

Final exam KAP 2026

Solve at least 4 of the following problems.

JUSTIFY YOUR ANSWERS! (No credits for answers without explanation).

Problem 1. a) Compute $GCD(546, 137)$ and write the Bézout identity.

b) Find the multiplicative inverse of $\overline{137}$ in $\mathbb{Z}/546\mathbb{Z}$.

Problem 2. Show that each of the following statements is false by giving a counterexample:

a) for every integer $n \geq 1$, if 3 divides n then 3 divides $\varphi(n)$;

b) for every integer $n \geq 1$, if 3 divides $\varphi(n)$ then 3 divides n .

Problem 3. (a) Compute the order of $(\bar{2}, \bar{2})$ in $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

(b) Compute the order of $(\bar{2}, \bar{2})$ in $(\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/7\mathbb{Z})^*$.

Problem 4. Given the relation $114 \cdot 3543 - 1333 \cdot 303 = 3$,

a) determine

$$\gcd(3543, 303), \quad \gcd(114, 1333), \quad \gcd(114, 303);$$

b) determine which of the following inverses exist

$$\overline{114}^{-1} \in (\mathbb{Z}/1333\mathbb{Z})^*, \quad \overline{303}^{-1} \in (\mathbb{Z}/114\mathbb{Z})^{-1}, \quad \overline{101}^{-1} \in (\mathbb{Z}/38\mathbb{Z})^{-1};$$

c) determine the inverses of point b), when they exist.

Problem 5. Consider $N = 7933$ (N is a prime number). Compute

$$a) 2^{15868} + N^{15} \mod N, \quad b) 2^{15868} + N^{15} \mod 3N.$$

Problem 6. a) Determine a primitive root modulo 41.

b) How many primitive roots are there modulo 41?

c) If g is a primitive root modulo 41, which of the following powers of g are primitive roots?

$$g^8, \quad g^9, \quad g^{10}, \quad g^{11}.$$

Problem 7. Let $N = 101 \cdot 53$, $E = 19$ and $D = 4379$.

a) Verify that N , E , D above are a set of RSA keys.

b) Encrypt the message $m = 11$ with above keys (it is sufficient to write the formula, without calculations).

Problem 8. Mr. White and Mr. Red agree on the prime $p = 23$ and on the primitive root $g = 5$. Mr. White has the secret key $k_w = 10$ and Mr. Red has the secret key $k_r = 15$. After the Diffie-Hellman key exchange, what is their shared key?