Криптографические протоколы

Лекция 9

Протоколы распределения ключей (Часть 3)

Деркач Максим Юрьевич

October 18, 2018

Ссылки

1. ISO/IEC 11770-1:2010 – Information technology – Security techniques – Key management – Part 1: Framework
2. ISO/IEC 11770-2:2008 – Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques
3. ISO/IEC 11770-3:2008 – Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques
4. ISO/IEC 11770-4:2006 – Information technology – Security techniques – Key management – Part 4: Mechanisms based on weak secrets
5. СТБ 34.101.45-2013 "Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых". http://apmi.bsu.by/assets/files/std/bign-spec19.pdf
6. СТБ 34.101.60-2014 "Информационные технологии и безопасность. Алгоритмы разделения секрета". http://apmi.bsu.by/assets/files/std/bels-spec12.pdf

Протоколы распределения ключей

Предварительное распределение ключей

Предварительное распределение ключей нужно для уменьшения объёма распределяемой и хранимой информации.

$A_1, ..., A_n$ - абоненты.
K - множество ключей.
P - множество исходных ключевых параметров (p_i - пароль каждого абонента).
Q - множество значений ключевых материалов абонентов (q_i - секрет каждого абонента).
R - множество значений открытой информации ($r_1, ..., r_n$ - в открытом доступе).

Протоколы распределения ключей

Предварительное распределение ключей

Схема предварительного распределения ключей:
$S(n) = (K, P, Q, R, A_0, A_1)$

1. $A_0 : P \times R -> Q$ - алгоритм формирования секретных ключевых материалов.
   $A_0(p_i, r_i) = q_i,\ 1 \leq i \leq n$
2. $A_1 : Q \times R -> K$ - алгоритм вычисления ключа парной связи.
   $A_1(q_i, r_j) = A_1(q_j, r_i)$,
   $K_{ij} = A_1(q_i, r_j), i = j$: либо не рассматривается либо некий личный секретный ключ.

$A_0(p, r_i) = Q_i \subseteq K^{t_i} \subseteq Q,\ 1 \leq i \leq n$

Протоколы распределения ключей

Предварительное распределение ключей

Предложение 1

$\forall r_i \in R,\ q_i \in Q,\ 1 \leq i \leq n$

$A_0(p, r_i) = q_i$ - имеет одинаковое число решений относительно $p \in P$.

Предложение 2

$\forall r_i \in R,\ k \in K,\ 1 \leq i \leq n$

$A_1(q_i, r_i) = k$ - имеет одинаковое число решений относительно $q_i \in Q$.

Протоколы распределения ключей

Предварительное распределение ключей

Пусть $1 \leq m \leq n-2$ $S(n)$ является стойкой к m-кратной компрометации ключей (к сговору m абонентов), если после того как злоумышленнкиу станут известны ключевые материалы m абонентов ($q_1, ..., q_m$ - не ограничивая общности) он не сможет получить никакой информации о ключах парной связи остальных абонентов ($K_{i,1}, ..., K_{i,m}$ $\forall A_i$, $m+1 \leq i \leq n$).

Предложение 3

$\forall r_1, ..., r_{m+1} \in R$,
$K_{i,1}, ..., K_{i,m+1} \in K$,
то система имеет одинаковое число решений относительно $q_i \in Q$.

Теорема

$S(n)$, удолетворяющая предположению 1, является стойкой к m-кратной компрометации ключей $\leftrightarrow$ когда выполнено предположение 3.

Следствие

Если $S(n)$ является стойкой к m-кратной компрометцаии, то

1. каждый абонент должен хранить не менее $(m+1)log_2(K)$ бит ключевых материалов;
2. центр распределения ключей должен хранить не менее $\frac{(n+1)n}{2} log_2(K)$ бит исходных ключевых материалов.

Схема $S(n)$ называется оптимальной, если для неё выполняются нижние границы указанных выше ограничений.

Протоколы распределения ключей

Предварительное распределение ключей

Схема Блома

F - конечное поле, имеющее достаточно большое число элементов(n элементов).

$r_1, ..., r_n \ \in F \neq 0 \ r_i \rightarrow A_i$

$f(x,y) = \sum_{s=0}^{m} \sum_{t=0}^{m} a_{st} x^s y^t, \ a_{st} = a_{ts}, \ s \neq t, \ s,t = 0, ..., m$

$1 \leq m \leq n-2, \ a_{st}$ - секретные материалы, хранимые только в центре распределения.

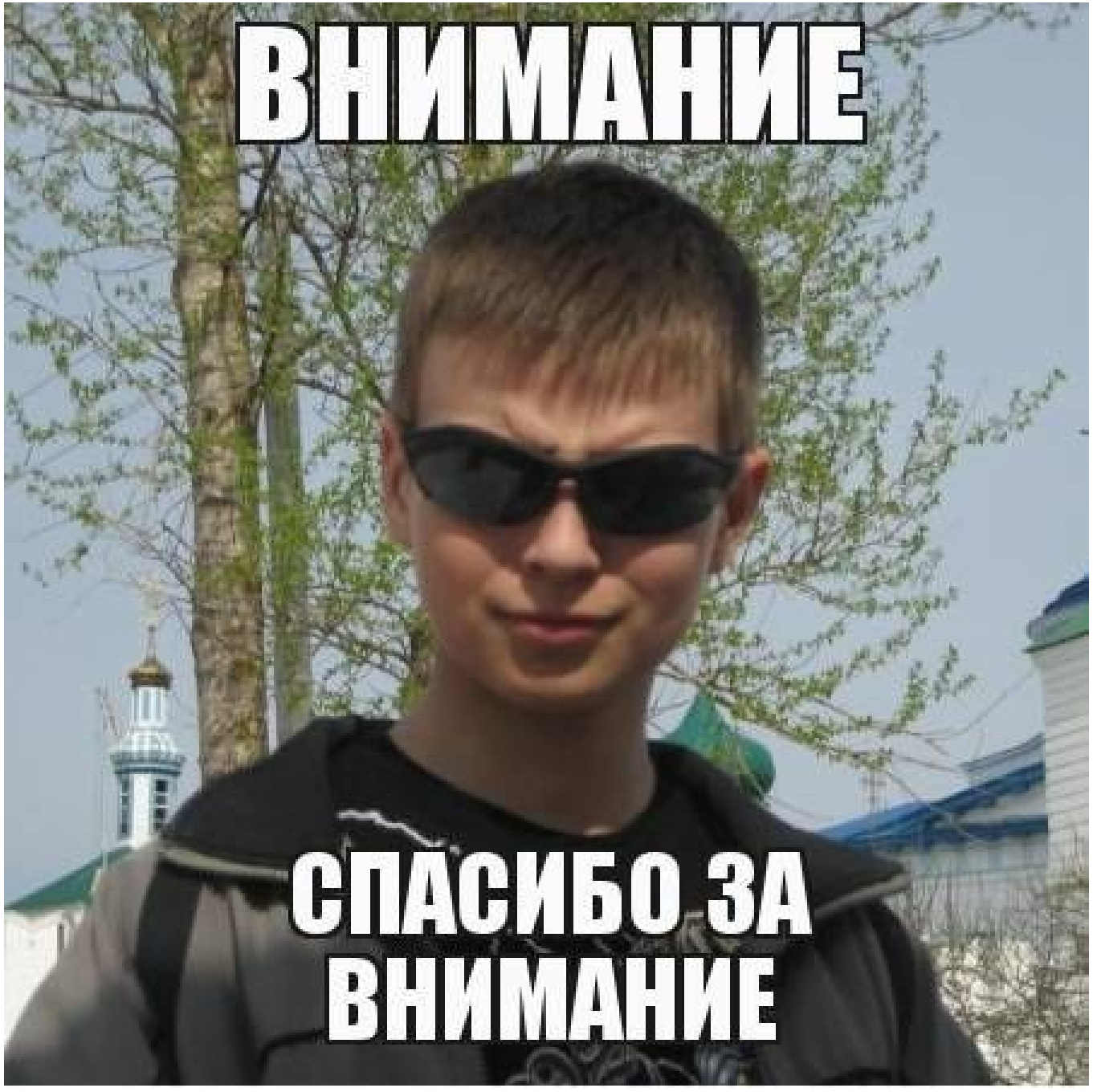
$A_i : \ q_i = (a_0^{(i)}, a_1^{(i)}, ..., a_m^{(i)})$

$q_i(x) = f(x, r_i) = a_0^{(i)} + a_1^{(i)} x + ... + a_m^{(i)} x^m$

$K_{ij} = K_{ji} = f(r_i, r_j) = q_i(r_j) = q_j(r_i)$

A_i хранит $m+1$ значение ключевых паролей.

Схема Блома является стойкой к m-кратной компрометации ключей.


ВНИМАНИЕ
СПАСИБО ЗА ВНИМАНИЕ