SDU
DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE

# Questions and Answers

## Exercise 1 (*Casesar Cipher*)

a) What does "ZQOØQOØ, RI." say?

b) What does this say about how many keys should be possible?

**Solution 1**

- "RIGTIGT, JA."
- There must be so many keys that it is infeasible to ever enumerate and try them.

## Exercise 2 (*Introduction to Number Theory*)

a) $15 \equiv 22 \pmod 7$?

b) $15 \equiv 1 \pmod 7$?

c) $15 \equiv 37 \pmod 7$?

d) $58 \equiv 22 \pmod 9$?

**Solution 2**

- $15 \equiv 22 \equiv 1 \pmod 7 \implies 15 = 2 \cdot 7 + 1;\ 22 = 3 \cdot 7 + 1 \ \to$ correct
- $15 \equiv 1 \pmod 7 \implies 15 = 2 \cdot 7 + 1 \ \to$ correct
- $15 \equiv 37 \pmod 7 \implies 37 = 35 + 2 = 5 \cdot 7 + 2 \ \to$ wrong
- $58 \equiv 22 \pmod 9 \implies 58 = 54 + 4 = 6 \cdot 9 + 4;\ 22 = 18 + 4 = 2 \cdot 9 + 4 \ \to$ correct

## Exercise 3 (*RSA Example*)

Compute RSA keys using $N = 35$, $e = 11$.

a) What are $p_A$ and $q_A$?

b) What is $d$? Try $d = 11$ and check it.

c) Encrypt $4$. Decrypt the result.

**Solution 3**

- $p_A = 5$ and $q_A = 7$
  $\Rightarrow (p_A - 1)(q_A - 1) = 24$
- $e_A = 11$ and $d_A = 11$.
  $e_A \cdot d_A \equiv 121 \equiv 1 \pmod{24}$
- $m = 4$
  $c = m^{e_A} \pmod{N_A} = 4^{11} \pmod{35} = 9$
  $r = c^{d_A} \pmod{N_A} = 9^{11} \pmod{35} = 4$

## Exercise 4 (*RSA Inversion*)

Calculate the following:

a) $gcd(6,9)$

b) $s$ and $t$ such that $s \cdot 6 + t \cdot 9 = gcd(6,9)$

c) $gcd(15,23)$

d) $s$ and $t$ such that $s \cdot 15 + t \cdot 23 = gcd(15,23)$

### Solution 4

- $gcd(6,9) = 3$ and $s$ and $t$ such that $s \cdot 6 + t \cdot 9 = gcd(6,9)$:

| $n$ | $q$ | $d$ | $s$ | $t$ |
|---|---|---|---|---|
| 0 | – | $b = 9$ | 0 | 1 |
| 1 | – | $a = 6$ | 1 | 0 |
| 2 | $\lfloor 9/6 \rfloor = 1$ | $9 - 1 \cdot 6 = 3$ | $0 - 1 \cdot 1 = -1$ | $1 - 1 \cdot 0 = 1$ |
| 3 | $\lfloor 6/3 \rfloor = 2$ | $6 - 2 \cdot 3 = 0$ | | |

$s = -1$, $t = 1$, $gcd(6,9) = 3$

$s \cdot 6 + t \cdot 9 = -1 \cdot 6 + 1 \cdot 9 = gcd(6,9) = 3$

- $gcd(15,23)$ and $s$ and $t$ such that $s \cdot 15 + t \cdot 23 = gcd(15,23)$:

| $n$ | $q$ | $d$ | $s$ | $t$ |
|---|---|---|---|---|
| 0 | – | $b = 23$ | 0 | 1 |
| 1 | – | $a = 15$ | 1 | 0 |
| 2 | $\lfloor 23/15 = 1 \rfloor$ | $23 - 1 \cdot 15 = 8$ | $0 - 1 \cdot 1 = -1$ | $1 - 1 \cdot 0 = 1$ |
| 3 | $\lfloor 15/8 = 1 \rfloor$ | $15 - 1 \cdot 8 = 7$ | $1 - 1 \cdot (-1) = 2$ | $0 - 1 \cdot 1 = -1$ |
| 4 | $\lfloor 8/7 = 1 \rfloor$ | $8 - 1 \cdot 7 = 1$ | $-1 - 1 \cdot 2 = -3$ | $1 - 1 \cdot (-1) = 2$ |
| 5 | $\lfloor 7/1 = 7 \rfloor$ | $7 - 7 \cdot 1 = 0$ | | |

$s = -3$, $t = 2$, $gcd(15,23) = 1$

$s \cdot 15 + t \cdot 23 = -3 \cdot 15 + 2 \cdot 23 = gcd(15,23) = 1$

$\Rightarrow -3 \cdot 15 = 1 \pmod{23}$

$\Rightarrow -3 + 23 \cdot 15 = 1 \pmod{23}$

$\Rightarrow 20 \cdot 15 = 1 \pmod{23}$

## Exercise 5 (*Combining Symmetric and Public Key Systems*)

How does Bob decrypt? Why is this efficient?

### Solution 5

Bob first decrypt the RSA-encrypted encapsulates key and then the actual message using that key.

This is efficient, since only a 128-256 bit long symmetric key needs to be encrypted using RSA and not a message of arbitrary length.