RFMA310-1 20H Diskret matematikk
Hjemmeeksamen

Stian Onarheim

October 25, 2020

Contents

1 The Elgamal Encryption Algorithm

Helloo

2 The source code

I have implemented Elgamal in python as it supports enormous numbers within its default libraries. Before encrypting the plaintext, I convert its characters to ASCII values and concatenates them together.

The message to be encrypted has to be an element of the cyclic group G, creating a limit to the message's length. To support longer messages, the message is divided into blocks smaller than G's order. As the ASCII values varies from one - three digits, zeros are appended at the beginning to make every value the same length. This is needed to make decryption easier. **??**.