**Защита от копирования.**

1. Какими требованиями должен обладать параметр к которому привязываешься?

Ответ: 1 - УНИКАЛЬНОСТЬ (его нельзя подделать (например, имя учетной записи можно) )

2 - НЕИЗМЕНЯЕМОСТЬ (он является важной частью компьютера ( материнская плата, BIOS, HDD) )

3 - ДОСТУПНОСТЬ

1. Что такое WMI (для винды), что такое DMI для ubuntu

**Энигма.**

1. Для чего нужен рефлектор?   
   Ответ: Для того, чтобы процесс шифрования не отличался от процесса расшифровки. (Тут что-то про то, что на прямом ходу мы работаем со значениями по индексу, а на обратном с индексами по значению).
2. Чем отличается расшифровка от зашифровки?

Ответ: ничем

1. Что быстрее - прямой ход или обратный?

Ответ: прямой. Потому что на прямом ходе ты получаешь значение по индексу, а на обратном индекс по значению, что, очевидно, сложнее, т.к. подразумевает перебор всех значений.

1. Как изменяется размер файла после шифрования?

Ответ: никак (тк шифруем посимвольно, один символ переводится ровно в один символ)

**AES**

<https://habr.com/post/212235/> во если весь алгоритм нужен

1. Как бороться с незаполненным до конца блоком?

Ответ: до конца блока заполнить 0

1. Спрашивает про поле Галуа

Ответ: числа в поле Галуа представляются как наборы коэффициентов перед многочленами. В нем переопределены операции сложения (xor) и умножения (Умножение на 1 - тождественно. умножение на 2 - это умножение на x, остальное выводится из этих двух.). Используем для того, чтобы не выйти за пределы 1-байтных чисел.

1. Что будет если подать 1 байт?

Ответ: Дополняем 15 байт нулей

**DES**

<https://2hourscrypto.info/> - есть видео лекции, в шапке ссылки на них, там подробнее объясняется вроде

<https://youtu.be/mE_s-R5wvpw?t=2343> -- лекция Яндекса

<http://www.enlight.ru/crypto/algorithms/des/des00.htm>

1. Как генерируются раундовые ключи?
2. Как зашифруется файл, если он меньше 64 бит?

**RSA**

1. Знать как формируются ключи, от чего зависит открытый и закрытый ключ **(Кто ответил на это, напишите подробнее что вы говорили)**
2. Как вы возводили в степень?
3. Расширенный алгоритм Евклида - <http://fitp.ifmo.ru/shared/files/201111/1_278.pdf> 6 страница
4. Ну и алгоритм (лучше знать как именно в Вашем коде реализовано)

**Подпись**

1. Как формируется подпись  
   Прогнать документ через хэш-функцию, затем закодировать получившийся хэш приватным ключом RSA. Получившаяся подпись поставляется с документом, вместе с публичным ключом. При этом на публичный ключ имеется сертификат, что он принадлежит автору.

Алгоритмы хеширования знать не нужно, только названия  
SHA2, SHA3, MD6, мб еще что

1. Как проверяется подпись?  
   Подпись расшифровывается с публичным ключом. Документ прогоняется через такую же хэш-функцию, как при зашифровки. Сравниваем расшифрованную подпись и хэш. Если совпадают - все ок.

**Хаффман**

1. Какими могут быть коды значений по размеру?

Если смотреть по дереву то от 1 до 255 байт (смотря от реализации мб сразу биты у вас конечно)

1. Как хранится алфавит? Либо деревом, либо таблицей частот
2. И где хранится? (ну тут у каждого свое)
3. Как обрабатывается отступ до 8 бит, где хранится эта информация и как при расшифровке это работает?

Если максимальная длина 255, а была 8, то как файл может весить в итоге меньше - мы учитываем частоты, поэтому символы с коротким кодом компенсируют эту разницу.