This examination consists of 5 problems, which are subdivided into 9 questions, where each question counts for the explicitly given number of points, adding to a total of **44 points**. Please write your answers in the spaces indicated, or below the questions, using the back of the sheets for completing the answers and for all scratch work, if necessary. You are allowed to consult two 8.5in × 11in sheets with notes, but not your book or your class notes. If you get stuck on a problem, it may be advisable to go to another problem and come back to that one later.

You will have **60 minutes** to do this test.

Problem 1 _____

2 _____

3 _____

4 _____

5 _____

Total _____
Problem 1 (12 points)

(a, 4pts) True or false:

\[ \forall n \in \mathbb{Z}_{\geq 2}, a, b \in \mathbb{Z}: a \equiv b \pmod{n} \implies \gcd(a,n) = \gcd(b,n). \]

Please explain.

(b, 4pts) Please show that \( \phi(10^i) = 4 \cdot 10^{i-1} \) for all \( i \in \mathbb{Z}_{>0} \), where \( \phi \) is Euler’s totient function.

(c, 4pts) Please give the definition for being a pseudo-prime and the definition for being Carmichael number.
Problem 2 (6 points): Please prove for all integers $n \geq 1$ that $5^{2n} + 3 \cdot 2^{5n-2}$ is divisible by 7.

Problem 3 (6 points): Please compute residues $x, y \in \mathbb{Z}_7$ such that $3x + 5y \equiv 0 \pmod{7}$ and $5x + y \equiv 1 \pmod{7}$. Please show all your work.
Problem 4 (8 points): Consider $504 = 7 \cdot 8 \cdot 9$ and let $a \in \mathbb{Z}_{504}$ with

$$a \equiv 6 \pmod{7},$$
$$a \equiv 7 \pmod{8},$$
$$a \equiv 8 \pmod{9}.$$

Please compute $y_0 \in \mathbb{Z}_7$, $y_1 \in \mathbb{Z}_8$ and $y_2 \in \mathbb{Z}_9$ such that

$$a = y_0 + y_1 \cdot 7 + y_2 \cdot 7 \cdot 8.$$

Please show all your work. After seeing the answer, is there an easy way to interpret the result?
Problem 5 (12 points):

(a, 4pts) Consider the following instance of the RSA: the public modulus is $K = 55$ and the public (enciphering) exponent is $W = 9$. Please compute the private deciphering exponent $X$ such that $(M^9)^X \equiv M \pmod{55}$ (at least for all $M \in \mathbb{Z}_{55}$ that are relatively prime to $K$).

(b, 4pts) In the RSA, for all public keys $K$ and encryption exponents $W$ it is unwise to encrypt messages $M$ that are not relatively prime to $K$. Why? Please explain.

(c, 4pts) The original 1977 RSA public key crypto system has the flaw that it is malleable. What does that mean?