Evento	Salão UFRGS 2019: SIC - XXXI SALÃO DE INICIAÇÃO CIENTÍFICA DA UFRGS
Ano	2019
Local	Campus do Vale - UFRGS
Título	Sistema de Criptografia de ElGamal
Autor	CIBELE DA ROCHA SCHMITZ
Orientador	JULIANE GOLUBINSKI CAPAVERDE

TÍTULO DO TRABALHO: Sistema de Criptografia de ElGamal
AUTORA: Cibele da Rocha Schmitz
ORIENTADORA: Juliane Golubinski Capaverde
INSTITUIÇÃO DE ORIGEM: Universidade Federal do Rio Grande do Sul

A criptografia é utilizada há mais de mil anos para proteção de dados, através da codificação e decodificação de mensagens, possibilitando a troca de informações sem que uma pessoa intermediária tenha acesso às mesmas. Esta apresentação abordará um tipo específico de criptografia, chamada de criptografia de chave pública ou assimétrica.

A criptografia assimétrica baseia-se na utilização de duas chaves: uma pública, utilizada para cifrar a mensagem, e uma privada para decifrá-la. Um exemplo de sistema de criptografia assimétrica é a criptografia de ElGamal.

Em 1985 Taher ElGamal introduziu um método de encriptação de mensagens baseado no problema do logaritmo discreto. Este trabalho visa apresentar o problema do logaritmo discreto e mostrar o funcionamento da criptografia de ElGamal em $\mathbb{Z}_p$.