Kid-RSA

1. (Kid–RSA) *Генерация ключей*:

   - Выбирает случайным образом натуральные числа a, b, A, B.
   - Вычисляет $M = ab - 1$, $e = AM + a$, $d = BM + b$, $n = (ed - 1)/M$.
   - *Открытым ключом* является пара (n, e), *секретным ключом* — число d.

   Процесс зашифрования. Если m — это открытый текст, то то шифртекст вычисляется по формуле $c = me \pmod{n}$.

   Процесс расшифрования. Если c — это шифртекст, то то открытый текст вычисляется по формуле $m = cd \pmod{n}$.

   Обоснуйте корректность алгоритма.

2. (a) Для $a = 3$, $b = 4$, $A = 5$, $B = 6$ вычислите открытый и секретный ключи.
   (b) Пусть открытым ключом является пара (n, e), полученная в предыдущем пункте. Зашифруйте сообщение $m = 314$.
   (c) Пусть $d = 70$ — секретный ключ, $n = 369$. Расшифруйте сообщение $c = 220$.
   (d) Известно, что открытым ключом Алисы является пара $(9083, 691)$. Некто прислала Алисе зашифрованное сообщение $c = 911$. Прочитайте его.

3. Известно, что натуральное число N является произведением двух простых чисел p и q. Зная значения функции Эйлера $\varphi(n) = m$, найдите p и q.

4. Докажите теорему Эйлера: если $(a, n) = 1$, то $a^{\varphi(n)} \equiv 1 \pmod{n}$.

5. (RSA для взрослых) *Генерация ключей*:

   - Выбрать большие простые числа p и q. Вычислить $n = pq$.
   - Выбрать $e \in \mathbb{Z}_n^*$, $(e, \varphi(n)) = 1$. Пара (n, e) является *открытым ключом.*
   - Вычислить $d = e^{-1} \pmod{\varphi(n)}$. Число d будет *секретным ключом.*

   Процесс зашифрования. Если m — это открытый текст, то то шифртекст вычисляется по формуле $c = m^e \pmod{n}$.

   Процесс расшифрования. Если c — это шифртекст, то открытый текст вычисляется по формуле $m = c^d \pmod{n}$.

6. Бернардо не утруждал себя изучением теории, поэтому в качестве открытого ключа RSA он выбрал пару $(n, e) = (799, 3)$. Зашифруйте для него сообщение $m = 11$. Аглая прислала Бернардо шифртекст $c = 56$. Пользуясь факторизацией Ферма, разложите на множители число n, найдите d и расшифруйте сообщение. В ответе вы получите год наиболее известного извержения Везувия.

7. Открытыми ключами Боба, Бориса и Бена являются $(1247, 3)$, $(629, 3)$ и $(589, 3)$ соответственно. Анна хочет отправить им одно и то же сообщение m. Она шифрует его, используя указанные открытые ключи, и отправляет три шифртекста $c_1 = 739$, $c_2 = 68$ и $c_3 = 430$ Бобу, Борису и Бену соответственно. Не находя секретные ключи Боба, Бориса и Бена, расшифруйте сообщение. Сделайте выводы.

   Если вы правильно расшифруете сообщение, то в ответе получите первое число Кармайкла.