Haaga-Helia University of Applied Sciences, Bachelor of Business Administration, Business Information Technology, Helsinki Pasila, full-time studies

This document provides additional information about the entrance examination for Haaga-Helia's Business Information Technology BBA programme.

The entrance examination consists of the following sections:

Part based on material given in the examination

A true/false assignment based on the material given in the examination. See example questions below. Max 20 points.

Mathematical and logical skills

Questions measuring mathematical and logical reasoning. Max 50 points.

Motivation and written English language skills

Measuring study skills, motivation and written English language skills. Max 10 points.

Online-interview

Measuring study skills, motivation and oral English language skills. Max 20 points.

Duration: First three sections altogether: 3 hours
Online-interview: 10–15 minutes

The minimum and the maximum points:

An applicant must pass all of the sections separately to qualify any further in the admission process. The minimum and maximum points for each section are:

Examination section	**Minimum points**	**Maximum points**
Part based on material given in the examination	6	20
Mathematical and logical skills	15	50
Motivation and written English language skills	3	10
Online-interview	6	20
Total	**30**	**100**

Example questions from past exams:

Part based on material given in the examination

Task 1 The Phenomena of the Digital Era

Please see the source article on attachment 1.

Based only on the article, indicate whether the following statements are true or false or not mentioned in the article at all.

Assessment: Correct answer +2 points
Wrong answer -0.5 points
No answer 0 points

		TRUE	FALSE	NOT IN THE ARTICLE
1.	According to the text, phishing is the biggest internal cyber security risk.			
2	Max Schrems is famous for his legal challenge to the US government mass surveillance practices.			
3.	Cryptocurrency mining programs are one form of malware.			
4.	Nowadays, it is more difficult to be a cybercriminal due to better computer security awareness.			
5.	Ransomware is a subset of malware in which the data on a victim's computer is locked.			
6.	Cloud computing businesses are likely targets of ransomware attacks.			
7.	Cryptocurrencies are based on cloud computing and various set of blockchain technologies.			
8.	Electrical grids, transportation systems and other types of national critical infrastructures are under increasing cybersecurity threat.			
9.	Blockchain is a centralised register of every transaction that has been carried out in cryptocurrency.			
10.	Cryptocurrencies are not controlled by any central authority, like politicians, states or central banks.			
	TOTAL			

Mathematical and logical skills

Task 1 (5 p)

The price of a shirt was reduced by 40%. Currently the price is 90 €. How many € was the discount?

Task 2 (5 p)

Think of integer numbers from 0 to 999. In how many of the numbers there are at least one digit seven (7)?

Task 3 (5 p)

Picture a set where Paul looks at Sally but Sally looks at Steve. We know that Paul is married but Steve is unmarried.

How would you comment a statement "In this scene there is one married person looking at unmarried person"?

a) True
b) False
c) Can't be determined

Task 4 (5 p)

A sequence of numbers (A_1, A_2, A_3, …) is defined as follows:

$A_1 = 0$
$A_2 = 1$
$A_n = 3 \times A_{n-2} + A_{n-1} + 2$; when $n > 2$

Define the value of A_5

Task 5 (5 p)

First day of June a farmer bought a big number of chickens and let them stay on a big open field. During the following nights a small group of foxes killed and ate 10% of the chicken every night. The farmer noticed the destruction only after the number of chicken had decreased below the half of the initial number. On which day of June did this happen?

Task 6 (5 p)

In a student group there are 36 students. One third (1/3) of them have studied programming language C# and 75% have studied programming language Java. Five of the students have studied no programming languages. What is the number of students who have studied both C# and Java?

Task 7 (5 p)

A small software company employs five persons. The salary of the manager (**M**) was higher than the salary of the programmer (**P**) but not as good as the salary of the software architect (**A**). The software tester (**T**) was better paid than the sales engineer (**E**) but a bit worse than the programmer. List the employees in order from highest to lowest with respect to their salaries.

You can use abbreviations (A, E, M, P, T) in your answer.

Task 8 (5 p)

How much money would I start with if, in spending 1/5 and then 1/5 of the remaining amount, I had altogether spent 72.00 €?

Task 9 (5 p)

A string function s is defined as follows:

A is string of characters, n and m are positive integer numbers

s(A;n;m) returns m-character sub-string starting from n^{th} character of original string A.

Example: s(CITYOFHELSINKI ; 4 ; 6) = YOFHEL

Strings can be connected together with function +

Example:

TRAM + BUS = TRAMBUS

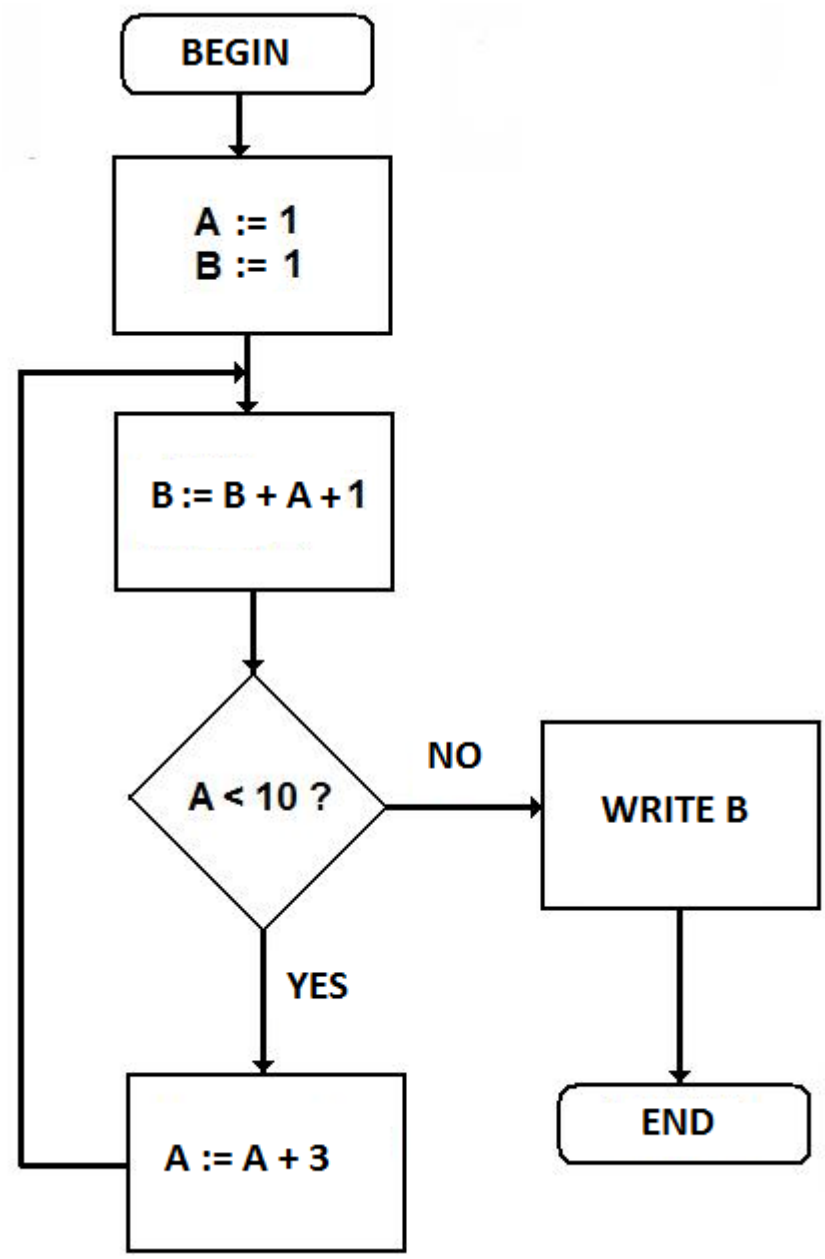
Which string would you get from

s(s(MOBILE ; 2 ; 3) + s(PROGRAMMING ; 5 ; 4) + s(WIZARD ; 3 ; 3) ; 6 ; 3) ?

Task 10 (5 p)

Notation A := B means that variable gets value B. For example A := 7 means that value of variable A will be 7. As well as A := A + 1 means that 1 is added to variable A:s old value.

Follow the logic of following flow chart:



Which value will be printed in the end?

Motivation and written English language skills

Tasks 1–3 or tasks 1–4

This part consists of few short questions or short essays that will be used to assess your readiness and motivation to study at Haaga-Helia's Business Information Technology programme, as well as your written English skills.

Online-interview

The interview is an online-interview with one applicant and one interviewer, who provides discussion topics and questions for the applicant. The interview lasts typically 10–15 minutes. The aim of the interview is to measure motivation and career orientation towards the programme studies, realistic expectations to complete the bachelor's studies and oral English language skills required in the programme.

Attachment 1

Article: The Phenomena of the Digital Era

- You have 30 minutes to read the article, and then the teacher collects the article from you.
- You can make notes and keep them while answering the article questions (Part based on material given in the examination, Task 1).

The Phenomena of the Digital Era

In the midst of businesses becoming General Data Protection Regulation (GDPR) compliant, cybersecurity measures have moved from purely technical to political ones, according to a Tuesday report from AlienVault. The company surveyed 900 security professionals at the Infosecurity Europe 2018 conference to gain insight into the current state of cybersecurity threats. Some 56% of respondents said they believe that cybersecurity is becoming a political pawn. This shift indicates that cybersecurity isn't only infiltrating personal lives, but society, as well.

Phishing is the reigning winner of internal threats, with nearly 55% of participants agreeing it is the biggest risk, said the survey. AlienVault explained that it's the human element of phishing that makes it appealing to cybercriminals. Unfortunately, no single precaution can be used to prevent a phishing attack, continued the report. Most breaches are actually caused by human error, said the survey, highlighting the vitality of user awareness and education. However, AlienVault warned that user education alone isn't enough—businesses need a multilayered defense of technology, processes, and people.

Weighing in at 45%, ransomware was the second-highest internal worry for professionals. Since ransomware is a highly public threat, business pros feel even more pressure, having to respond to the security breach in the public spotlight, said the survey. Participants said they were growing concerned about possible attacks in the cloud, with 52% worried that cloud-based threats will become an increasing reality in the future. While the cloud is extremely useful to businesses, it can quickly turn into a threat if not secured properly, said the survey. Cloud functionality is still so new, however, that most threats have yet to be realized, continued the survey.

Industry observers are still waiting for a breach with GDPR, but until then, it brings a host of different concerns for business, said the survey. Companies have been forced to completely rearrange and reorganize the management of customer records, said the survey. And failure to be compliant with GDPR standards can be a huge hit to businesses financially and socially, causing consumers to shy away from businesses that don't protect their data.

Cryptocurrency mining is a relatively new trend, in which cybercriminals infect machines in order to commandeer their CPU power and steal Bitcoin, said the survey. Businesses still have some work to do to stay protected, with 29% of respondents not confident in their cryptomining protection and 24% unable to detect cryptomining activity.[1]

More than 90% of cyberattacks and resulting data breaches start with a spear phishing campaign—and many employees remain unable to discern these malicious emails from benign ones. To improve cybersecurity education, some companies are turning to a nontraditional method: Phishing their own employees. Too often, companies offer only annual training on cybersecurity that doesn’t keep up

[1]Macy Bayern, Techrepublic, 2018.

with the evolving threat landscape, according to Wesley Simpson, COO of (ISC)[2]. "Using internal phishing exercises is a very inexpensive tool that helps fight the risk and is an investment in staff's knowledge and education," Simpson said. "It's not something that should happen once a year—it should be continuous." Before making the campaign public, companies should take a baseline measurement of how employees react to one of the phishing exercises, said Carl Leonard, principal security analyst at Forcepoint. Then, you have a metric to measure improvement against.[2]

Every year, the security industry tries to predict what the biggest threats will be in hopes of pulling together a stronger defense. It's impossible to get this 100% right, but if we use what we learned in 2017, we can leverage that knowledge to safeguard businesses and consumers in the new year. In 2017, we saw the severity — and the frequency — of cyberattacks reach a level that no one could've predicted. WannaCry, NotPetya and Locky, dominated the news cycle as hackers were able to target businesses internationally and cost them billions of dollars. Every year we think the biggest attacks will go unmatched, but we know that a secure future is the only way to prevent cybercrimes from having a bigger and bolder impact. In the coming year, there are five key security issues that will occur and for which we must be prepared.

The cybercriminal "underground" network will grow and evolve. You thought 2017 was bad for cyberattacks? This year 2018 won't be any better. Over the past few years, it has become easier to be a cybercriminal. You don't even have to have a lot of technical knowledge -- just the ability to find the right tools. The more we publicize the success of cybercrimes, the more likely criminals are to take notice. For example, the ransomware profits saturated news headlines, touting it as a $1 billion industry last year — meaning, for too many is becoming too profitable to ignore. The educated cybercriminals will make their attacks more destructive and harder to prevent in order to establish dominance in the saturated criminal market.

Cybercriminals will continue looking to cash in on the cryptojacking "gold rush" that has become more mainstream. Cryptocurrencies are exploding in popularity and driving the escalation of cryptojacking activity or the secret use of your computer to mine cryptocurrency. Most people don't understand that with this type of threat, there is a chance everyday users could "mine" their own wallet. This blurs the line between true cybercrime and makes it harder to monitor for. Due to mining by visitors to a web property in disclosed cryptojacking activity, an individual could use this technique to replace advertising on their websites to create a new means of revenue. However, the most likely scenario for cryptojacking is that legitimate websites will be compromised due to criminals mining for cryptocurrencies. This leads to a belief that it will be one of the top cybercrime tactics to look out for in 2018.

From a technique perspective, more malware families will launch malware using worms in 2018. With the widespread effectiveness of WannaCry and Trickbot, criminals see this method work much faster to compromise networks than most others. If these criminals could adjust their methods to make less noise — the biggest downfall of this approach — then this method could begin to amass even more victims in a quicker timeframe the following year. We also will see industry verticals such as education

[2]Techrepublic, 2018

and healthcare take a broader hit from hackers. Cybercriminals will continue to target the vulnerable, and educational institutions often lack the resources to defend their endpoints. Most school systems have only a slightly secured network of endpoints that contains personally identifiable information on students, parents and staff.

Cybercriminals who target data often focus on those who are data rich, making education institutions a big target in 2018 due to their lack of proper security measures. The increased use of IoT in the healthcare industry will also create data security concerns in 2018. Greater technological advancements mean better patient care, but the more we rely on it, the more we fear the loss of personal health data. In the era of connected devices, healthcare industry needs to make patient security a top priority by increasing security protocols. [3]

Ransomware is a subset of malware in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access returned to the victim. The motive for ransomware attacks is nearly always monetary, and unlike other types of attacks, the victim is usually notified that an exploit has occurred and is given instructions for how to recover from the attack. Payment is often demanded in a virtual currency, such as bitcoin, so that the cybercriminal's identity isn't known. Ransomware malware can be spread through malicious email attachments, infected software apps, infected external storage devices and compromised websites. A growing number of attacks have used remote desktop protocol and other approaches that don't rely on any form of user interaction.

In a lockscreen variant of a ransomware attack, the malware may change the victim's login credentials for a computing device; in a data kidnapping attack, the malware may encrypt files on the infected device, as well as other connected network devices. While early instances of these attacks sometimes merely "locked" access to the web browser or to the Windows desktop -- and did so in ways that often could be fairly easily reverse-engineered and reopened -- hackers have since created versions of ransomware that use strong, public-key encryption to deny access to files on the computer.

Perhaps the first example of a widely spread attack that used public-key encryption was Cryptolocker, a Trojan horse that was active on the Internet from September 2013 through May of the following year. The malware demanded payment in either bitcoin or a prepaid voucher, and experts generally believed that the RSA cryptography used -- when properly implemented -- was essentially impenetrable. In May 2014, however, a security firm gained access to a command-and-control server used by the attack and recovered the encryption keys used in the attacks. An online tool that allowed free key recovery was used to effectively defang the attack. In May 2017, an attack called WannaCry was able to infect and encrypt more than a quarter million systems globally. The malware uses asymmetric encryption so that the victim cannot reasonably be expected to recover the (private and undistributed) key needed to decrypt the ransomed files.

Ransomware kits on the deep web have allowed cybercriminals to purchase and use a software tool to create ransomware with specific capabilities and then generate this malware for their own

[3]Marcin Kleczynski, Forbes, 2018

distribution and with ransoms paid to their bitcoin accounts. As with much of the rest of the IT world, it's now possible for those with little or no technical background to order up inexpensive ransomware as a service (RaaS) and launch attacks with very little effort. In one RaaS scenario, the provider collects the ransom payments and takes a percentage before distributing the proceeds to the service user. Attackers may use one of several different approaches to extort digital currency from their victims.[4]

Ransomware targeting cloud services is one of the six biggest cyber threats likely to face organisations in 2018, according to the Massachusetts Institute of Technology (MIT). Cloud computing businesses are likely targets of ransomware attacks because they typically store huge amounts of data for companies. While the biggest and oldest cloud service providers such as Google, Amazon, and IBM have the resources and experience to make it difficult for attackers to succeed, the MIT Review points out that the smaller cloud providers are likely to be more vulnerable and more likely to pay up if customer data were encrypted and held for ransom. MIT warns that cyber attackers hijacking computers for cryptocurrency mining could have a devastating effect if they target computing resources at hospitals, airports and other similar locations. Such attacks are becoming more common and MIT predicts that more cyber attacks targeting electrical grids, transportation systems and other types of national critical infrastructure are likely in 2018. Cyber-physical attacks are expected to be designed to either cause immediate disruption or to threaten to shut down vital systems to extort money from operators. MIT also predicts that 2018 will see researchers and attackers uncovering cyber vulnerabilities in older planes, trains, ships and other modes of transport. Despite the efforts to address vulnerabilities ahead of the midterm elections in November 2018, MIT warns that determined attackers still have plenty of potential targets, including electronic voter rolls, voting machines and the software used to collate and audit results.[5]

Before getting to grips with the process of cryptocurrency mining, we need to explain what blockchain is and how that works. Blockchain is a technology that supports almost every cryptocurrency. It is a public ledger (decentralised register) of every transaction that has been carried out in that cryptocurrency. These transactions are assembled into what are called "blocks". These are then verified to ensure they are legitimate by cryptocurrency miners. This checks if the same coin hasn't been expended again before the transaction has cleared, and that the input and output expenses tally. Then the next sequential transaction block is connected to it. This is how cryptocurrencies are created and how new cryptocoins are made. As there is no central authority or central bank, there has to be a way of gathering every transaction carried out with a cryptocurrency in order to create a new block. Network nodes that carry out this task are called dubbed 'miners'. Every time a slew of transactions is amassed into a block, this is appended to the blockchain. Whoever appends the block gets rewarded with some of that cryptocurrency. To prevent the devaluation of the currency by miners building lots of blocks, the task is made harder to conduct. This is achieved by making miners solve complicated mathematical problems called proof of work.[6]

[4]Margaret Rouse, Techtarget 2018.
[5] Warwick Ashford, Computer Weekly 2018
[6] Adam Shepherd, ITPro 2018

Sources:

1. https://www.techrepublic.com/article/cybersecurity-rundown-the-5-most-critical-threats-to-businesses-in-2018/

2. https://www.techrepublic.com/resource-library/whitepapers/phishing-attacks-a-guide-for-it-pros-free-pdf/

3. https://www.forbes.com/sites/forbestechcouncil/2018/01/02/a-look-at-the-five-biggest-future-cyberthreats-of-2018/

4. https://searchsecurity.techtarget.com/definition/ransomware

5. https://www.computerweekly.com/news/450432488/Ransomware-to-hit-cloud-computing-in-2018-predicts-MIT

6. https://www.itpro.co.uk/digital-currency/30249/what-is-cryptocurrency-mining