„Теоретико-сложностные основы криптографии“. Заметки к курсу в СПбАУ

А.В. Смаль

21 февраля 2018 г.

Аннотация

Курс посвящён изучению теоретических оснований, на которых строится надёжность криптографических протоколов.

Содержание

Введение

Мы будем предполагать, что алгоритмы шифрования/дешифрования всем известны (т.е. no security by obscurity).

1. Совершенная надёжность

Определение 1.1. *Система шифрования с закрытым ключом* — это пара алгоритмов $E(k, m)$ и $D(k, c)$, такая, что для любых k и m выполняется $D(k, E(k, m)) = m$. Система называется *совершенно надёжной*, если для любых двух сообщений m_1 и m_2 случайные величины $E(k, m_1)$ и $E(k, m_2)$ при $k \leftarrow \mathcal{U}(K)$ распределены одинаково ($\mathcal{K}$ — пространство ключей).

Замечание 1.1. Система шифрования с одноразовым шифроблокнотом является совершенно надёжной.

Замечание 1.2. Для совершенной надёжности необходимо, чтобы длина ключа была не менее длины сообщения.

Теорема 1.1. *Пусть $P = NP$. Тогда для любой системы шифрования с закрытым ключом (E, D) с полиномиальным алгоритмом E, в которой $|m| > |k|$, существуют сообщения m_0 и m_1 и полиномиальный алгоритм A, для которого*

$$\left|\Pr_k[A(E(k, m_0)) = 1] - \Pr_k[A(E(k, m_1)) = 1]\right| \geq \frac{1}{2}.$$

Доказательство. Не уменьшая общности предположим, что $\mathcal{K} = \{0, 1\}^{n-1}$. Возьмём в качестве $m_0 = 0^n$. Пусть $S = \{E(k, 0^n) \mid k \in \mathcal{K}\}$. Легко видеть, что $S \in NP$ и $|S| \leq 2^{n-1}$. Возьмём в качестве алгоритма A полиномиальный разрешающий алгоритм для S, т.е. $A(y) := [y \in S]$ (он существует по предположению $P = NP$).

Для каждого сообщения m рассмотрим $t_m = \left|\{k \mid E(k, m) \in S\}\right|$. Если существует сообщение m^*, для которого $t_{m^*} \leq 2^{n-1}$, то $m_1 = m^*$ удовлетворяет требованиям.

Предположим теперь, что $t_m > 2^{n-2}$ для любого m. Это значит, что существуют более $2^{n-2} \cdot 2^n = 2^{2n-2}$ пар ключ-сообщение (k, m), для которых $E(k, m) \in S$. Следовательно, для некоторого $y \in S$ существует более $2^{2n-2}/|S| \geq 2^{n-1}$ пар $(k, m) : E(k, m) = y$, т.е. существуют ключ k и два различных сообщения m' и m'': $E(k, m') = E(k, m'')$. Это противоречит корректности системы шифрования. □

2. Односторонние функции

Доказывать надёжность криптографических протоколов без каких-либо предположений, к сожалению, не получается — из такого доказательства следовало бы $P \neq NP$. Было бы здорово показать, что криптография возможна, если $P \neq NP$, но это тоже не получается сделать. Поэтому в дальнейшем мы будем отталкиваться от более сильного предположение — предположения о существовании *односторонней функции*.

В дальнейшем мы будем рассматривать семейства функций $f_n : \{0,1\}^{k(n)} \to \{0,1\}^{l(n)}$, где $k(n)$ и $l(n)$ будут некоторыми полиномами. Кроме того, нас почти всегда будут интересовать функции, которые можно вычислить за полиномиальное время.

Определение 2.1. Семейство функций $f_n : \{0,1\}^{k(n)} \to \{0,1\}^{l(n)}$ называется *полиномиально вычислимым*, если имеется алгоритм, который получая на вход число n и x длины $k(n)$ вычисляет $f_n(x)$ за полиномиальное от n время.

2.1. Односторонние функции с худшем случае

Определение 2.2. Полиномиально вычислимое семейство функций $f_n : \{0,1\}^{k(n)} \to \{0,1\}^{l(n)}$ называется *односторонним в худшем случае*, если не существует полиномиально вычислимой функции g_n, что для любого $x \in \{0,1\}^{k(n)}$ верно $f_n(g_n(f_n(x))) = f_n(x)$.

Теорема 2.1. *Односторонние функции с худшем случае существуют* $\iff$ $P \neq NP$.

Доказательство.

- $\Rightarrow$ Пусть $P = NP$. Определим язык $L = \{(1^n, y, z) \mid \exists x, |x| = k(n), z \sqsubset x, f_n(x) = y\}$, $L \in NP$. По предположению для L существует полиномиальный разрешающий алгоритм. Для нахождения прообраза y запустим этот алгоритм сначала на слове $(1^n, y, \lambda)$, где λ — пустая строка. Если это слово не принадлежит L, то y не имеет прообраза. В противном случае восстановим прообраз y по битам: сначала запустим алгоритм для слова $(1^n, y, 0)$ и проверим, есть ли у y прообраз начинающийся с нуля. Далее аналогично восстановим второй и все последующие биты. Нам потребуется $k(n)+1$ запуск полиномиального алгоритма, т.е. прообраз можно найти алгоритмически за полиномиальное время.

- $\Leftarrow$ Если $P \neq NP$, то можно построить одностороннюю в худшем на основе любой NP-трудной задачи. Пусть $R(x, y)$ — это отношение, задающее NP-трудную задачу S (например, для $S = SAT$: $R(\phi, a) = 1 \iff \phi(a) = 1$). Пусть $f_n(x, y) = (x, R(x, y))$. Если f_n^{-1} вычисляется за полиномиальное время, то и задачу S можно решить за полиномиальное время, вычислив $f^{-1}(x, 1)$.

$\square$

2.2. Односторонние функции для алгоритмов

Мы будем определять *односторонние функции* для противника, который является вероятностным полиномиальным алгоритмом, т.е. для *равномерного противника.*

Определение 2.3. Полиномиально вычислимое семейство f_n называется *слабо односторонним для равномерного противника*, если существует такой полином p, что для любого полиномиального вероятностного алгоритма R при всех достаточно больших n

$$\Pr_{x,R}[f_n(R(1^n, f_n(x))) = f_n(x)] < 1 - \frac{1}{p(n)}.$$

Определение 2.4. Полиномиально вычислимое семейство f_n называется *сильно односторонним для равномерного противника*, если существует такой полином q, что для любого полиномиального вероятностного алгоритма R при всех достаточно больших n

$$\Pr_{x,R}[f_n(R(1^n, f_n(x))) = f_n(x)] < \frac{1}{q(n)}.$$

2.3. Односторонние функции для неравномерного противника

Аналогичным образом можно определить односторонние функции для противника, являющегося последовательностью схем, т.е. для *неравномерного противника*.

Определение 2.5. Полиномиально вычислимое семейство f_n называется *слабо односторонним для неравномерного противника*, если существует такой полином p, что для любой последовательности схем C_n полиномиального размера при всех достаточно больших n

$$\Pr_{x}[f_n(x) = f_n(C_n(f_n(x)))] < 1 - \frac{1}{p(n)}.$$

Определение 2.6. Полиномиально вычислимое семейство f_n называется *сильно односторонним для неравномерного противника*, если существует такой полином q, что для любой последовательности схем C_n полиномиального размера при всех достаточно больших n

$$\Pr_{x}[f_n(x) = f_n(C_n(f_n(x)))] < \frac{1}{q(n)}.$$

Замечание 2.1. Односторонние функции для неравномерного противника можно было бы определять для *вероятностных* схем, т.е. для схем, которым на вход подают не только $f_n(x)$, но и некоторую строку со случайными битами r. Однако, легко показать, что от случайных битов в таких определениях можно избавиться: для этого нужно для каждого n выбрать одну "самую лучшую" строку r_n, на которой достигается максимальная вероятность обращения f_n и "зашить" её в схему. Нетрудно увидеть, что вероятность обращения при $r = r_n$ будет не меньше, чем по всем r в среднем.

В дальнейшем мы часто будем говорить про односторонние *функции*, подразумевая под этим *семейства* односторонних функций. Когда говорят про *одностороннюю функцию*, то имеется в виду сильно односторонняя функция.

Определение 2.7. Если в определении односторонней функции убрать требование полиномиальной вычислимости, то получится определение *необратимой* функции.

Список литературы

[1] Н.К. Верещагин. *Курс лекций "Теоретико-сложностные проблемы криптографии"*, МГУ, http://lpcs.math.msu.su/~ver/teaching/cryptography/index.html.

[2] Д.М. Ицыксон. *Курс "Теоретико-сложностные основы криптографии"*, CS центр, https://compsciclub.ru/courses/cryptography-foundations/2016-spring/.

[3] O. Goldreich. *Foundations of cryptography.*

[4] J. Håstad, R. Impagliazzo, L.A. Levin, M. Luby. *A Pseudorandom Generator from any One-way Function*. SIAM J. Comput. 28, 4 (March 1999), 1364-1396.
DOI: https://doi.org/10.1137/S0097539793244708

[5] J. Katz, Y. Lindell. *Introduction to Modern Cryptography.*