Мои контакты: Алексей Давыдов <adavydow@gmail.com>
Задачи можно сдавать мне на почту или письменно до конца курса.
Задачи с практики сдавать, естественно, не надо.

Криптография с открытым ключом

Практика

Проверки на простоту

1. Рассмотрим число a, не являющееся ни простым, ни числом Кармайкла. Докажите, что вероятность того, что оно пройдет тест Ферма не превосходит $\frac{1}{2}$.

2. Перед нами стоит задача: получить случайное простое число в диапозоне от 1 до 2^{128}. Решать ее будем так: выбираем случайное число и запускаем тест Миллера-Рабина. Этот метод не так плох как кажется, т.к. простые числа достаточно часты (среди чисел от 1 до n примерно $\frac{n}{\ln n}$ простых чисел). Известно, что любое составное число проваливает тест Миллера-Рабина с вероятностью $\frac{3}{4}$.

   Сколько раз надо запустить тест Милера-Рабина для того, чтобы вероятность того, что полученное в итоге число — простое была 90%?

RSA

3. Алена отправила сообщение m, зашифрованное через RSA, двум людям. Для каждого человека определено свое e_i, но везде одинаковое $N = pq$, Оказалось, что e_i взаимно простые. Найдите сообщение Алены за $\texttt{poly}\log N$.

4. Иногда при шифровании RSA $(n = pq, e, d)$ возможно совпадение исходного и зашифрованного текста. Чему равно число таких совпадений?

5. В распоряжении взломщиков оказался волшебный оракул. Для любого открытого ключа (N, e) оракул может взломать 1% из возможных зашифрованных сообщений. Придумайте алгоритм, который взламывает любое сообщение со средним временем работы $O(poly(\log n))$.

Линейные коды

6. Пусть длина исходного сообщения m, а длина линейного кода исправляющего d ошибок — n. Докажите, что $2^m \leq \frac{2^n}{\sum\limits_{i=0}^{d} C_n^i}$.

Криптосистема МакЭлиса

7. Доказать, что алгоритм декодирования, предложенный на лекции корректен.

8. Возможно ли заменить перестановку P на произвольную невырожденную матрицу?

9. Можно ли использовать МакЭлиса для электронной подписи?

Протокол Диффи-Хелмана

10. (a) Покажите, что зная $p, g, y_i \equiv g^{x_i} \pmod{n}$ мы можем узнать младший бит x_i.

    (b) Рассмотрим такой алгоритм:

    - Вычисляем младший бит x_i
    - Если бит единица — рассмотрим $y_i^{'} = y_i g^{-1}$, иначе $y_i^{'} = y_i$.
    - Вычисляем квадратный корень из $y_i^{'}$ и сводим задачу к задаче меньшего размера.

    Удастся ли таким алгоритмом взломать Диффи–Хеллмана за полиномиальное время?

Задачи для самостоятельного решения

1. Алена шифрует сообщение алгоритмом RSA (n, e, d). Однако алгоритм она помнила плохо и потому вместо $n = pq$, она взяла простое n. Дешифруйте сообщение m^e за $O(poly(\log n))$.

2. Пусть длина исходного сообщения m, а длина линейного кода исправляющего d ошибок — n. Докажите, что если выполнено неравенство $2^{m-1} \leq \frac{2^n}{\sum\limits_{i=0}^{2d} C_n^i}$, то код с заданными параметрами существует.

3. Если мы хотим, чтобы RSA было сложно взломать, то хорошо бы выбирать n побольше. Однако генерация большого простого числа не особо быстрый процесс. Расмотрим такой вариант RSA: Сперва выбирается s-битное простое число p, затем выбирается случайное число q размера ts (t может быть, например, десятью). Затем выбирается e и шифрование происходит аналогично обычному RSA ($c(m) = m^e mod n$), длина сообщения m меньше s. Публичный ключ опять-таки (n, e).

    - Какие ограничения нужно наложить на e, чтобы заданное отображение было инъективным?
    - Пусть e выбранно в соответствии с предложенными в пункте 1 ограничениями. Как расшифровывать?
    - Оцените сложность алгоритмов выбора ключей, шифровки и расшифровки.
    - Покажите, что если $e \leq t$, то такую криптосистему можно быстро(полиномиально) взломать.
    - Докажите, что если у нас есть оракул, умеющий взламывать такую криптосистему на любых сообщениях, то зная n мы сможем найти p.
    - Уязвима ли такая система к choosen ciphertext attack? Если да, придумайте как это исправить.