа a и b соответственно
Алиса находит остаток от деления:
$A = g^a \bmod p$
Далее пересылает результат Бобу
Боб тоже вычисляет остаток от деления:
$B = g^b \bmod p$
Передаёт Алисе
Оба этих значения могут передаваться по незащищённому каналу связи
Алиса повторяет свои действия с новым числом B:
$C = B^a \bmod p = g^{ab} \bmod p$
Боб всё делает зеркально:
$C = A^b \bmod p = g^{ab} \bmod p$
У обоих получилось одно и тоже число C, которое и является ключом. Его будет трудно найти за конечное время
P. S. Фактически, мы работали в поле F_p

ПРИМЕР АЛГОРИТМА

Возьмём числа p = 23 и g = 5
Алиса и Боб сгенерировали числа a = 6 и b = 15
A = 5^6 mod 23 = 8
B = 5^{15} mod 23 = 19
У Алисы K = 19^6 mod 23 = 2
У Боба K = 8^{15} mod 23 = 2

ИСТОРИЯ ШИФРА ЭЛЬ-ГАМАЛЯ

Тахер Эль-Гамаль родился в 1955 году в Каире. С детства будущий криптограф любил производить всевозможные операции над числами, поэтому не удивительно, что в будущем, во время обучения в Стенфордском университете он увлёкся линейной алгеброй.
В 1985 году опубликовал статью под названием «Криптосистема с открытым ключом и схема цифровой подписи на основе дискретных логарифмов». Эта работа в последствии была названа криптосистемой или шифром Эль-Гамаля, позднее дополнившись цифровой подписью с аналогичным названием.



Тахер Эль-Гамаль
Род. 18.06.1955, 66 лет

АЛГОРИТМ ШИФРА ЭЛЬ-ГАМАЛЯ

Шифр Эль-Гамаля – это один из способов выработки ключей Диффи-Хеллмана.

Ключи:
p – некоторое простое число
$g^{\varphi(p)} \equiv 1 \pmod p$
Так как p – простое, то $\varphi(p) = p - 1$
$g^{p-1} \equiv 1 \pmod p$
Берём $x \in (1; p - 1)$
Вычисляем $y = g^x \bmod p$
Получаем открытые ключи (y, g, p) и закрытый ключ x

Зашифровка:
Пусть есть сообщение (число) $M < p$
Выбираем ключ k, взаимно простой с $p - 1$, причём $k \in (1; p - 1)$
Вычисляем два числа a и b:
$a = g^k \bmod p$
$b = yk \cdot M \bmod p$
Пара (a, b) и является зашифрованным сообщением.

Расшифровка:
Рассмотрим формулу $M = ba^{-x} \bmod p$
Докажем её правильность
$a = g^k \bmod p \rightarrow a^{-x} = g^{-kx} \bmod p$
$b = yk \cdot M \bmod p$
$ba^{-x} = yk \cdot M \cdot g^{-kx} \bmod p$
$y = g^x \bmod p$
$ba^{-x} = g^{kx} \cdot M \cdot g^{-kx} \bmod p = M$
$M = ba^{-x} \bmod p = ba^{p-x-1} \bmod p$

ЦИФРОВАЯ ПОДПИСЬ ЭЛЬ-ГАМАЛЯ

Цифровая подпись – это элемент обмена сообщений, который может подтвердить подлинность источника. Предполагается, что у нас в распоряжении есть некая хеш-функция $h(\cdot)$, причём результаты её выполнения $\in (1, p - 1)$

Подпись сообщения:
Пусть есть сообщение M
Вычисляем хеш-сумму
$m = h(M)$
Берём случайное $k \in (1, p - 1)$
Причём k и $p - 1$ являются взаимнопростыми
Вычисляем $r = g^k \bmod p$
И $s = (m - x \cdot r) \cdot k^{-1} \bmod p - 1$
k^{-1} – это такое целое число, что $k \cdot k^{-1} = k^{-1} \cdot k = 1 \bmod p - 1$
Подписью является пара чисел (r, s)

Проверка подписи:
Сначала проверим, что
$r \in (0; p)$, а $s \in (0; p - 1)$
Если всё хорошо, вычисляем хеш-сумму $m = h(M)$
Подпись считается верной при выполнении равенства:
$y^r \cdot r^s \equiv g^m \pmod p$

Особенности данной подписи:
Главным преимуществом схемы цифровой подписи Эль-Гамаля является возможность вырабатывать цифровые подписи для большого числа сообщений с использованием только одного секретного ключа.
Нельзя допустить утечки ключа k, так как злоумышленник сможет найти секретный ключ: $x = (m - k \cdot s) \cdot r^{-1} \bmod p - 1$.
На принципе Эль-Гамаля построены стандарты цифровой подписи США и России.

ЭЛЛИПТИЧЕСКАЯ КРИПТОГРАФИЯ

Каноническое уравнение эллиптической кривой:
$y^2 = x^3 + a \cdot x + b$

Алиса хочет переслать сообщение m Бобу.
Сообщение m пересылается в виде значения x – y точки P_m
Рассмотрим точку G и эллиптическую группу $E_p(a, b)$.
Алиса генерирует закрытый ключ n_A и открытый ключ $P_A = n_A \cdot G$.
Далее она берёт случайное число k и вычисляет пару точек G_m
$G_m = (k \cdot G, P_m + k \cdot P_B)$, $P_B = n_B \cdot G$ – это открытый ключ Боба.
Сообщение успешно зашифровано, Алиса отправляет его.
Теперь попробуем дешифровать сообщение со стороны Боба.
Боб умножает первую точку на свой секретный ключ n_B и вычитает результат из второй:
$(P_m + k \cdot P_B) – n_B \cdot (k \cdot G) = P_m + k \cdot (n_B \cdot G) – n_B \cdot (k \cdot G) = P_m + k \cdot n_B \cdot G - k \cdot n_B \cdot G = P_m$
Сообщение успешно расшифровано!

ИТОГИ

Мы рассмотрели 2 крайне популярных по сей день алгоритма шифрования: шифр Эль-Гамаля и шифр с использованием эллиптических кривых.
Оба алгоритма были опубликованы практически одновременно: в 1985 году и сразу же стали очень востребованными: алгоритм Эль-Гамаля, так как был достойной и причём бесплатной альтернативой RSA, а эллиптическая криптография – за счёт своей новизны и сложности.

СПАСИБО ЗА ВНИМАНИЕ!