1. надо знать как работает рса и на чем держится его безопасность, почему нарушитель зная e не может узнать d (потому что факторизация числа N - трудоемкая задача при больших размерностях N). Попросит зашифровать/расшифровать НЕ текстовый файл (в моем ридме шифруется обычный тхт). протестируйте на пдф или exe там - все должно работать. Может спросить про asn заголовок - лично я переделал формирование заголовка и добавил в отчет скриншот заголовка. МОжет попросить показать в зашифрованном файле заголовок (я это делаю утилитой dumpasn1). Также важно понимать что в лабе шифрование файла идет обычной шенцово-симметричной криптографией (а именно AES-CBC) а RSA мы юзаем ток чтобы зашифровать AES ключ и присобачить к файлу согласно заголовку ASN. Синхропосылка - я ебашу просто нули она поругала за это но пох. Ну и все вприцнипе. Ещё может спросить какой размер ключей должен быть у RSA (хотя бы 1024 бит но лучше 2048). Ещё может понадобиться - в крутых криптосистемах параметр е в двоичном виде имеет вид 10…01 это чтоб все быстро работало (не для безопасности)

2. Шарить за атаки, за их матчасть, быть готовым показать по коду и пояснить. Меня просила взять ручку тетрадку и прям математику написать как атакти работают. Я проебался с атакой винера - должен ей матчасть - прикрепляю сюда же. Потом в генерации параметров рса она меня просила доработать прогу чтоб параметры формировались именно по результаттам првоеденных атак, типа чтоб они потенциально не проходили. Тут просто важно понимать какие должны быть параметры RSA чтоб атаки не проходили - об этом я в отчете в выводе подробно расписал этого вроде достаточно

3. просто пояснить за атаку и за криптосистему RSA-OAEP которую реализовыввали тип зачем она нужна че не так с обычным RSA (я если честно хуй знает ей я ответил тип затем чтоб защищаться от этой атаки которую реализовали в этой лабе она вроде не поспорила с этим). Понимать надо зачем в криптосистеме соль и хеш от нее (чтобы атакер не подготовил дохуя коллизий второго рода)

4. Спрвшивала про то как работает алгоритм и в целом про эллиптические кривые и точки на них. Как минимум надо знать как складывать точки на ЭК. Читаем хабр https://habr.com/ru/post/335906/

5. Меня спросила ток про то ккак складывать точки на ЭК. Все. Но могу предположить что может спросить больше