Instructions. Answer each of the questions on your own paper, and be sure to show your work so that partial credit can be adequately assessed. Put your name on each page of your paper.

1. [20 Points]
   (a) State Euler’s Theorem precisely. Be sure to carefully state the requisite hypotheses.
   (b) Compute $\varphi(100)$. As usual $\varphi(n)$ denotes the Euler $\varphi$-function applied to $n$.
   (c) Compute $7^{523} \mod 100$.
   (d) What are the last two digits in the ordinary decimal expansion of $7^{523}$?

2. [15 Points] Suppose that the RSA algorithm starts with an enciphering key $(e, n) = (11, 2867)$ where the enciphering exponent $e = 11$ and the modulus $n = 2867 = 47 \times 61$.
   (a) What is the congruence that must be solved to compute the deciphering exponent $d$?
   (b) Solve this congruence to compute $d$.

3. [30 Points] The following two permutations in $S(7)$ are given in two-rowed notation:
   \[
   \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 2 & 1 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 6 & 7 & 2 & 1 & 3 \end{pmatrix}.
   \]
   (a) Compute the products $\sigma \tau$ and $\tau \sigma$. Express your answers in two-rowed notation. Are these two products equal?
   (b) Compute $\sigma^{-1}$. Again express your answer in two-rowed notation.
   (c) Write each of $\sigma$, $\tau$, $\sigma \tau$ and $\tau \sigma$ as a product of disjoint cycles.
   (d) Compute the order and parity of each of the elements $\sigma$, $\tau$, $\sigma \tau$, and $\tau \sigma$.

4. [20 Points] Suppose that $X = \{a, b, c\}$ so that $|X| = 3$ where $|X|$ is the number of elements of $X$.
   (a) How many different subsets does $X$ have?
   (b) How many elements are there in the set $X \times X$?
   (c) How many different functions $f : X \to X$ are there?
   (d) How many different bijective functions $f : X \to X$ are there?

5. [15 Points] Let $X$ be the set $\{1, 2, 3, 4\}$ and let
   \[ R = \{(1, 1), (1, 4), (2, 2), (2, 3), (3, 2), (3, 3), (4, 1), (4, 4)\}. \]
   (a) Write the adjacency matrix $M(R)$ of $R$.
   (b) Verify that $R$ is an equivalence relation and write down the equivalence classes.