Криптографические примитивы и протоколы

Евтушенко Н.В., Винарский Е.М.
по всем вопросам писать на vinevg2015@gmail.com

Высшая школа экономики (факультет компьютерных наук)

8 ноября 2019 г.

Содержание

Слабые места защиты информации

- Атаки на архитектуру (Криптографическая система не может быть надежнее использованных в ней отдельных алгоритмов шифрования)
- Атаки на конкретные реализации
  - Переполнение буферов
  - Не стёртая до конца секретная информация
- Атаки на сетевое оборудование
- Атаки на пользователей
- Атаки с использованием побочных каналов
- ...

Для того чтобы преодолеть систему защиты, достаточно взломать любой из ее компонентов

Мультипликативная группа

Мультипликативная группа G – непустое множество, на котором определена ассоциативная бинарная операция умножения $(*)$, причём

- Для этой операции имеется нейтральный элемент (1) такой, что $\forall a \in G : a * 1 = 1 * a = a$
- Каждый элемент a множества G имеет обратный a^{-1}, то есть такой $a * a^{-1} = a^{-1} * a = 1$

$|G|$ – порядок группы G (количество элементов в группе G)

$(G, *)$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Пример группы с операцией умножения по модулю 5

Мультипликативная группа

Мультипликативная группа G – непустое множество, на котором определена ассоциативная бинарная операция умножения $(*)$, причём

- Для этой операции имеется нейтральный элемент (1) такой, что $\forall a \in G : a * 1 = 1 * a = a$
- Каждый элемент a множества G имеет обратный a^{-1}, то есть такой $a * a^{-1} = a^{-1} * a = 1$

$|G|$ – порядок группы G (количество элементов в группе G)

$(G, *)$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Пример группы с операцией умножения по модулю 5

Можно ли построить группу с операцией умножения по модулю 4?

Мультипликативная группа (2)

Нет, нельзя, не у каждого элемента есть обратный

$(G, *)$	1	2	3
1	1	2	3
2	2	**0**	3
3	3	2	1

- Группа G – циклическая, если существует $g \in G$ такой, что группа G есть множество степеней этого элемента
- Множество натуральных чисел $\{1, \ldots, p-1\}$ с операцией умножения по модули p является группой, если и только если p – простое число

  Такая группа является циклической

Например, для группы с операцией умножения по модулю 5, $g = 2$ – образующий элемент: $\{2^1 = 2,\ 2^2 = 4,\ 2^3 = 3,\ 2^4 = 1\}$

? 5 *mod* 7

? образующий элемент в $(\{1, \ldots, 6\}, *)$

Криптографические примитивы

- Алгоритмы симметричного шифрования
- Алгоритмы ассимметричной криптографии (выработка общих сессионных ключей и т.д.)
- Датчик псевдослучайных чисел
- Алгоритмы хэширования

В этом блоке считаем, что все криптографические примитивы не могут быть скомпрометированы раньше, чем перестанут использоваться

Какие достоинства и недостатки асимметричной криптографии?

Протокол (алгоритм) Диффи-Хеллмана

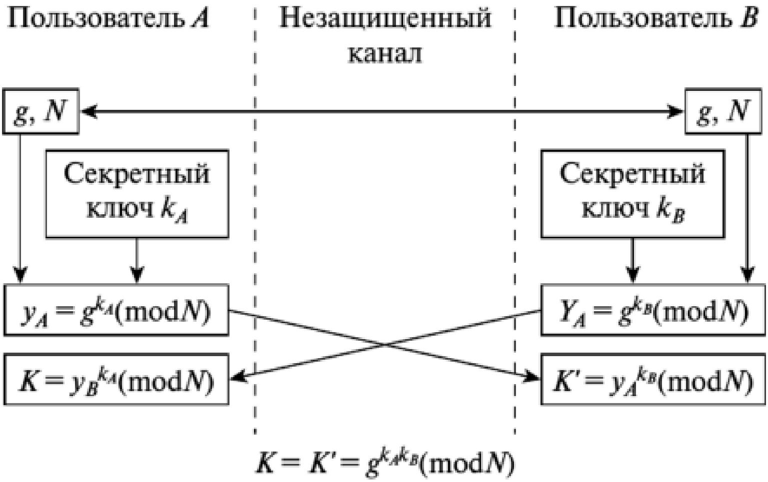

Схема протокола Диффи-Хеллмана

Модель противника

- *Пассивный противник* (противник может читать зашифрованные пересылаемые данные в открытом канале)
- ***Dolev-Yao (Активный) Противник*** может:
  - читать сообщения в канале
  - модифицировать сообщения в канале
  - удалять сообщения из канала
- Противник, учитывающий временные задержки (может определить, какая именно проверка не прошла, ...)
- ...

Рассуждать о стойкости криптосистемы можно только в терминах модели противника

- E – пассивный противник, слушающий незащищённый канал
- E известно значение g, N и y_A, y_B

Пусть E скомпрометировал $K = g^{k_A k_B} \ (mod \ N)$, тогда:

- узнал k_A
  - решил задачу дискретного логарифмирования, т.е. вычислил k_A из уравненя $y_A = g^{k_A} \ (mod \ N)$
- узнал k_B
  - решил задачу дискретного логарифмирования, т.е. вычислил k_B из уравненя $y_B = g^{k_B} \ (mod \ N)$
- узнал $k_A * k_B$

Протокол Диффи-Хэллмана стойкий по отношении к пассивному противнику

G – группа по модулю N, g – образующий элемент

Alice	Eva	Bob
$k_A \in_U G$ $y_A = g^{k_A} (mod\ N)$ $\xrightarrow{y_A}$	$k_A^E \in_U G$ $y_A^E = g^{k_A^E} (mod\ N)$ $\xrightarrow{y_A^E}$	
	$k_B^E \in_U G$ $y_B^E = g^{k_B^E} (mod\ N)$ $\xleftarrow{y_B^E}$	$k_B \in_U G$ $y_B = g^{k_B} (mod\ N)$ $\xleftarrow{y_B}$
$K_{AE} = (y_B^E)^{k_A} = g^{k_B^E * k_A}$	$K_{AE} = (y_A)^{k_B^E} = g^{k_A * k_B^E}$ $K_{BE} = (y_B)^{k_A^E} = g^{k_B * k_A^E}$	$K_{BE} = (y_A^E)^{k_B} = g^{k_A^E * k_B}$

Протокол Диффи-Хэллмана не является стойким по отношении к активному противнику

Свойства безопасности протоколов выработки общих ключей обмена

- Аутентификация
  - Ложная аутентификация
  - Unknown key share (Неизвестный общий ключ)
- Установление одинаковых ключей
- Секретность ключей обмена
- Уникальность установленных ключей обмена
- Forward secrecy (Прямая секретность)
- Backward secrecy (Обратная секретность)

Протокол Нидхема-Шрёдера

Протокол выработки общего сессионного ключа (N_A, N_B)

Alice (pkA, privA)		Bob (pkB, privB)
- генерация N_A - шифрует $<A, N_A>_{pk(B)}$	$<A, N_A>_{pk(B)}$ ------------------>	
	$<N_A, N_B>_{pk(A)}$ <------------------	- дешифровка сообщения $<A, N_A>_{pk(B)}$ - $<N_A, N_B>_{pk(A)}$
- дешифровка сообщения $<N_A, N_B>_{pk(A)}$ - $<N_B>_{pk(B)}$	$<N_B>_{pk(B)}$ ------------------>	
(N_A, N_B) -- общий секрет		

Уязвимость протокола Нидхема-Шрёдера

Alice	Intruder (pkI, privI)	Bob
- генерация N_A - шифрует $<A, N_A>_{pk(I)}$ $<A, N_A>_{pk(I)}$ ------------------>		
	- дешифрует $<A, N_A>_{pk(I)}$ - шифрует $<A, N_A>_{pk(B)}$ $<A, N_A>_{pk(B)}$ ------------------>	
		- дешифровка сообщения $<A, N_A>_{pk(B)}$ - $<N_A, N_B>_{pk(A)}$ $<N_A, N_B>_{pk(A)}$ <------------------

Уязвимость протокола Нидхема-Шрёдера (2)

	$\langle N_A, N_B \rangle_{pk(A)}$ <------------------	
- дешифровка сообщения $\langle N_A, N_B \rangle_{pk(A)}$ - $\langle N_B \rangle_{pk(I)}$ $\langle N_B \rangle_{pk(I)}$ ------------------>		
	- дешифровка $\langle N_B \rangle_{pk(I)}$ $\langle N_B \rangle_{pk(B)}$ ------------------>	
(N_A, N_B) -- общий секрет, который известен I		