Note: Due Wednesday, Mar. 13th at midnight;
Each problem is worth equal points (10 points).

7 common problems for everyone, 10 problems in total (3 additional ones):

Problems 12.2, 12.3, and 13.8 from the textbook;
Note: for 13.8, there's a typo: $V_i=E(K_i, U_i)$, instead of $V_i=E(k_i, U_i)$.

Problem 4: The following two sub problems involve Fermat's Theorem (same as problems 2.20 and 2.22 from the textbook).

(a) Using Fermat's Theorem, find $3^{201} \bmod 11$.

(b) Using Fermat's Theorem, find a number x between 0 and 28 with x^{85} congruent to 6 modulo 29. (you should not use any brute-force searching)

Problem 5: The following two sub problems involve Euler's Theorem (same as problems 2.23 and 2.24 from the textbook).

(a) Using Euler's Theorem, find a number a between 0 and 9 such that a is congruent to $7^{1000} \bmod 10$. (note: this is the same as the last digit of the decimal expansion of 7^{1000})

(b) Using Euler's Theorem, find a number x between 0 and 28 with x^{85} congruent to 6 modulo 35. (you should not use any brute-force searching)

Problem 6: Suppose Fred sees your RSA signature on m_1 and on m_2 (i.e. he sees $m_1^d \bmod n$ and $m_2^d \bmod n$). How does he compute the signature on each of these messages: $m_1^j \bmod n$ (for positive integer j), $m_1^{-1} \bmod n$, $m_1 \cdot m_2 \bmod n$, and in general $m_1^j \cdot m_2^k \bmod n$ (for arbitrary integers j and k)?

Problem 7: Suppose Alice and Bob know each other's public key. Alice sends a message to Bob. How can she encrypt the message so that, when Bob receives it, he is sure about all of the following?

(1) Nobody else can view the content (confidentiality),
(2) The message is from Alice and no one has modified it (authentication, integrity).
(3) Nobody else (Eve) could trick Bob into thinking that Eve also generated the same message.

Additional problems for 471 students only:

Problems 9.3, 9.8, and 11.1, all from textbook.

Additional problems for 571 students only:

Problems 9.18, 11.3, and 12.9, all from the textbook;
Hint: for 11.3 (b), you can use the quadratic residue problem:
https://en.wikipedia.org/wiki/Quadratic_residuosity_problem
(Or, taking square roots modulo a large composite integer n is considered to be infeasible)