**1. Зашифрование сообщения.**

Дано значение модуля шифрования N, открытого ключа e и открытого текста X. Найти значение шифртекста Y, полученного при зашифровании X на открытом ключе (N, e) по алгоритму RSA.

N = 8633; e = 13; X = 688

**2. Расшифрование сообщения.**

Дано значение модуля шифрования N, открытого ключа e и шифртекста Y. Найти значение открытого текста X, который при зашифровании на открытом ключе (N, e) по алгоритму RSA дает Y (иными словами, расшифровать Y).

N = 209; e = 131; Y = 92

**3. Атака на шифр методом Ферма.**

Дано значение модуля шифрования N и открытого ключа e. Используя метод факторизации Ферма, найти значение закрытого ключа d.

N = 5917; e = 1103

**4. Атака методом перешифрования.**

Дано значение модуля шифрования N, открытого ключа e и шифртекста Y. Используя метод перешифрования, найти значение открытого текста X, не находя значения секретного ключа d.

N = 323; e = 7; Y = 86

**5. Атака методом бесключевого чтения.**

Два пользователя используют общий модуль N, но разные взаимно простые экспоненты e1 и e2. Пользователи получили шифртексты Y1 и Y2, которые были получены в результате зашифрования на экспонентах e1 и e2 соотетственно одного и того же сообщения X. Найти исходное сообщение X методом бесключевого чтения.

N = 1927; e1 = 7; e2 = 3; Y1 = 13; Y2 = 321

**6. Атака на основе китайской теоремы об остатках.**

Три пользователя имеют модули N1, N2, N3. Все пользователи используют экспоненту e = 3. Всем пользователям было послано некое сообщение X, причем пользователи получили шифртексты Y1, Y2, Y3. Найти открытый текст X, пользуясь атакой на основе китайской теоремы об остатках.

N1 = 115; N2 = 319; N3 = 141; Y1 = 48; Y2 = 35; Y3 = 38