If your answers do not fit on the page, use some other paper page. it is OK to write multiple names, values, and formulas on one line.

Scan the page(s) and submit the resulting image file into **Exercise7** folder.

All given numbers (the parameter names and values, it is OK to write multiple numbers on one line)

$$P = 7, \quad q = 37, \quad C = 257, \quad d = 137, \quad M = 65$$

While calculating ciphertext number C

All calculated numbers (the parameter names and values)

$$n = 259, \quad \phi(n) = 216, \quad C = 151$$

All formulas that you used to calculate them

$$n = P \times q = 7 \times 37 = 259 \quad \phi(n) = (P-1)(q-1) = 6 \times 36 = 216$$

$$C = M^e \% n = 65^{257} \% 259 = 151$$

While calculating plaintext number M'

All calculated numbers s (the parameter names and values)

$$M = 65$$

All formulas that you used to calculate them

$$M = C^d \% n = 151^{137} \% 259 = 65$$

Below write just the names, not actual values

What numbers Bob shall communicate to everybody?

e and n

What numbers Bob shall keep to himself?

d and n

What numbers Alice can safely show to other people (so the people still cannot read her message to Bob)?

d   d   and   Ciph

What numbers Alice has to calculate before sending the encrypted message?

$$M^e \,\%\, n = C$$

What numbers Bob has to calculate before decrypting the message (except the numbers communicated to everybody)?

d   Since $C^d \,\%\, n = M$