Public-Key Encryption and the RSA Cryptosystem

1. An adversary can generate a list of plaintexts and associated ciphertexts, if the plaintext space is small. This requires only the public key. Then eavesdropped ciphertexts can be decrypted using that list.
2. Generate a large random prime p and a number e with $1 < e < p$. Compute d with $ed \equiv 1 \bmod p-1$. The encryption key is $k = (e, p)$. The plaintext and ciphertext space is $\mathbb{Z}_p^*$, the encryption function is $\mathcal{E}_k(m) = m^e \bmod p$, the decryption function is $\mathcal{D}_k(c) = c^d \bmod p$. The scheme provides correct decryption. Since the decryption key $d \equiv (e \bmod p)^{-1}$ can be easily derived from e and p using the Extended Euclidean Algorithm, this scheme is insecure as a public-key encryption scheme. It is rather a secret-key scheme.
3. a) $c = 100^5 \bmod 437 \equiv 85$.
   b) $N = 19 \cdot 23$, $\varphi(N) = 18 \cdot 22 = 396$, $d \equiv (5 \bmod 396)^{-1}$. Running the Extended Euclidean Algorithm on input 396 and 5 yields the equation $1 = 396 - 79 \cdot 5$. Hence $d = -79 \equiv 317 \bmod 396$.
   c) $m = c^d = 85^{317} \bmod 437 \equiv 100$.
4. Suppose $x \in \mathbb{Z}_N$ is chosen uniformly at random and $x \notin \mathbb{Z}_N^*$. Then an integer representative of x must be zero or a multiple of p or q. Since $\text{size}(p) = \text{size}(q) = n$ and $\text{size}\,(N) = 2n$, the probability of this being the case is negligible in n.
5. Let $e = 3$ and $N = 667$. Then ciphertexts c with $c = m^3 < 667$ are vulnerable, i.e., the plaintexts $m = 0, 1, \dots, 8$, their ciphertexts $c = 0, 1, 8, 27, 64, 125, 216, 343, 512$ and also their negatives modulo 667, i.e., $666, 659, 640, 603, 542, 451, 324, 155$. For $\text{size}\,(N) = 2048$ and $e = 2^{16} + 1 = 65537$, we infer from the inequality $m^{65537} < 2^{2048}$ that only $m = 0$ and $m = \pm 1 \bmod N$ are vulnerable.
6. a) $c = m^e \bmod N \equiv 66^{35} \equiv 66^{32} \cdot 66^2 \cdot 66 \equiv 35 \cdot 157 \cdot 66 \equiv 264 \bmod 323$. We use fast exponentiation: the sequence of modular squares of 66 is 157, 101, 188, 137, 35.
   b) $c_1 c_2 \bmod N \equiv 26 \cdot 213 \equiv 47 \bmod 323$ is the ciphertext of $m_1 m_2$, since $(m_1 m_2)^e = m_1^e m_2^e = c_1 c_2 \bmod 323$.
   Similarly, $c_1 c_2^{-1} \bmod N$ is the ciphertext of $m_1 m_2^{-1}$. We compute $c_2^{-1} \bmod N \equiv (213 \bmod 323)^{-1}$ by running the Extended Euclidean Algorithm on input $N = 323$ and $c_2 = 213$.

$323 : 213 = 1$ rem. 110	$323 = 213 + 110$	$110 = 323 - 213$
$213 : 110 = 1$ rem. 103	$213 = 110 + 103$	$103 = 213 - 110$
$110 : 103 = 1$ rem. 7	$110 = 103 + 7$	$7 = 110 - 103$
$103 : 7 = 14$ rem. 5	$103 = 14 \cdot 7 + 5$	$5 = 103 - 14 \cdot 7$
$7 : 5 = 1$ rem. 2	$7 = 5 + 2$	$2 = 7 - 5$
$5 : 2 = 2$ rem. 1	$5 = 2 \cdot 2 + 1$	$1 = 5 - 2 \cdot 2$

This yields:

$$\begin{aligned}\mathbf{1} &= 5 - 2 \cdot 2 = 5 - 2 \cdot (7 - 5) = 3 \cdot 5 - 2 \cdot 7 = 3 \cdot (103 - 14 \cdot 7) - 2 \cdot 7 \\ &= 3 \cdot 103 - 44 \cdot 7 = 3 \cdot 103 - 44 \cdot (110 - 103) = -44 \cdot 110 + 47 \cdot 103 \\ &= -44 \cdot 110 + 47 \cdot (213 - 110) = 47 \cdot 213 - 91 \cdot 110 = 47 \cdot 213 - 91 \cdot (323 - 213) \\ &= -91 \cdot 323 + 138 \cdot 213\end{aligned}$$

Hence $(213 \bmod 437)^{-1} \equiv 138$. The ciphertext is $26 \cdot 138 \bmod 323 \equiv 35$.

c) Mallory computes $y = s^e \bmod N = 5^{35} \bmod 323 \equiv 23$. Then

$$c' = y \cdot c \bmod N = 23 \cdot 104 \bmod 323 \equiv 131.$$

In a chosen ciphertext attack, he asks Bob to decrypt the ciphertext $c' = 131$. Bob returns $m' = (yc)^d = y^d c^d = sm \equiv 142$. Mallory computes $(5 \bmod 323)^{-1} \equiv 194$ using the Extended Euclidean Algorithm and finds the plaintext

$$m = s^{-1} m' \equiv 5^{-1} \cdot 142 \equiv 194 \cdot 142 \bmod 323 \equiv 93.$$

d) Fermat factorization of $N = 437$ gives $p = 19$ and $q = 17$. Thus $\varphi(N) = 288$. Compute $(35 \bmod 288)^{-1}$ using the Extended Euclidean Algorithm.

$288 : 35 = 8$ rem. 8	$288 = 8 \cdot 35 + 8$	$8 = 288 - 8 \cdot 35$
$35 : 8 = 4$ rem. 3	$35 = 4 \cdot 8 + 3$	$3 = 35 - 4 \cdot 8$
$8 : 3 = 2$ rem. 2	$8 = 3 \cdot 2 + 2$	$2 = 8 - 3 \cdot 2$
$3 : 2 = 1$ rem. 1	$3 = 2 + 1$	$1 = 3 - 2$

This gives:

$$\begin{aligned} \mathbf{1} &= 3 - 2 = 3 - (8 - 3 \cdot 2) = -8 + 3 \cdot 3 = -8 + 3 \cdot (35 - 4 \cdot 8) \\ &= -13 \cdot 8 + 3 \cdot 35 = -13(288 - 8 \cdot 35) + 3 \cdot 35 = -13 \cdot 288 + 107 \cdot 35 \end{aligned}$$

Hence $d = 35^{-1} \bmod 288 \equiv 107$.

7. Solve the following congruences using the Chinese Remainder Theorem:

$$c = 98 \bmod 901, \; c = 974 \bmod 2581, \; c = 2199 \bmod 4141$$

Set $N = N_1 N_2 N_3 = 901 \cdot 2581 \cdot 4141 = 9629816821$. The quotients of N by the three moduli N_i are $M_1 = 10687921$, $M_2 = 3731041$, $M_3 = 2325481$. The modular inverses $(M_i \bmod N_i)^{-1}$ are: $y_1 = -327$, $y_2 = 157$, $y_3 = 1251$. We obtain:

$$c = 98 y_1 N_1 + 974 y_2 N_2 + 2199 y_3 N_3 = 6625317842741 \bmod N = 3869893$$

We compute the real cube root and obtain $m = 157$.

8. a) The given sequence of modular squarings and multiplications yields the binary expansion of the private key. The first bit (MSB) must be 1. For the next bits, SQ (without MULT) corresponds to 0 and the combination SQ, MULT corresponds to 1. Hence $d = 1000\ 0110\ 0011 = 2147$.

b) $ed - 1 = 23616$ is a multiple of $\varphi(N)$, say $ed - 1 = k\varphi(N)$ with $k \in \mathbb{N}$. This gives the integer equation $\varphi(N) = \frac{ed-1}{k}$. One computes $\frac{ed-1}{k}$ for small integers k. The result should be somewhat smaller than N. For $k = 3$ one obtains $\frac{ed-1}{3} = 7872 = \varphi(N) = (p-1)(q-1) = pq - p - q + 1$. This implies $p + q = N + 1 - \varphi(N) = 180$, but p and q are still unknown. Since $pq = N = 8051$, the factors p and q are the zeros of the quadratic equation $x^2 - 180x + 8051$. This implies $x = 90 \pm \sqrt{90^2 - 8051}$. The solutions are $x_1 = p = 97$ and $x_2 = q = 83$.

9. The Fermat test is correct, since $a^{p-1} \equiv 1 \bmod p$ for prime numbers p and $a \not\equiv 0 \bmod p$. Now let $n = 561 = 3 \cdot 11 \cdot 17$. Then $\mathbb{Z}_n^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_{11}^* \times \mathbb{Z}_{17}^*$. The group orders are 2, 10 and 16, respectively. We have $n - 1 = 560$ and $560 \equiv 0 \bmod 2$, $560 \equiv 0 \bmod 10$ and $560 \equiv 0 \bmod 16$. Therefore, $a^{560} \equiv 1 \bmod n$ for all $a \in \mathbb{Z}_n^*$, and so 561 is a Carmichael number.

10. $n - 1 = 262 = 2 \cdot 131$. Hence $d = 131$ and $s = 1$.
Let $a = 3$. Then $gcd(3, 263) = 1$ and we compute $3^{131} \equiv 1 \bmod 263$. The Miller-Rabin algorithm outputs that n could be a prime.
Now let $a = 5$. Then $gcd(5, 263) = 1$ and we have $5^{131} \equiv 262 \equiv -1 \bmod 263$. Again, the test outputs that n could be a prime. In fact, $n = 263$ is a prime.

11. $c = m^e \bmod n = 2314^5 \bmod 10573 \equiv 6637$.
$\sqrt{10573} = 102.8$, $103^2 = 10609$, $10609 - 10573 = 36 = 6^2$. Hence $10573 = (103 - 6)(103 + 6) = 97 \cdot 109$. We have $(p - 1)(q - 1) = 10368$. Then $gcd(5, 10368) = 1$, i.e., $e = 5$ is admissible, whereas $gcd(3, 10368) = 3$, i.e., $e = 3$ is not admissible.
$d = 5^{-1} \bmod 10368 \equiv -4147 \equiv 6221 \bmod 10368$ (use the Extended Euclidean Algorithm).
$d_p = d \bmod (p - 1) \equiv 77$, $d_q = d \bmod (q - 1) \equiv 65$, $c_p = c \bmod p \equiv 41$, $c_q = c \bmod q \equiv 97$, $m_p = c_p^{d_p} \bmod p \equiv 83$, $m_q = c_q^{d_q} \bmod q \equiv 25$.
Running the Extended Euclidean Algorithm on input $p = 97$ and $q = 109$ gives

$$1 = 9p - 8q = 9 \cdot 97 - 8 \cdot 109.$$

Then the Chinese Remainder Theorem (CRT) gives

$$m = m_q(9p) + m_p(-8q) = -50551 \equiv 2314 \bmod 10573.$$

Without the CRT, we would have to compute

$$m = c^d \bmod N = 6637^{6221} \bmod 10573 \equiv 2314.$$

12. In this case, a divisor of N_1 and N_2 can be easily computed: $\gcd(N_1, N_2) = 10007$. Both moduli are insecure and we obtain the factorizations $N_1 = 10007 \cdot 10133$ and $N_2 = 10007 \cdot 11003$.

13. Since $(m^2)^e = (m^e)^2 = c^2 \bmod N$, the adversary only needs to square the ciphertext $\bmod N$. However, if an adversary modifies an RSA-OAEP ciphertext, then the data block DB which contains the plaintext m is almost certainly invalid. The result is a decryption error.

14. The ciphertext is $c = 2090^5 \bmod 10057 \equiv 1981$. Factorization with Fermat's method gives $N = 89 \cdot 113$, hence $\varphi(N) = 88 \cdot 112 = 9856$. Using the Extended Euclidean Algorithm, we obtain $d = (5 \bmod 9856)^{-1} \equiv -1971 \equiv 7855$.

15. Since $c = m^e = m^{(2^{16})} \cdot m \bmod N$, the encryption requires 17 modular multiplications. For decryption, the exponent d has almost the same size as N, i.e., 1024 bits. Thus the computation of $c^d \bmod N$ requires (at most) 1023 quadratures and 1023 multiplications modulo N, if fast exponentiation or the square-and-multiply algorithm is used. Hence at most 2046 modular multiplications are needed.

16. We have $\lceil \sqrt{N} \rceil = 46$. We are looking for smooth numbers $x^2 - N$ with respect to a factor base consisting of 2, 3, 5 and 7.

```
sage: N=2041
sage: for x in range(46,60):
          s=factor(x^2-N)
          print x, x^2 - N, "=", s
```

```
46 75 = 3 * 5^2
47 168 = 2^3 * 3 * 7
48 263 = 263
49 360 = 2^3 * 3^2 * 5
50 459 = 3^3 * 17
51 560 = 2^4 * 5 * 7
52 663 = 3 * 13 * 17
53 768 = 2^8 * 3
54 875 = 5^3 * 7
55 984 = 2^3 * 3 * 41
56 1095 = 3 * 5 * 73
57 1208 = 2^3 * 151
58 1323 = 3^3 * 7^2
59 1440 = 2^5 * 3^2 * 5
```

Let $x = 46 \cdot 47 \cdot 49 \cdot 51$ and $y = 2^5 \cdot 3^2 \cdot 5^2 \cdot 7$. Then $x^2 \equiv y^2 \bmod N$. We have $x \equiv 311$, $y \equiv 1416$ and $\gcd(1416 - 311,\ 2041) = 13$. Hence $N = 2041 = 13 \cdot 157$.

17. Let $N = 10573$ and $k = 2^3 3^3 = 216$; then $a^k - 1 \bmod N \equiv 1744$ and $\gcd(1744,\, N) = 109$. The method is successful since $N = 109 \cdot 97$ and $108 = 2^2 3^3 \mid k$, whereas $96 = 2^5 3 \nmid k$. However, choosing $k = 2^5 3^3 = 864$ would not work since k is divisible by 108 *and* 96.

18. If the random padding string is short and the number of possible plaintexts is small, then an adversary can conduct a brute-force attack by encrypting all combinations of plaintexts and padding strings.