

☑ Instructions

Uppsala University

Department of Information Technology

Cryptology (1DT075)

2021-06-15

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.

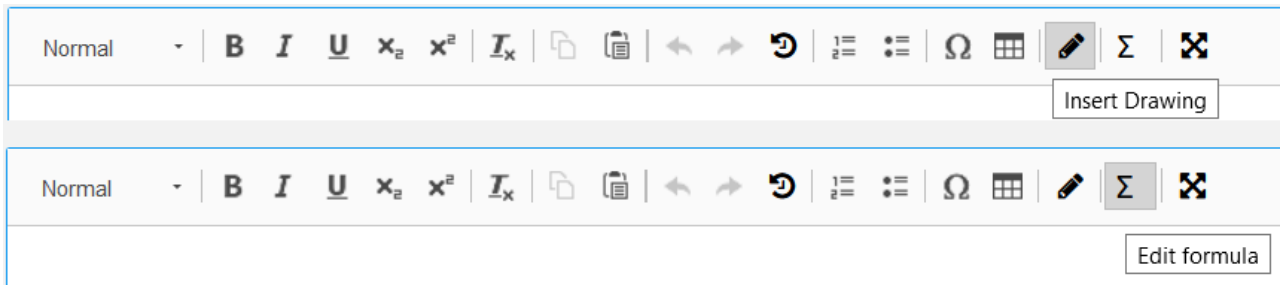
Grading scale. 0-49 pts. (U), 50-69 pts. (3), 70-84 pts. (4), 85-100 pts. (5)

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.

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

2 Unpadded RSA

A value has been encrypted using unpadded RSA. You do not know the private key (but you do have access to the public key).

a) How would you go about finding the encryption of double the encrypted value?

(2 pts)

b) Discuss why, generally speaking, using unpadded ("textbook") RSA for encryption is not a good idea.

(3 pts)

Fill in your answer here

Format

B


I


U


x_2


x^2


I_x




















Ω





Σ



Words: 0

Maximum marks: 5

- 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

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

- 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.

(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

Format
|
B
|
I
|
U
|
 \times_2
|
 \times^2
|
 $\frac{\square}{\square}$
|
 $\frac{\square}{\square}$
|
 $\frac{\square}{\square}$
|
↶
|
↷
|
↺
|
↻
|
≡
|
≡
|
Ω
|

|
✎
|
Σ
|

✕

Words: 0

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


$\frac{1}{x}$




















Ω





Σ

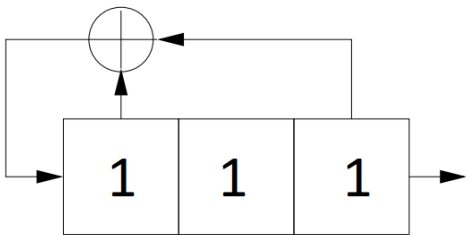


Words: 0

Maximum marks: 10

9 LFSR

Consider the following linear feedback shift register (where \oplus denotes addition modulo 2):



a) Compute the output sequence generated by this LFSR.

(3 pts)

b) Assume we use the output of this LFSR as bits of keys used for encryption using the Vernam cipher. Does it provide perfect secrecy? If yes, why? If no, why not?

(2 pts)

Fill in your answer here

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

Words: 0

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:

Alice's bit values: 1 1 0 1 0 0 0 1 0 1

Alice's photon source:          

Bob's filter orientation:          

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             

Σ 

Words: 0

Maximum marks: 5