RSA и вероятностные алгоритмы

1. Алиса хочет послать сообщение 42 Бобу. Закрытый ключ Боба $(103, 209)$.

1. Какой открытый ключ у Боба?

2. Найдите зашифрованное сообщение, которое должна отправить Алиса.

2. В жизни сообщения (пакеты по сети) пересылаются не по одну каналу между двумя знакомыми людьми. Третьи лица могут не просто пытаться узнать содержимое сообщение, но и выдать себя за другого человека или организацию. Так, фишинговый сайт может прикинуться банком и попытаться украсть ваш пароль. Чтобы этого избежать, используют цифровую подпись, которая подтверждает подлинность отправителя.

Придумайте способ имплементировать цифровую подпись в криптосистеме RSA. Боб отправляет Алисе пару (c_m, s_m) из зашифрованного сообщения c_m и подписи s_m. Вам нужно придумать алгоритм получения подписи удовлетворяющий условиям: зная s_m и c_m, но не зная секретный ключ Алисы нельзя («легко») восстановить исходное сообщение m; получив пару (c_m, s_m), Алиса может установить, что сообщение действительно отправил Боб.

3. В этой задаче нужно доказать, что сортировка Bucket Sort работает в среднем за линейное время. Эта сортировка предназначена для чисел из интервала $[0, 1)$ в предположении, что они распределены равномерно. При сортировке массива A размера n, интервал $[0, 1)$ делится на n равных частей, которым соответсвтуют «корзины» $B[i]$, каждая из которых является связным списком (изначально пустым). Элементы массива A распределяют по корзинам по принципу $A[i] \to B[\lfloor nA[i] \rfloor]$; нумерация корзин начинается с 0. После распределения каждую корзину сортируют сортировкой вставками (Insertion Sort), после чего отсортированный массив получается путём объединения списков.

1. Проверьте, что сортировка вставками работает даже на односвязных списках. Оцените время её работы.

2. Докажите, что математическое ожидание времени работы сортировки Bucket Sort есть $O(n)$ (Массив A содержит случайные числа, распределение описано выше).

4. Фирма разработала следующую стратегию найма сотрудников на единственную должность. Стопку резюме кандидатов перетасовали в случайном порядке, после чего последовательно приглашают кандидатов на собеседование. В результате собеседования, кандидата нанимают, если он лучше текущего сотрудника (первого кандидата нанимают сразу). Формально, каждому кандидату присваивают ранг, который однозначно определяет его место среди всех кандидатов, прошедших собеседование на данный момент и сравнивают его ранг с рангом текущего сотрудника. При увольнении нужно выплатить работнику компенсацию c. Найдите математическое ожидание суммарно выплаченных компенсаций, если фирма будет действовать согласно описанной стратегии.

5. Для вероятностных алгоритмов часто важно перетасовать массив в случайном порядке. Докажите, что следующий алгоритм делает это — формально, из массива чисел $1, \ldots, n$ получает равновероятно любую перестановку. **Алгоритм: for** i := 1 **to** n: обменять элемент $A[i]$ с элементом $A[j]$ местами, где j выбирается равномерно среди чисел $i, \ldots, n$.

6. Ева решила подобрать закрытый ключ Боба, зная открытый ключ (e, N), используя вероятностны поиск: её алгоритм будет перебирать числа от 1 до N в случайном порядке (каждый раз берётся новое число) и проверять, является ли оно парой к e. Ева надеется, что вероятностный поиск сильно ускорит её перебор.

1. Как Еве эффективно проверить, является ли текущее число d парным к e?

2. Найдите асимптотику математического ожидания числа проверок.