

✓ Instructions

Uppsala University

Department of Information Technology

Cryptology (1DT075)

2021-08-25

Instructions: Read through the complete exam and note below any unclear directives before you start solving the questions.

The exam is **open book**: you are allowed to use course material, text books, your own notes, and any material that was created before the start of the exam. Remember to give credit (i.e. to provide references) when you use a third-party source. You are also allowed to use technical aids, e.g. a calculator.

The exam is **individual**: you are NOT allowed to get help from other people to answer the questions. Do NOT share or discuss the questions with other people (online or otherwise). Do NOT share or discuss solution approaches with other people. Do NOT submit other people's answers as your own.

Grading scale. 0-49 pts. (U), 50-69 pts. (3), 70-84 pts. (4), 85-100 pts. (5)

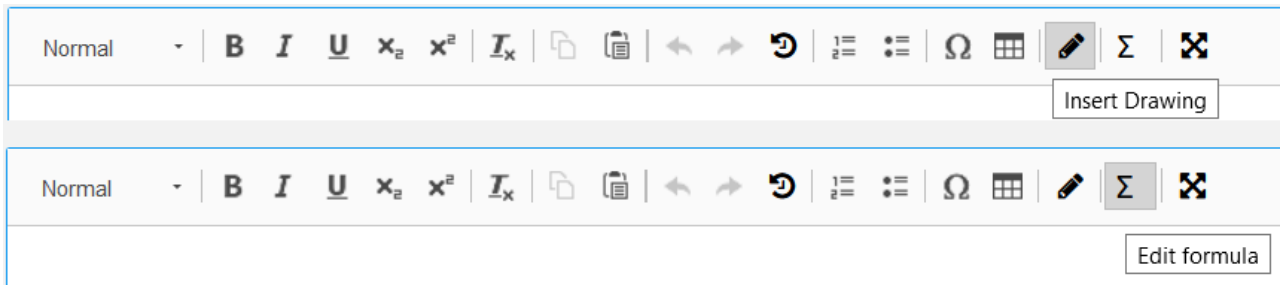
You can email me at tjark.weber@it.uu.se for any emergency questions during the examination. Important announcements or clarifications will be communicated via Inspira.

If you find any unclear directives, please note the question number below and explain what you think is unclear.

Fill in your answer here

1 Optional Supplementary PDF

The answers to the questions should, generally speaking, be filled out in the provided text input areas for each question. Please note the tools available in the toolbar, in particular:



However, if you find the available tools restrictive when answering some part of a question, you may upload a supplementary PDF here with figures, equations, etc. and refer to the relevant parts of the supplementary PDF in your answers here on Inspira.

This upload is optional. If you do not have any problems answering the questions using the tools provided here, there is no need to upload a supplementary PDF.



Upload your pdf here (optional). Maximum one file.

The following file types are allowed: **.pdf** Maximum file size is **1 GB**

 Select file to upload

Maximum marks: 0

3 Man-in-the-middle

Assume there is a man-in-the-middle, Mallory, in between a customer's (Alice's) computer and a bank. Mallory is listening to messages between the bank and its customers and has figured out some properties of the messages:

- She can identify messages from a customer to the bank that indicate that some amount of money, x , should be transferred from the customer's account y_1 to account y_2 . These have the form

$$z \parallel enc_{\tau}(y_1) \parallel enc_{\tau}(y_2) \parallel h(z \parallel enc_{RSA}(x) \parallel enc_{\tau}(y_1) \parallel enc_{\tau}(y_2)) \parallel enc_{RSA}(x)$$

where \parallel indicates concatenation, $enc?$ is some unknown encryption function that always returns the same value for a given input, h is a known, fixed hash function, and enc_{RSA} is RSA encryption using the bank's public RSA key, z is a random-looking string, which differs from message to message, but whose value does not depend on any of the other bits of the message.

- Mallory does not know how to generate such messages herself (in particular, she does not know how to generate z).
- The lengths for each part z , enc , and h are fixed and do not vary between messages.
- A transfer of money from Alice to Bob is performed by Alice sending such a message to the bank, where y_1 is Alice's account, y_2 is Bob's account and x is the amount of money that should be transferred.
- The bank checks whether messages have been changed using the hashed value.

a) Mallory captures such a transfer message sent from Alice to the bank, intending to transfer money from her account to Bob's. How can Mallory modify the captured message so that it instead requests to transfer an amount of money chosen by Mallory to Mallory's account from Alice's? You may make reasonable assumptions as long as they are clearly stated.

(5 pts)

b) Having been made aware of its completely flawed system, the bank has tasked you with coming up with a better approach for providing internet banking services (i.e. money transfers) to its customers. What knowledge from the course could you apply to this task, and how? Discuss the cryptographic aspects of your system design (e.g. confidentiality, message integrity, authentication, potential attacks, and so on). What choices would you make, and why? What are the main issues that need to be addressed and how have you tackled them? Provide a detailed technical discussion; explain and motivate your choices.

(The scope and depth of your discussion should be commensurate with the relatively large number of points that this question is worth.)

(35 pts)

Fill in your answer here

Words: 0

Maximum marks: 40

4 Hash Functions

a) Show that any hash function must have collisions.

(2 pts)

b) Since any hash function must have collisions, how can we hope to provide collision resistance?

(1 pt)

c) Given a collision resistant function f that takes 1024-bit values and yields a digest of size 256 bits, can we use f to construct a collision resistant hash function (taking values of any length) that returns digests of size 256 bits? If yes, how? If no, why not?

(2 pts)

Fill in your answer here

Maximum marks: 5

5 Blind Signature Scheme

Explain, in detail, the concept of a blind signature scheme and suggest a way of using homomorphic encryption to implement such a scheme.

(10 pts)

Fill in your answer here

Format

B

I

U

x_2

x^2

I_x

Ω

Σ

Words: 0

Maximum marks: 10

6 Cryptosystem

Let (P, C, K, E, D) be a cryptosystem. Is it true that, given any $k \in K$, decryption for any pair of ciphertexts $c_1, c_2 \in C$ has the property $d_k(c_1) = d_k(c_2) \implies c_1 = c_2$? If yes, prove it, if no, give a counterexample.

(5 pts)

Fill in your answer here

Format
|
B
|
I
|
U
|
 \times_2
|
 \times^2
|
 \mathcal{I}_x
|

|

|

|

|
 $\frac{1}{x}$
|
 $\frac{1}{x^2}$
|
 Ω
|

|

|
 Σ
|

✕

Words: 0

Maximum marks: 5

7 Hill Cipher Encryption

a) Using a Hill cipher with the key

$$k = \begin{bmatrix} 5 & 2 & 0 \\ 3 & 3 & 4 \\ 6 & 2 & 1 \end{bmatrix}$$

encrypt the last three characters of your exam registration code (where the characters are encoded in the usual way, i.e. A = 0, B = 1, ..., Z = 25, as elements of \mathbb{Z}_{26}). Briefly show and explain the calculation.

(5 pts)

b) What is required of the key, k , in order to be able to decrypt? Why?

(5 pts)

Fill in your answer here

Maximum marks: 10

- Fill in your answer here**

Maximum marks: 5

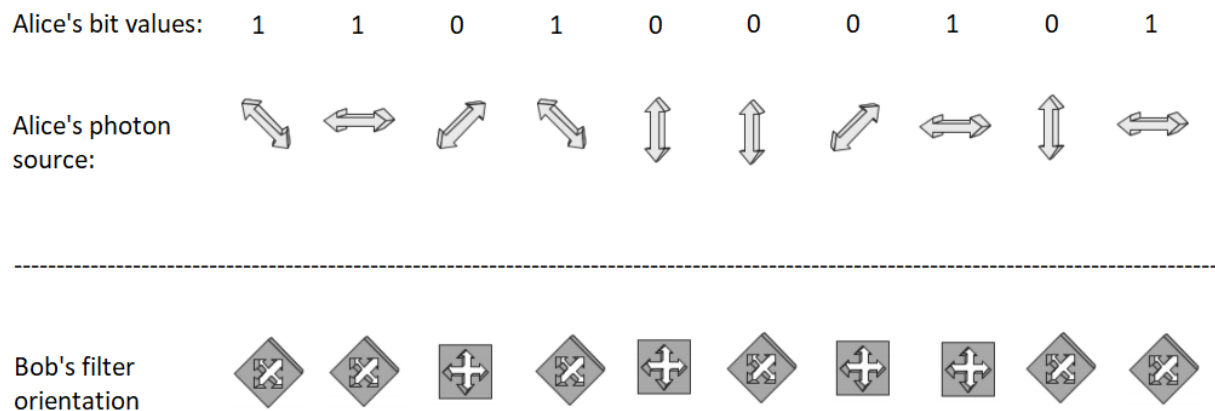
a) What is the entropy of the random variable X that models this coin flip? Include the calculation.
(1 pt)

- Flip the coin twice, recording the result of each flip as 1 for heads, 0 for tails.
- If the two flips yield different values (i.e. heads followed by tails or v.v.) output the first recorded value to our output sequence, otherwise do nothing.
- Repeat the above two steps until we have generated as many bits as we want.

c) What is the entropy of the random variable that models the generation of such a bit? Explain how you reached the answer.
(1 pt)

11 Quantum Key Distribution

Alice and Bob are using the BB84 quantum key distribution scheme. The following session occurs:



a) In the above session, what is the sifted key?

(1 pt)

b) What is an advantage that the quantum key distribution scheme has over non-quantum approaches?








(2 pts)


c) The next day Alice is trying to send a new key to Bob, however, this time Eve is eavesdropping. Explain how this can be detected by Alice and Bob.

(2 pts)

Fill in your answer here

Format

▼
B
I
U
 x_2
 x^2
 I_x





 $\frac{1}{2}$
 $\frac{1}{2}$
 Ω



Σ


Words: 0

Maximum marks: 5