Предпоследнее задание

1. В протоколе RSA выбраны $p = 17$, $q = 23$, $N = 391$, $e = 3$. Выберите ключ d и зашифруйте сообщение 41. Затем расшифруйте полученное сообщение и убедитесь, что получится исходное 41.

2. Пусть в протоколе RSA открытый ключ (N, e), $e = 3$. Покажите, что если злоумышленник узнаёт закрытый ключ d, то он может легко найти разложение N на множители.

3. Схема RSA позволяет также создавать защищенные электронные подписи. Если открытый ключ (N, e), то автор сообщения, обладающий закрытым ключом d, отправляет сообщение A^d, где A — незашифрованное сообщение. После этого идентификация подписи - это возведение в степень e. Пусть открытый ключ $(2021, 25)$. В какую степень автору нужно возвести сообщение, чтобы отправить его за своей электронной подписью?

4. Решите уравнение $\varphi(n) = 6$, где $\varphi(n)$ — функция Эйлера (количество чисел, не превосходящих n и взаимно простых с ним).

5. Докажите, что в шифре Шамира в итоге у B в действительности оказывается то сообщение, которое A планировал передать.

6. Докажите, что в шифре Эль-Гамаля в итоге у B в действительности оказывается то сообщение, которое A планировал передать.

7. Докажите, что в алгоритме шифрования Рабина B в итоге сможет найти исходное передаваемое сообщение среди $(\pm apm_q \pm bqm_p)$.

8. Рассмотрим алгоритм Sakurai и Takagi, напоминающий схему RSA. Выбирается модуль $N = pq$, где p и q — достаточно большие простые. Открытым ключом является пара (N, e), где e взаимно просто с $\varphi(N)$, а закрытый ключ Алисы имеет вид $d = e^{-1} \bmod ((p-1)(q-1))$. Для сообщения $m \in \mathbb{Z}_n$ выбирается случайно и равновероятно $r \in \mathbb{Z}_n^*$, зашифрованное сообщение имеет вид $c = f(r, m) = r^e(1 + mn) \pmod{n^2}$.

а) Докажите, что для всякого $c \in Z_{n^2}^*$ найдется единственный $r \in \mathbb{Z}_n^*$ и $m \in \mathbb{Z}_n$ такие, что $c = r^e(1 + mn) \pmod{n^2}$.

б) Покажите, как Алисе расшифровывать полученное сообщение c.

в) Заметим, что $f(r, m)f(\rho, \mu) = f(r\rho, m+\mu)$. Пусть Алиса получила от

Боба сообщение $f(r, m)$. Пусть Алиса достаточно доверчива и готова для Евы расшифровать произвольное зашифрованное ею сообщение. Покажите, как Еве действовать, чтобы выяснить m по $f(r, m)$, если Алиса согласна расшифровать для Евы одно любое сообщение $f(\rho, \mu)$ (но, конечно, что-то заподозрит, если попросить её расшифровывать непосредственно $f(r, m)$, и делать это откажется).