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.

1 Криптография с секретным ключом

1.1 Практика

1. За сколько вызовов DES в среднем можно угадать ключ, если можно сделать один запрос к сервису шифрования? А если два?

2. Одна из проблем DES — короткий ключ. Рассмотрим каскад из двух DES'ов, с ключами k_1 и k_2. Покажите, что для того, чтобы подобрать два ключа, которые на данном сообщении m дадут шифр c, хватит в среднем 2^{56} вызовов DES.

3. Каскад из двух DES плохо — возьмем из трех. Рассмотрим каскад из 3 DES с ключами k_1, k_2 и k_1. Покажите, как найти искомые ключи за 2^{60} вызовов DES. При этом к сервису шифрования можно обращаться произвольное количество раз (одно обращение считается одним DES'ом).

4. Докажите, что в случае каскада из двух DES найдутся такие ключи $k_1, k_1^{'}, k_2, k_2^{'}$ и сообщение m, что $k_1 \neq k_1^{'}$ или $k_2 \neq k_2^{'}$, но результаты шифровки сообщения m ключами k_1, k_2 и $k_1^{'}, k_2^{'}$ — совпадают.

5. Для каскада из двух DES мало найти пару ключей, которые на данном сообщении дадут данный шифр, надо, чтобы и на других сообщениях шифры выходили верные. Оцените, на скольких случайных сообщениях результат должен совпасть с результатом сервисом шифрования, чтобы с вероятностью 90% можно было сделать вывод, что ключи отгаданы верно?

1.2 Задачи для самостоятельного решения

1. Пусть есть OFB сервис шифрования с фиксированным ключом и IV (т. е. для каждого нового сообщения он использует один и тот же ключ и IV). Как расшифровать сообщение, зашифрованное сервисом, за полиномиальное время, при условии, что мы можем обращаться к сервису произвольное количество раз.

2. Допустим, что в качестве функции f для DES'а была выбрана линейная функция. Как тогда можно было бы взломать DES за 2^{10} вызовов? При этом к сервису шифрования можно обращаться произвольное количество раз (одно обращение считается одним DES'ом).

3. Рассмотрим каскад из k DES с k ключами. Оцените, на скольких случайных сообщениях результат должен совпасть с результатом сервисом шифрования, чтобы с вероятностью 90% можно было сделать вывод, что ключи отгаданы верно?