Задача 1.

a) Пусть $f(x)$ — односторонняя и вычислятеся за $O(n^k)$, тогда построим функцию $g(x,y) = \langle f(x), y\rangle$ для y длины $|x|^k$. Тогда её вычисление занимает квадратичное от размера входа время так как нужно просто скопировать число x в ответ, перенести число x по ленте и запустить алгоритм вычисления $f(x)$. При этом она также будет односторонней, так как, очевидно, с помощью обратителя для g легко построить обратитель для f.

b) Пользуясь пунктом a) покажем, что функция $f(M,x) = TM(M,x,n^3)$, которая запускает машину M на входе x на n^3 шагов (и возвращает результат или $\perp$) односторонняя. Пусть вообще существует какая-то односторонняя функция $g(x)$, будем считать, что она вычисляется за $O(n^2)$ по пункту a). Пусть f не односторонняя, тогда есть машина M_q, и многочлен p, такие что

$$P_{(M,x)\sim\{0,1\}^n}(M_q(f(M,x)) \in f^{-1}(f(M,x))) > \frac{1}{p(n)}$$

Потребуем, чтобы описание машины M у функции f занимало первые $log|x|$ бит, тогда с вероятностью хотя бы $\frac{1}{n}$ в качестве машины M выберется машина, вычисляющая g (для достаточно большого n). Это значит, что найдется обратитель для g, преуспевающий с вероятностью не менее $\frac{1}{np(n)}$, что противоречит тому, что она односторонняя.

Задача 2.

a) Если f — односторонняя перестановка, а функция $g = f^{n^c}$ обращается за полином, то можно обратить f, просто вычислив $g^{-1} \circ f^{n^c-1}$. Вычисление работает за полиномиальное время и вернёт корректный ответ с той же вероятностью, что и обратитель g в силу того, что все функции биективны.

b) Пусть f — односторонняя, положим также, что $f : \{0,1\}^n \to \{0,1\}^n$ сохраняет длину. Построим одностороннюю функцию g, такую, что $g^2(x) = const$. Положим $g(xy) = 0^n f(x)$, где $|x| = |y| = n$. Эта функция односторонняя, так как её обратителем можно обращать и функцию f. Однако $g(g(xy)) = g(0^n f(x)) = 0^n f(0^n) = const$, то есть функция тривиально обратима.

Задача 4.

a) Если длина строки есть $2n$, то количество строк, на которых генератор возвращает 0 есть хотя бы $\binom{2n}{n} \sim const \cdot \frac{4^n}{\sqrt{n}}$. Тогда алгоритм, возвращающий 1 на строке и всех нулей и 0 иначе различает ГСЧ и случайную величину с хорошей вероятностью.

b) Оценим долю строк, на которых выводы $G(s)$ и $G''(s)$ отличаются.

$$\frac{\binom{3n}{n}}{2^{3n}} = \frac{(3n)!}{8^n n!\,(2n)!} \sim const \cdot \frac{(3n)^{3n}}{8^n n^n (2n)^{2n}} = const \cdot \left(\frac{27}{32}\right)^n.$$

Это значит, что вероятность любого алгоритма отличить выходы алгоритмов на случайной стороке пренебрежимо малы. Стало быть, $G''(s)$ вычислительно неотличим от $G(s)$ и является ГСЧ.

Задача 7.

Изложим сразу алгоритм для n студентов. Предположим, что у них есть как общий чат, так и личные сообщения друг для друга. Тогда можно добиться линейного количества пересланных бит. Обозначим за c_i величину, отражающую, платил ли студент i за обед или нет, тогда им необходимо вычислить $c_1 \oplus \ldots \oplus c_n$. Алгоритм такой:

- Студенты i и $(i+1) \bmod n$ генерируют случайный бит a_i.
- В общий чат студентом i объявляется число $b_i = a_{(i-1) \bmod n} \oplus a_i \oplus c_i$.
- Сумма $\bigoplus_{i=1}^{n} b_i$ равна $\bigoplus_{i=1}^{n} c_i$, так как каждое a_i встречается по 2 раза.
- Однако точно узнать, кто платил никто не может, так как если студент j говорит, что якобы платил студент i, то всегда возможен случай, что платил на самом деле $i+1$ или $i-1$, а соответствующие случайные биты a_i, a_{i-1} были другими (пользуемся тем, что студент j не может быть одновременно левым и правым соседом i и знать обе этих величины), так что значения d_i были такие же.

Задача 8.

a) Рассмотрим два случая:

- Генерал честный, один из полковников предатель, другой нет. Полковник знает, какой приказ дал генерал, однако, второй говорит ему прямо противоположное.
- Генерал нечестный, оба полковника честные. Генерал выслал противоречивые приказы.

Ясно, что эти две ситуации неразличимы с точки зрения честного полковника, а действовать он в них должен по-разному. Значит искомого протокола нет.

b) Протокол такой: генерал высылает приказы, полковники пересылают их друг другу и выполняют тот приказ, которого больше.

Исполнительность: если генерал честный, все получили одинковые приказы, значит у всех честных полковников есть правильный приказ хотя бы в двух экземплярах, значит все честные выполнят приказ.

Согласованность: если генерал нечестный, то все командиры честные, они переслали друг другу какие-то данные и одинаковым образом выбрали то, что надо сделать.

Задача 9.

В общем случае действуем так:

- Все получают приказ и рассылают его всем остальным командирам. У каждого получается $3m$ каких-то приказов. Будем рассматривать честных командиров. Каждый из них попадает одну из трёх категорий: те, что получили хотя бы $2m$ приказов атаки, те, что получили хотя бы $2m$ приказов отступления и остальные. Заметим, что эти остальные точно знают, что генерал предатель, так как иначе бы они получили хотя бы $2m$ честных приказов от остальных.

- Не бывает двух честных командиров в разной категории. Если генерал честный, то все честные командиры точно будут в той категории, которая соответствует приказу генерала. Если же генерал нечестный, то честных полковников $2m + 1$, значит, как бы ни были отданы им приказы, каких-то будет хотя бы $m+1$ (положим, приказов на атаку), значит либо все честные полковники будут в наступательной категории, либо в третей ($m + 1$ приказ не даст другой категории взять большинство в $\frac{2}{3}$).

- Каждый озвучивает каждому свою категорию. Если хотя бы $m+1$ человек считают, что генерал предатель, то из них был кто-то честный, значит генерал в самом деле предатель. Аналогично, если сигнала какого-то действия было не меньше, чем $m+1$, то этот командир может быть уверен, что у всех честных командиров есть либо информация об этом действии, либо информация о том, что генерал нечестный.

- Путь честных командиров, которые считают, что генерал предатель, больше или равно $m + 1$. Тогда все честные командиры это узнают. В противном случае Есть хотя бы $m + 1$ честный командир с одним и тем же приказом, тогда все узнают этот приказ. Осталось всем честным командиром обменяться своими знаниями и различить эти две ситуации.

- Все пересылают всем своё мнение, честный ли генерал или нет. Если хотя бы $2m$ человек считают, что да, то полковник принимает одно фиксированное решение, например, отступать. В противном случае можно быть уверенным, что все честные командиры в одной категории, значит они сделают одно и то же действие, которое, если генерал честный, будет его приказом.

Задача 10.

Задача является одной из вариаций известной задачи Mental poker. Классическое решение состоит в использовании коммутирующего шифрования:

- Нам нужны функции $E(K, X), D(K, X)$.

- $D_K(E_K(X)) = X$ для всех возможных сообщений X и ключей K.
- $E_K(E_J(X)) = E_J(E_K(X))$ для всех возможных сообщений X и пар ключей K, J.
- $X \mapsto E(K, X)$ односторонняя.
- Ключи неподменяемы, то есть по сообщениям X, Y нельзя полиномиально быстро найти ключи K, J такие что $E_K(X) = E_J(Y)$. такие

Существование такой криптосистемы (вроде) не следует из существования односторонней функции, но на практике такие системы используются. Используя это, можем реализовать протокол раздачи карт так:

- Первый игрок перемешивает карты $A_1, \ldots, A_4$ случайно. Он выбирает ключ K и посылает $E(K, A_1), \ldots, E(K, A_4)$ второму.
- Второй игрок выбирает из четырёх зашифрованных карт две, выбирает ключ J и пересылает $E(J, E(K, A_p)), E(K, A_q)$.
- Первый игрок забирает себе одну карту A_q, которую он узнал по $E(K, A_q)$ с помощью расшифровки. Он также расшифровывает вторую карту, получая $E(J, A_p)$ и отправляет это второму.
- Второй игрок расшифровывает свою карту A_q.
- Первый игрок гарантирует случайность выбора своей карты, так как он тасовал изначальную колоду.
- Второй игрок гарантирует случайность своей карты, так как он сам её случайно выбрал.
- После сыгранной игры в покер они могут проверить, что жульничества не было, раскрыв оба ключа и проверив все пересылки.