TalTech (Tallinna Technical University) Cyber Security Engineering bachelor program sample admission test

Solution time: 5 hours

Similar test has been used in 2018-2025

Exercise no 1

In an IT company, a UNIX server administrator was hired with a base salary and an additional contractual clause stating that the addition of an extra server under his administration would increase his salary. The salary adjustments were calculated with one-day accuracy. The employment contract specified that adding one extra server would increase the salary by 12%. Due to continuous inflation, it was also stated that when the additional administration work ended (it is usually a fixed-term assignment), the salary would be reduced by 11%, not by 12%.

Tasks:

- During one calendar year, there were seven temporary extra server administrations. That is, the salary was increased seven times and subsequently decreased seven times. By what percentage did the final salary change compared to the initial salary?
- If the annual inflation rate is 3%, what percentage should replace the 11% decrease in the contract (upon termination of the extra administration) in order to keep the real wage at the same level? Assume that there are still seven temporary extra assignments per year and that the 12% increase remains unchanged.

Exercise no 2

We analyzed a program that was allegedly used to crack certain cryptographic algorithms. During the investigation, we determined that the program's input size can vary over a wide range and that, for an N-bit input, the program's output is always N bits long. We also found that the program's running time depends

significantly on the input length N, especially when N exceeds 10–15 bits. Our tests further revealed that the running time depends only on the input length and not on the specific input data.

During testing, we measured the following running times (with an accuracy of one hundredth of a second):

- N=2 – 16.38 seconds
- N=5 – 16.38 seconds
- N=10 – 16.44 seconds
- N=15 – 18.39 seconds
- N=20 – 1 minute 4.22 seconds

We also planned to test the program for N=25 and N=30, but in both cases the program did not finish within half an hour, and we were forced to terminate it. Finally, for N=30, we decided not to terminate the program but instead to wait longer. The total running time was 18 hours, 16 minutes, and 14.62 seconds. We repeated the test for N=30, and it produced exactly the same result (more than 18 hours).

Tasks:

- Estimate the program's running times for the following input sizes: N=25, N=40, and N=50.
- Explain your reasoning and solution process.

Exercise no 3

The Estonian personal identification number consists of 11 decimal digits.

The first digit determines both the sex and the century of birth:

- 1 and 2 – male and female (respectively), born in the 19th century;
- 3 and 4 – male and female (respectively), born in the 20th century;
- 5 and 6 – male and female (respectively), born in the 21st century.

The second and third digits represent the last two digits of the year of birth. The fourth and fifth digits represent the month of birth. The sixth and seventh digits represent the day of birth. The eighth to tenth digits form a three-digit serial number assigned to the person. The eleventh digit is a checksum calculated from the previous ten digits using the appropriate algorithm. The age of the oldest Estonian citizen is 106 years.

Our aim is to calculate cryptographic hashes for all potential current inhabitants of Estonia. The hashes are computed using a specified algorithm and an implementation program. We have verified that computing a single hash takes exactly 1 millisecond. Each hash is 256 bits long. In addition, storing each personal identification number requires 11 bytes (88 bits).

Tasks:

- Estimate the amount of disk storage required to store the personal identification numbers together with their corresponding hashes for all potential current inhabitants of Estonia.
- Estimate how much time it would take to compute all hashes for all potential current inhabitants of Estonia.

Exercise no 4

Let us suppose that in the year 2034 a major breakthrough occurs in the field of quantum computing. It becomes possible to build a new type of quantum computer whose word length is equal to the number of direct neighbors of a single elementary particle, plus the number of neighbors of those neighbors.

The developers of this quantum computer specify that this statement is valid only under the following assumptions: the elementary particles behave like balls in a children's "ball pit." More precisely, the particles are assumed to have a spherical shape, all particles are of equal size, and they can move freely relative to one another, although they remain in close contact. Furthermore, only those particles that are in direct physical contact are considered neighbors.

Task:

What is the word length of such a quantum computer? In other words, how many direct neighbors does a single fixed elementary particle have in three-dimensional space, and how many neighbors of neighbors does it have?

Exercise no 5

The message validation server is capable of validating two types of messages: Type A and Type B. It is commonly believed that the validation time for a Type B message is somewhat longer than for a Type A message. Additionally, it is widely assumed that the actual validation time depends primarily on the message type (A

or B) and does not significantly depend on the message content. However, these claims have not been verified in practice.

We have reliable statistics for four different sessions:

- 1st session – 4,566 Type A messages and 7,059 Type B messages were validated; the session lasted 12 minutes and 15.80 seconds.
- 2nd session – 5,047 Type A messages and 2,734 Type B messages were validated; the session lasted 8 minutes and 47.60 seconds.
- 3rd session – 7,059 Type A messages and 9,846 Type B messages were validated; the session lasted 17 minutes and 52.20 seconds.
- 4th session – 5,074 Type A messages and 4,274 Type B messages were validated; the session lasted 10 minutes and 15.56 seconds.

Tasks:

- Determine the extent to which the validation time depends solely on the message type (Type A vs. Type B), rather than on the message content.
- Determine the average validation time for both Type A and Type B messages.