1 Diffie-Hellman and El Gamal

Dario Köllner ...

Introduction

Here comes the intro....

1.1 Diffie-Helmann Security

1.1.1 Computational-Diffie-Hellman-Problem

1.1.2 Decisional-Diffie-Hellman-Problem

1.1.3 Primenumber p and Bitlength q

1.1.4 Man in the middle attack

1.2 El Gamal problems

1.2.1 Protocol problems

1.2.2 Subgroup problems