Semanais

Gabriel Zocal Santos

Escola Politecnica
(Poli-USP)

10/25

Estrutura da apresentação

1 Texto

Conceitos novos

Familiarização com novos conceitos

- Perfect security
- Limitações one time pad
- Semantic secure
- Feistel NT,DES, 3DES
- PRF, Block cipher

FHE

Novos topicos de Matemática

- Group Theory
- Polynomial Ring

Fim da apresentação!