Петров Роман 015 группа

Timed-released crypto

Общие сведения.

Криптография с временным раскрытием (Timed-released crypto) – способ защиты информации с возможностью расшифровки сообщения лишь по прошествию определенного промжутка времени. Т. May (Тимоти Мэй) был первым, кто обратил внимание на эту проблему.

Практическое применение timed-released crypto может найти, например, в шифровании личных дневников, с последующим обнародованием, допустим через 100 лет. Если зашифровать таким образом сообщения, цель которых – перевести деньги с одного счета на другой, но с разными датами, то мы получим возможность «помесячной оплаты». И, наконец, схема шифрования с депонированием ключей может быть легко реализована на базе TRC. Таким образом, ключи будут доступны лишь по прошествию определенного промежутка времени.

Существует два подхода для создания Timed-Released Message:

- Использование так называемых «шарад с временным замком» (Time-Lock Puzzles) – задач, которые не могут быть решены без продолжительных вычислений и требуют определенного промежутка времени для нахождения ответа.
- Использование доверенных лиц, которые не открывают секрета в течение указанного срока

Каждый способ имеет свои недостатки. Так, процессорное время, необходимое дл ярешения задачи может меняться как из-за технического прогресса (более быстрые машины), научного прогресса или простого распараллеливания вычислений.

А при использовании доверенных лиц встает проблема их надежности.

Time-Lock Puzzles

Итак, создание time-lock puzzles, основано на некотором процессе вычислений, который занимает определенное время. Решение дает ключ К, которым и расшифровывается сообщение М. Поскольку мы стремимся сделать реальное время эквивалентным «компьютерному», необходимо не допустить возможности распараллеливания, поскольку в противном случае задача может быть решена в несколько раз быстрее. Ключ также должен быть достаточно большим, чтоб нельзя было его подобрать грубой атакой за время, меньшее, чем отведено по условию time-lock puzzle. Необходимо учитывать то, что шарады дают решения через $T_{действия}$, а не точно в назначенный момент.

Решения, получаемые на разных технологических элементах (на базе арсенида галия быстрее чем на базе кремния). Поэтому метод доверенных лиц предпочтительнее, когда речь идет о долгих сроках (более дешев) или при необходимости открытия точно в заданное время.

Методический вариант

Сначала рассмотрим не работающий вариант создания головоломки, полезный в методических целях, предложенный Мерклем (Mercle R. C.) (который ввел термин Time-lock puzzle):

Пусть M – сообщение и S- скорость компьютера (расшифровок в секунду). Чтобы существовала возможность расшифровать M не раньше, чем через T секунд, будем

шифровать, например, используя RC5 с ключем K длины $\mathbf{Len_K = \log_2 (2ST)}$ бит, а затем удалим ключ K. Тогда простым перебором вариантов удастся подобрать K приблизительно за T секунд (в среднем, разумеется).

Легко видеть два недостатка такой схемы:

- дает возможность распараллелить вычисления
- ключ можно найти как значительно раньше T, так и значительно позже

Метод Ривеста, Шамира и Вагнера (Rivest, Shamir, Vagner)

Пусть пользователь A хочет зашифровать сообщение M на T секунд.
Он создает число **n=pq**, где p и q – простые числа.
1) **Φ(n)= (p-1)*(q-1)**. Также A вычисляет **t= T*S**, где S количество возведений в квадрат по модулю n за секунду компьютера, который будет производить решение TLP.
2) A берет достаточно длинный ключ K (опять же чтоб его нельзя было найти грубой атакой за время T) и зашифровывает своё сообщение M ключем K, используя для этого, например, RC5.
$\mathbf{C_м = RC5(M, K)}$.
3) A берет произвольное число a (1<a<n) и создает
$\mathbf{C_k = K + a^{2t} \pmod n}$. Чтобы сделать это быстро (ведь мы знаем p и q)
$\mathbf{E = 2^t \bmod (\Phi(n))}$
$\mathbf{B = a^e \pmod n}$
4) $\mathbf{TLP = \{n, a, t, C_k, C_m\}}$; при этом параметры p и q стерты.

Решение

Поскольку K достаточно длинен по построению, искать его прямым перебором бессмысленно. Наиболее быстрым вариантом будет высчитать
$B = a^{2t}$,
Поскольку мы не знаем Φ(n)
А так как B будет высчитываться последовательно (ведь каждый раз возводится в квадрат предыдущий вариант) то распараллелить такой процесс будет невозможно. Правда стоит заметить, что существует возможность распараллелить саму операцию возведения в квадрат – но это несущественно.
Таким образом головоломка будет раскрыта лишь по прошествию определенного времени

Использование доверенных лиц

Естественный путь – использование доверенного агента, который будет хранить сообщение M до необходимой даты.

Улучшение этого метода состоит в разделении M на фрагменты, которые будут храниться у разных агентов, которые также опубликуют свои части M во время T, тем самым позволяя реконструировать сообщение. (таким образом мы уменьшаем вероятность досрочного получения сообщения подкупом)

Дальнейшее улучшение – агенты хранят лишь часть ключа (похоже на Time Lock Puzzle), что уменьшает объем хранимой информации. При этом сам шифр C=E(K, M) находится в доступном месте. После того, как все части ключа опубликованы, ключ восстанавливается и M расшифровывается.

Подход Ривеста, Шамира и Вагнера (Rivest, Shamir, Vagner)

- Агентам нет необходимости хранить никакой информации, выданной пользователем. Объем информации строго фиксирован независимо от числа попросивших об услуге.
- Главная задача агента – периодически (допустим, раз в час) опубликовывать свой так называемый секрет. Пусть «секрет», опубликовываемый i-тым агентом во время t, обозначается как S_{it}. Агент подписывает свой секрет своей цифровой подписью.
- Всё, что разрешено агенту, - отвечать на запросы вида «Вот значения Y и t – верните $C=E(S_{it}, Y)$ – Y зашифрованное личным ключем агента K_{Ri} который будет открыт во время t. Предполагается, что алгоритм шифровки защищен от атак вида «chosen message attack», т.е. по ответам на разные сообщения клиент не сможет узнать S_{it}
- Агент возвращает подписанное сообщение $M= \{I, t, t_0, E(S_{it}, Y)\}$, где I – идентификатор агента, t – время открытия, t_0- текущее время по часам агента. M зашифровано K_U клиента и подписано K_R агента.
- Кто угодно может предложить свои услуги в качестве агента без координации с другими агентами. Т. е. Последовательность секретов одного агента независима от последовательности секретов другого агента.
- Последовательность секретов, опубликовываемая агентом, должна иметь следующее свойство – из S_{it} должна легко посчитать $S_{it'}$, где $t'<t$. Поэтому достаточно узнать последний секрет, чтобы просчитать все предыдущие. Итак $S_{i(t-1)} = f(S_{it})$. Причем, функция f не должна иметь обратной, чтобы нельзя было узнать будущие ключи. (1)
- Для того, чтобы получить trc пользователь шифрует C=E(K, M) произвольным ключем K. Выбирает d агентов с id $i_1, i_2, …., i_d$ и получает от них r1, r2, ..r_d. Trc={ c, $i_1, i_2, .., i_d, r_1, r_2, …r_d$}.
- Пользователь также может выбрать ɵ порог (т.е. число агентов из d, получив S_{it} которых, можно восстановить ключ).

Агентам необходимо:

- создать последовательность S_{it}, удовлетворяющую (1)
- расшифровать своим K_R сообщение от клиента и получить y и t/
- зашифровать y S_{it} получив C
- возвратить C подписанное цифровой подпись агента и зашифрованное K_U клиента
- опубликовать S_{it} во время t

С такими требованиями вполне по силам справиться и простому устройству.

Использованная литература:

Rivest Ronald L., Shamir A., Wagner David A. Time-lock puzzle and timed-released Crypto. Manuscript, 1996. http://theory.lcs.mit.edu/~rivest/publication.html