Московский физико-технический институт
Физтех-школа прикладной математики и информатики
Кафедра дискретной математики
Криптография, осень 2022
Домашние задачи, набор №2

Вам предлагается 7 задач. Каждая задача оценивается в 10 баллов. В зачёт идут 5 наилучшим образом решённых задачи. В отдельных случаях (например, решение задачи, которую больше никто не решил) могут начисляться бонусы сверх этой квоты. Задачи принимаются в письменном виде по почте `musatych@gmail.com` или в Телеграме `@musatych` одним файлом в формате PDF. (Желательно набрать решение в TEXe, можно также отсканировать или сфотографировать написанное от руки, собрав всё в PDF. При фотографировании следите за резкостью, контрастностью и балансом белого. Фотографии плохого качества, например снятые на телефон при слабом освещении, проверяться не будут). Если вы решаете задачи совместно с кем-то, то в работе нужно указать, с кем и в каком объёме вы сотрудничали. При этом собственно тексты решений необходимо записывать самостоятельно. Обнаруженные списанные решения не засчитываются всем авторам. Для получения экзаменационной оценки x достаточно суммарно набрать $25 + 10x$ баллов по итогам двух заданий и контрольной.

1. Схема шифрования с закрытым ключом (G, D, E) называется *семантически надёжной*, если для любого полиномиального (от параметра безопасности n) вероятностного алгоритма A существует полиномиальный вероятностный алгоритм A', такой что для любого семейства случайных величин $\{X_n\}_{n\in\mathbb{N}}$, таких что $|X_n| < \mathrm{poly}(n)$, для любых двух функций $f, h\colon \{0,1\}^* \to \{0,1\}^*$, увеличивающих длину не более чем полиномиально, и любого полинома p при всех достаточно больших n выполнено:

$$\Pr\{A(n, |X_n|, E(G(n), X_n), h(1^n, X_n)) = f(1^n, X_n)\} < \\ < \Pr\{A'(n, |X_n|, h(1^n, X_n)) = f(1^n, X_n)\} + \frac{1}{p(n)}.$$

а) Объясните интуитивный смысл этого определения;

б) Докажите, что если A и A' не получают $|X_n|$ в качестве аргумента, то семантически надёжных схем не существует.

в) Докажите, что после замены полиномиальных вероятностных алгоритмов на схемы из функциональных элементов полиномиального размера определение получится эквивалентным исходному.

2. Формализуйте задачу и опишите, как с использованием протокола привязки реализовать такую раздачу карт по интернету: есть колода из четырёх карт. Нужно раздать каждому из двух игроков по одной карте, а две оставить на столе в некотором порядке. При этом раздача должна быть (почти) случайной, каждый должен знать только свою карту, но при этом ни у кого не должно быть возможности подменить ни свою карту, ни карты, лежащие на столе, ни их порядок.

3. Рассмотрим протокол Шнорра идентификации на основе задачи дискретного логарифмирования. Пусть клиент и сервер знают некоторую группу размера n и её генератор g. Клиент имеет закрытый ключ x, а сервер — открытый ключ $y = g^x$. Протокол производится в 3 шага:

1. Клиент выбирает случайное $r \in \mathbb{Z}_n$ и посылает на сервер $z = g^r$.
2. Сервер выбирает случайный бит $b \in \{0, 1\}$ и посылает клиенту.
3. Клиент подсчитывает $s = r + bx$ и посылает результат на сервер.

Ответьте на следующие вопросы о протоколе:

а) Какую проверку должен осуществить сервер для завершения протокола, чтобы честный клиент её всегда проходил?

б) Докажите, что клиент, не знающий закрытого ключа, сможет пройти проверку с вероятностью не больше $\frac{1}{2}$. Точнее, докажите, что более успешное прохождение может быть использовано для решения задачи дискретного логарифмирования в данной группе.

в) Докажите, что протокол имеет нулевое разглашение в случае честного сервера.

г) Докажите, что протокол имеет нулевое разглашение в случае произвольного сервера.

д) (Бонусный пункт, до 5 баллов) Рассмотрим вариацию протокола, когда b не обязательно бит, а может быть числом из $\mathbb{Z}_n$. Как будет модифицирована проверка сервера? Докажите, что в случае честного сервера нулевое разглашение сохранится. Почему не пройдёт доказательство в случае произвольного сервера? (Построение конкретной атаки в этом случае — открытая проблема).

4. Докажите, что из существования семейства хеш-функций с трудно обнаружимыми коллизиями следует существование односторонних функций. (При необходимости уточняйте определения, добавляя условия на области определения функций).

5. Пусть $f\colon \{0,1\}^n \to \{0,1\}^n$ — односторонняя перестановка. Определим $f^{(k)}$ как k-ю итерацию f, т.е. $f^{(0)}(x) = x$, $f^{(k+1)}(x) = f(f^{(k)}(x))$. Рассмотрим следующую схему цифровой подписи с открытым ключом сообщения $i \in \{0, 1, \ldots, m\}$, где $m = \mathrm{poly}(n)$:

- Закрытый ключ x равномерно выбирается среди всех слов из $\{0,1\}^n$.
- Открытый ключ y равен $f^{(m)}(x)$.
- Подпись под сообщением i равняется $f^{(m-i)}(x)$.
- Верификатор, проверяющий корректность подписи s под сообщением i, проверяет равенство $f^{(i)}(s) = y$.

Ответьте на следующие вопросы:

а) Докажите, что такая схема не является надёжной схемой одноразовой подписи сообщения $i \in \{0, 1, \ldots, m\}$. Под какими сообщениями сможет подделать подпись противник, перехвативший подпись под сообщением i?

б) Докажите, что полиномиальный вероятностный противник не сможет с существенной вероятностью подделать подписи под всеми остальными сообщениями.

в) Модифицируйте схему, так чтобы она стала надёжной одноразовой схемой цифровой подписи, и докажите, что построенная схема подходит. (Указание: например, можно удвоить длину обоих ключей, в одной половине взять ту же схему, в другой — модифицированную).

6. Рассмотрим протокол Эвена–Голдрайха–Лемпеля слепой передачи одного сообщения из двух. Предполагается, что уже сгенерированы открытый ключ e и закрытый ключ d для схемы шифрования, E и D — соответствующие функции шифровки и дешифровки соответственно.

1. Алиса имеет 2 сообщения m_0, m_1, Боб имеет $\sigma \in \{0, 1\}$.
2. Алиса посылает случайные x_0, x_1.
3. Боб генерирует случайное k и посылает Алисе $v = x_\sigma \oplus E(e, k)$.
4. Алиса вычисляет $k_\tau = D(d, v \oplus x_\tau)$, $\tau = 0, 1$ и посылает Бобу $m'_\tau = m_\tau \oplus k_\tau$, $\tau = 0, 1$.
5. Боб восстанавливает $m_\sigma = m'_\sigma \oplus k$.

Ответьте на следующие вопросы:

а) Докажите, что если схема шифрования надёжна, то данный протокол надёжен в получестной модели.

б) Будет ли он надёжен в нечестной модели?

7. (**Византийское соглашение**). Генерал командует дивизией, состоящей из k полков, каждый под командованием своего полковника. Каждый из $k+1$ командира может оказаться честным или предателем. Генерал передаёт каждому из полковников команду «Атаковать» или «Отступать». Полковники могут общаться между собой, но только по двусторонним каналам. Предатели могут действовать согласованно. В итоге каждый из полковников должен решить, атаковать или отступать. На протокол накладываются следующие ограничения:

- *Исполнительность:* Если генерал честный, то его приказ для всех полковников одинаков и все честные полковники его выполняют.

- *Согласованность:* В любом случае все честные полковники выполняют одно и то же действие.

Таким образом, если все командиры честные, то генерал передаёт всем полковникам одинаковый приказ, и те его выполняют.

а) Докажите, что в случае $k = 2$ такой протокол невозможен, даже для одного предателя.

б) В случае $k = 3$ постройте протокол, устойчивый против одного предателя.

в) Постройте для $k = 3m$ протокол, устойчивый против m предателей.