NTNU Department of Information Security and Communication Technology

TTM4135 Applied Cryptography and Network Security
Semester Spring, 2023

Worksheet 1: Introduction and discrete mathematics

QUESTION 1

Review the definitions of the following terms given in the lectures slides. You may be expected to know these for the final examination.

- confidentiality
- integrity
- availability
- entity authentication
- data origin authentication
- non-repudiation
- group generator
- finite field.

QUESTION 2

Visit the National Vulnerability Database http://nvd.nist.gov/. Choose the search page https://nvd.nist.gov/vuln/search and then find out, using the search function, how many security vulnerabilities have been issued in the last three months for:

- common desktop and mobile operating systems;
- popular web browsers.

What are you (or should you be) doing to minimise the impact of these on your own systems?

QUESTION 3

For each of the following applications consider threats concerning each of: confidentiality, integrity, and availability. Which type of threat would you rate as most important in each case, and why?

(a) An online medical database
(b) A mobile banking application
(c) A supermarket website

QUESTION 4

Determine $\gcd(23, 29)$, $\gcd(893, 703)$ and $\gcd(1045, 77)$ using Euclid's algorithm.

cont/...

QUESTION 5

Without using a calculator of any kind, compute the following values of $a \bmod b$ and write each a value as $a = bq + r$ where $r < b$.

(a) $35 \bmod 31$
(b) $3 \bmod 1000$
(c) $65 \bmod 21$
(d) $236 \bmod 5$
(e) $123 \bmod 3$

QUESTION 6

Use the Euclidean algorithm to find which of the following inverses exist. For those that do exist use back substitution to find the inverse.

(a) $3^{-1} \bmod 31$
(b) $21^{-1} \bmod 91$
(c) $39^{-1} \bmod 195$
(d) $41^{-1} \bmod 195$

QUESTION 7

Demonstrate that $\mathbb{Z}_5$ is a field by writing out the addition and multiplication tables. (What do you need to check in the tables?)

QUESTION 8

(a) How many elements are there in $\mathbb{Z}_{11}^*$? Find a generator for this group.
(b) How many elements are there in $\mathbb{Z}_{12}^*$? Does this group have a generator?

QUESTION 9

Suppose that we try to define $GF(2^8)$ in a different way by defining multiplication of two strings to be multiplication modulo 2^8. Show that this would *not* satisfy the requirements to be a field.

QUESTION 10

Write the XOR operation ($\oplus$) as a Boolean truth table. Then show, using their truth tables, that $z = x_1 \vee x_2$ defines the same Boolean function as $z = x_1 \oplus x_2 \oplus (x_1 \wedge x_2)$.