Защита от копирования

1) **Какими требованиями должен обладать параметр к которому привязываешься?**
    a) УНИКАЛЬНОСТЬ (его нельзя подделать, например, имя учетной записи можно)
    b) НЕИЗМЕНЯЕМОСТЬ (он является важной частью компьютера, например, материнская плата, BIOS, HDD)
    c) ДОСТУПНОСТЬ
2) 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
3) **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.
4) **Как изменяется размер файла после шифрования?** Ответ: никак (тк шифруем посимвольно, один символ переводится ровно в один символ)
5) **Чем рефлектор отличается от ротора?**

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 -- еще хуйня какая-то

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

AES

https://habr.com/post/212235/ во если весь алгоритм нужен
https://youtu.be/mE_s-R5wvpw?t=3390 -- лекция Яндекса
https://youtu.be/CxU4ROAYGzs -- наглядная работа AES-128

1) **Как бороться с незаполненным до конца блоком?** Ответ: записываем все свободные байты числом свободных байт. Если блок заполнен полностью, добавляем в конец шифра блок, заполненный нулями.
   https://youtu.be/M_Ohbwoxf-E?t=868

2) **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.
3) **Почему числа Галуа не выходят за рамки 1-го байта?** Потому что старшие разряды отбрасываются
4) **Что будет если подать 1 байт?** Ответ: Дополняем 15 байт нулей
5) **Сколько раундов у тебя в проге?** (обычно 10)
6) **Сколько XOR с ключом делается за 10 раундов?** 11
7) **Сколько раундовых ключей?** 11
8) **Как работает mixColumns и почему так называется?** Потому что он перемешивает элементы в каждой колонке (лол?)
9) Как работает shiftRows?

RSA

https://youtu.be/M_Ohbwoxf-E?t=2601 -- лекция Яндекса

1) Знать как формируются ключи. От чего зависит открытый и закрытый ключ?
2) Как вы возводили в степень?
3) **Как вы проверяете числа на простоту?** (тут у каждого своё)
    a) Тест Миллера — Рабина: https://ru.wikipedia.org/wiki/Тест_Миллера_—_Рабина#Алгоритм_Миллера_—_Рабина, https://youtu.be/qdylJqXCDGs
4) **Расширенный алгоритм Евклида**. http://fitp.ifmo.ru/shared/files/201111/1_278.pdf 6 страница, https://youtu.be/K5nbGbN5Trs
5) **В чем заключается расширение?** Используем не только остаток, а здесь ещё и целую часть.
6) **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
2) **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)
2) **Как хранится алфавит?** Либо деревом, либо таблицей частот
3) **И где хранится?** (ну тут у каждого своё)
4) **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.

LZW

https://ru.wikipedia.org/wiki/Алгоритм_Лемпеля_—_Зива_—_Велча
https://habr.com/en/post/132683
https://youtu.be/j2HSd3HCpDs?t=132

1) **Что алгоритму надо знать для расшифровки?** Ничего
2) **Описать процесс расшифровки.** тут
3) **Что происходит, когда расшифровщик натыкается на символ из нижней части таблицы (>255)?** У него есть уже коды одинарных символов, так как он идёт по порядку, если код больше то он просто возьмёт сумму текущего и след. Вот тут есть снизу пояснение. Там словарь заполняется одинарными каждый раз перед началом прогона алгоритма, если такого символа нет, значит это несколько символов то он берет предыдущий + текущий и заносит в словарь.