

Solutions – Final Exam KAP 2026

Problem 1

a)

Use the Euclidean algorithm:

$$546 = 3 \cdot 137 + 135$$

$$137 = 1 \cdot 135 + 2$$

$$135 = 67 \cdot 2 + 1$$

Hence,

$$\gcd(546, 137) = 1.$$

Now compute the Bézout identity:

$$1 = 135 - 67 \cdot 2$$

and since

$$2 = 137 - 135,$$

we get

$$1 = 135 - 67(137 - 135)$$

$$= 68 \cdot 135 - 67 \cdot 137.$$

Using

$$135 = 546 - 3 \cdot 137,$$

we obtain

$$1 = 68(546 - 3 \cdot 137) - 67 \cdot 137$$

$$= 68 \cdot 546 - 271 \cdot 137.$$

Therefore the Bézout identity is

$$1 = 68 \cdot 546 - 271 \cdot 137.$$

b)

From the Bézout identity,

$$-271 \cdot 137 \equiv 1 \pmod{546}.$$

Hence,

$$137^{-1} \equiv -271 \equiv 275 \pmod{546}.$$

$$\boxed{137^{-1} = 275 \text{ in } \mathbb{Z}/546\mathbb{Z}}$$

Problem 2

a)

The statement is false.

Take

$$n = 3.$$

Then

$$3 \mid n,$$

but

$$\varphi(3) = 2,$$

and

$$3 \nmid 2.$$

Hence the statement is false.

b)

The statement is false.

Take

$$n = 7.$$

Then

$$\varphi(7) = 6,$$

so

$$3 \mid \varphi(7),$$

but

$$3 \nmid 7.$$

Hence the statement is false.

Problem 3

a)

In the additive group

$$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z},$$

the order of

$$(\bar{2}, \bar{2})$$

is

$$\text{lcm}(5, 7) = 35.$$

Therefore,

$$\boxed{\text{ord}(\bar{2}, \bar{2}) = 35}$$

b)

Now consider the multiplicative group

$$(\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/7\mathbb{Z})^*.$$

Modulo 5:

$$2^4 \equiv 1 \pmod{5},$$

and no smaller positive exponent works, hence

$$\text{ord}_5(2) = 4.$$

Modulo 7:

$$2^3 = 8 \equiv 1 \pmod{7},$$

thus

$$\text{ord}_7(2) = 3.$$

Therefore,

$$\text{ord}(2, 2) = \text{lcm}(4, 3) = 12.$$

$$\boxed{\text{ord}(2, 2) = 12}$$

Problem 4

We are given

$$114 \cdot 3543 - 1333 \cdot 303 = 3.$$

a)

Since 3 is a linear combination of 3543 and 303,

$$\gcd(3543, 303) = 3.$$

Similarly, 3 is also a linear combination of 114 and 303, hence

$$\gcd(114, 303) = 3.$$

Now compute $\gcd(114, 1333)$:

$$1333 = 11 \cdot 114 + 79$$

$$114 = 1 \cdot 79 + 35$$

$$79 = 2 \cdot 35 + 9$$

$$35 = 3 \cdot 9 + 8$$

$$9 = 1 \cdot 8 + 1.$$

Thus,

$$\gcd(114, 1333) = 1.$$

Therefore,

$$\boxed{\gcd(3543, 303) = 3}$$

$$\boxed{\gcd(114, 1333) = 1}$$

$$\boxed{\gcd(114, 303) = 3}$$

b)

An inverse modulo m exists if and only if the number is coprime with m .

Since

$$\gcd(114, 1333) = 1,$$

the inverse

$$114^{-1} \in (\mathbb{Z}/1333\mathbb{Z})^*$$

exists.

Since

$$\gcd(303, 114) = 3 \neq 1,$$

the inverse

$$303^{-1} \in (\mathbb{Z}/114\mathbb{Z})^*$$

does not exist.

Finally,

$$101 \equiv 25 \pmod{38},$$

and

$$\gcd(101, 38) = 1,$$

therefore

$$101^{-1} \in (\mathbb{Z}/38\mathbb{Z})^*$$

exists.

c)

Using the extended Euclidean algorithm:

$$1 = -152 \cdot 114 + 13 \cdot 1333.$$

Hence,

$$114^{-1} \equiv -152 \equiv 1181 \pmod{1333}.$$

Thus,

$$\boxed{114^{-1} = 1181 \pmod{1333}}$$

Now compute $101^{-1} \pmod{38}$.

Since

$$101 = 2 \cdot 38 + 25,$$

we solve:

$$1 = -3 \cdot 101 + 8 \cdot 38.$$

Hence,

$$101^{-1} \equiv -3 \equiv 35 \pmod{38}.$$

Therefore,

$$\boxed{101^{-1} = 35 \pmod{38}}$$

Problem 5

Let

$$N = 7933,$$

where N is prime.

a)

Compute

$$2^{15868} + N^{15} \pmod{N}.$$

Since

$$N^{15} \equiv 0 \pmod{N},$$

it remains to compute

$$2^{15868} \pmod{N}.$$

Because N is prime, Fermat's theorem gives

$$2^{N-1} = 2^{7932} \equiv 1 \pmod{N}.$$

Now

$$15868 = 2 \cdot 7932 + 4,$$

thus

$$2^{15868} \equiv 2^4 = 16 \pmod{N}.$$

Therefore,

$$\boxed{2^{15868} + N^{15} \equiv 16 \pmod{N}}$$

b)

Now compute modulo $3N$.

First work modulo N :

$$2^{15868} + N^{15} \equiv 16 \pmod{N}.$$

Now modulo 3:

$$2 \equiv -1 \pmod{3},$$

and since 15868 is even,

$$2^{15868} \equiv 1 \pmod{3}.$$

Also,

$$7933 \equiv 1 \pmod{3},$$

hence

$$N^{15} \equiv 1^{15} = 1 \pmod{3}.$$

Therefore,

$$2^{15868} + N^{15} \equiv 1 + 1 = 2 \pmod{3}.$$

We now solve the system

$$x \equiv 16 \pmod{7933}$$

$$x \equiv 2 \pmod{3}.$$

Write

$$x = 16 + 7933k.$$

Reducing modulo 3:

$$16 + 7933k \equiv 2 \pmod{3}.$$

Since

$$16 \equiv 1 \pmod{3}, \quad 7933 \equiv 1 \pmod{3},$$

we obtain

$$1 + k \equiv 2 \pmod{3},$$

thus

$$k \equiv 1 \pmod{3}.$$

Taking $k = 1$,

$$x = 16 + 7933 = 7949.$$

Hence,

$2^{15868} + N^{15} \equiv 7949 \pmod{3N}$
--

Problem 6

a)

A primitive root modulo 41 is

$$g = 6.$$

b)

The number of primitive roots modulo 41 is

$$\varphi(40).$$

Since

$$40 = 2^3 \cdot 5,$$

we have

$$\varphi(40) = 40 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 16.$$

Therefore,

$$\boxed{16}$$

primitive roots exist modulo 41.

c)

If g is a primitive root modulo 41, then g^k is primitive iff

$$\gcd(k, 40) = 1.$$

Now:

$$\gcd(8, 40) = 8$$

not primitive.

$$\gcd(9, 40) = 1$$

primitive.

$$\gcd(10, 40) = 10$$

not primitive.

$$\gcd(11, 40) = 1$$

primitive.

Hence the primitive roots are

$$\boxed{g^9 \text{ and } g^{11}}.$$

Problem 7

Given

$$N = 101 \cdot 53, \quad E = 19, \quad D = 4379.$$

a)

First compute

$$N = 5353.$$

Then

$$\varphi(N) = (101 - 1)(53 - 1) = 100 \cdot 52 = 5200.$$

To verify RSA keys we check:

$$ED \equiv 1 \pmod{\varphi(N)}.$$

Indeed,

$$19 \cdot 4379 = 83201,$$

and

$$83201 \equiv 1 \pmod{5200}.$$

Hence the keys are valid RSA keys.

b)

To encrypt the message $m = 11$,

$$c \equiv m^E \pmod{N}.$$

Therefore,

$$c \equiv 11^{19} \pmod{5353}$$

Problem 8

Given

$$p = 23, \quad g = 5,$$

Mr. White chooses

$$k_w = 10,$$

and Mr. Red chooses

$$k_r = 15.$$

The shared Diffie–Hellman key is

$$K = g^{k_w k_r} \pmod{p}.$$

Thus,

$$K = 5^{150} \pmod{23}.$$

Computing the power modulo 23,

$$K = 6.$$

Therefore,

$$\boxed{6}$$

is the shared secret key.