① Coding exercise.

② 1. $x = \underset{a_1}{3} \bmod \underset{b_1}{7}$ and $x = \underset{a_2}{5} \bmod \underset{b_2}{9}$

- Compute T, i.e., $7^{-1} \bmod 9$:

$9 = 7 \cdot 1 + 2$

$7 = 2 \cdot 3 + 1 \Rightarrow 1 = 7 - 2 \cdot 3$

$= 7 - (9 - 7 \cdot 1)3$

$= 4 \cdot 7 - 3 \cdot 9 \Rightarrow 4 \cdot 7 = 1 \bmod 9 \Rightarrow 7^{-1} \bmod 9 = 4$

Compute $\gcd(7,9)$ using Euclidean algo. | Reverse it to write $\gcd(7,9)=1$ as a linear comb. of 7 and 9 | Reduce it mod 9 so that $-3 \cdot 9$ disappears since $9 \equiv 0 \bmod 9$. | Follows by definition of inverse in modulo

- Compute u, i.e., $(5-3) \cdot 4 \bmod 9 = 8$.

- Compute x, i.e., $3 + 8 \cdot 7 = 59$

2. In the computation of T, number of steps is mainly determined by number of steps in the Euclidean algorithm, and Euclidean algo. terminates in finite no. of steps since in each step remainder is smaller than the one previous remainder and set of remainders is bounded from below by 0. Computation of u and x are clearly finite many steps.

Output is correct, and we can check this by replacing final output x into given equations: $x = a_1 + u \cdot b_1 \bmod b_1 = a_1 \bmod b_1$ since $b_1 \equiv 0 \bmod b_1$

$$x = a_1 + u \cdot b_1 \bmod b_2 = a_1 + (a_2 - a_1) T \cdot b_1 \bmod b_2$$
$$= a_1 + (a_2 - a_1) b_1^{-1} \cdot b_1 \bmod b_2$$
$$= a_1 + (a_2 - a_1) \cdot 1 \bmod b_2 = a_2 \bmod b_2$$

③ 1. $c = m^e = m^{2^{16}+1} = m^{2^{16}} \cdot m \bmod N$ and $m^{2^{16}} = m^{2^{15}} \cdot m^{2^{15}} \bmod N$

1 mult.

$m^{2^{15}} = m^{2^{14}} \cdot m^{2^{14}} \bmod N$

$\vdots$

$m^{2^1} = m \cdot m \bmod N$

16 mult.

2. Let $sk' = (d, p, q) \leftarrow \text{Keygen}()$, then $\text{Dec}(sk, c)$ should compute $c^d \bmod N$. We can do this by computing $c^d \bmod p$ and $c^d \bmod q$, then apply CRT to compute unique solution $c^d \bmod N$.

3. Coding exercise.

Hint: When you have mod N in the base, you can work in mod $\varphi(N)$ in the power. You need to compute $m = c^d \bmod N$, instead compute $m = c_p^{d_p} \bmod p$ and $m = c_q^{d_q} \bmod q$ where $d_p = d \bmod \varphi(p)$, $d_q = d \bmod \varphi(q)$, $c_p = c \bmod p$, $c_q = c \bmod q$. Then apply CRT.

4. Assume $e = 2^{16} + 1$ and $|\varphi(N)| = 2000$ bits.

Recall that $d = e^{-1} \bmod \varphi(N)$, i.e., $e \cdot d = 1 \bmod \varphi(N)$. This means $e \cdot d = 1 + k \cdot \varphi(N)$ for some $k \in \mathbb{Z}$ over integers. Then $d = \frac{1 + k \cdot \varphi(N)}{e}$. Observe that $|1 + k \cdot \varphi(N)| \geq 2000$ bits and $|e| = 17$. So, $|d| \geq 2000 - 17 > 1980$

④ 1. $\varphi(N)$ is the number of integers from 1 to N that are relatively prime with N.

Consider $N = p \cdot q$ for different primes p and q, then any integer in $\{1, \cdots, N\}$ is relatively prime with N as long as it is not a multiple of p or q. So

$\varphi(N) = (p-1)(q-1) = pq - (p+q) + 1$.

Given $\varphi(N)$ and N, $N - \varphi(N) + 1 = pq - (pq - (p+q) + 1) + 1 = p + q$.

2. Roots of a degree two poly. $p(x) = ax^2 + bx + c$ are $\frac{\sqrt{\Delta} - b}{2a}$ and $\frac{-\sqrt{\Delta} - b}{2a}$, $\Delta = b^2 - 4ac$

Roots of $f(x)$ are clearly p and q since $f(p) = f(q) = 0$. Given N and $p+q$ (by 1) we can construct $f(x) = x^2 - (p+q)x + N$ and apply above formula to compute the roots p and q.