Ассиметричные криптосистемы

1. Компания T разработала многопользовательскую систему передачи сообщений.

   Каждому абоненту предоставляется свой открытый ключ (n, e) и секретный ключ d системы RSA. Чтобы отправить сообщение абоненту A, необходимо взять его открытый ключ (n_A, e_A) и зашифровать сообщение на этом ключе.

   Ради экономии ресурсов, компания решила использовать одинаковый модуль n для всех абонентов.

   Расшифруйте перехваченный шифртекст c_A, предназначенный абоненту A, если вы законный пользователь системы с открытым ключем (n_B, e_B) и секретным ключем d_B.

2. Абонент A использует для получения сообщений систему шифрования RSA с публичным ключем (n, e).

   Известно, что ради ускорения процесса расшифрования была выбрана небольшая секретная экспонента d.
   Расшифруйте перехваченный шифртекст c.

3. Сгенерируйте эллиптическую кривую $E_{a,b}(\mathbb{Z}_p)$, удовлетворяющую требованиям стандарта ГОСТ-34.10-2012 такую, что все точки этой кривой имеют одинаковый порядок. В качестве характеристики поля взять любой из делителей модуля системы RSA из пункта 2.

4. Подпишите сообщение из пункта 1 используя ЭЦП ГОСТ-34.10-2012 и кривую, которая получена в пункте 3. Проверьте подпись.