Контрольная работа №2 Вариант 1

Пожалуйста, впишите только ответы. Ход решения записывать не надо.

1. Вычислите *(2 балла)*:
   `29 mod -4` ☐ `31 mod 10` ☐
   `9 mod -2` ☐ `14 mod 4` ☐

2. Вычислите *(2 балла)*:
   `(960+864) * (528+169) в` Z_3 ☐ `(498-331) * (879-706) в` Z_5 ☐

3. Рассчитать обратное значение *(2 балла)*:
   `19 (mod 47)` ☐ `24 (mod 26)` ☐

4. Распишите шаги расширенного алгоритма Евклида для Упр. 3 *(2 балла)*:
   ☐

5. Вычислить *(2 балла)*: 2^{2804} в Z_2 ☐

6. Запишите разложение на простые множители и вычислите по формуле `phi(377)` *(2 балла)*:
   ☐

7. Пользователь системы RSA, выбравший `p = 13, q = 7` и `e = 5`, получил шифрованное сообщение `y = 63`. Написать, чему равен закрытый ключ, и дешифровать `y` *(3 балла)*.
   Ответ: d = ☐, dec(y) = ☐

8. У пользователя системы RSA есть открытая ключевая пара `(221, 13)`. Зашифровать с ее помощью сообщение `x = 7`, а также взломать код и расшифровать сообщение `y = 176` *(5 баллов)*.
   Ответ: p = ☐, q = ☐, phi = ☐, d = ☐, enc(x) = ☐, dec(y) = ☐