ICMC USP
SÃO CARLOS

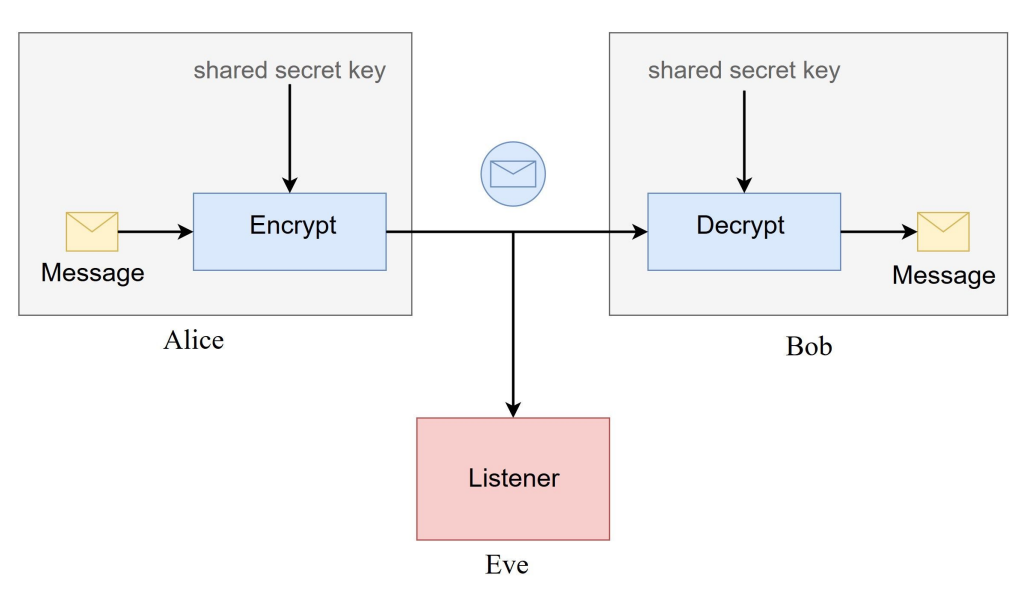
GANESH

Introdução à Criptografia

O que é criptografia?

- É o estudo e prática de princípios e técnicas para comunicação segura na presença de terceiros, chamados “adversários”
- Proteção de Informação
- Comunicação Segura

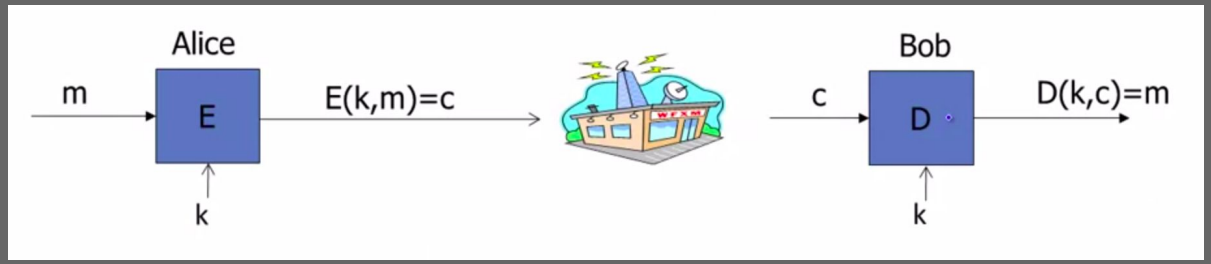
Cenário


shared secret key
shared secret key
Encrypt
Decrypt
Message
Message
Alice
Bob
Listener
Eve

Objetivos da criptografia

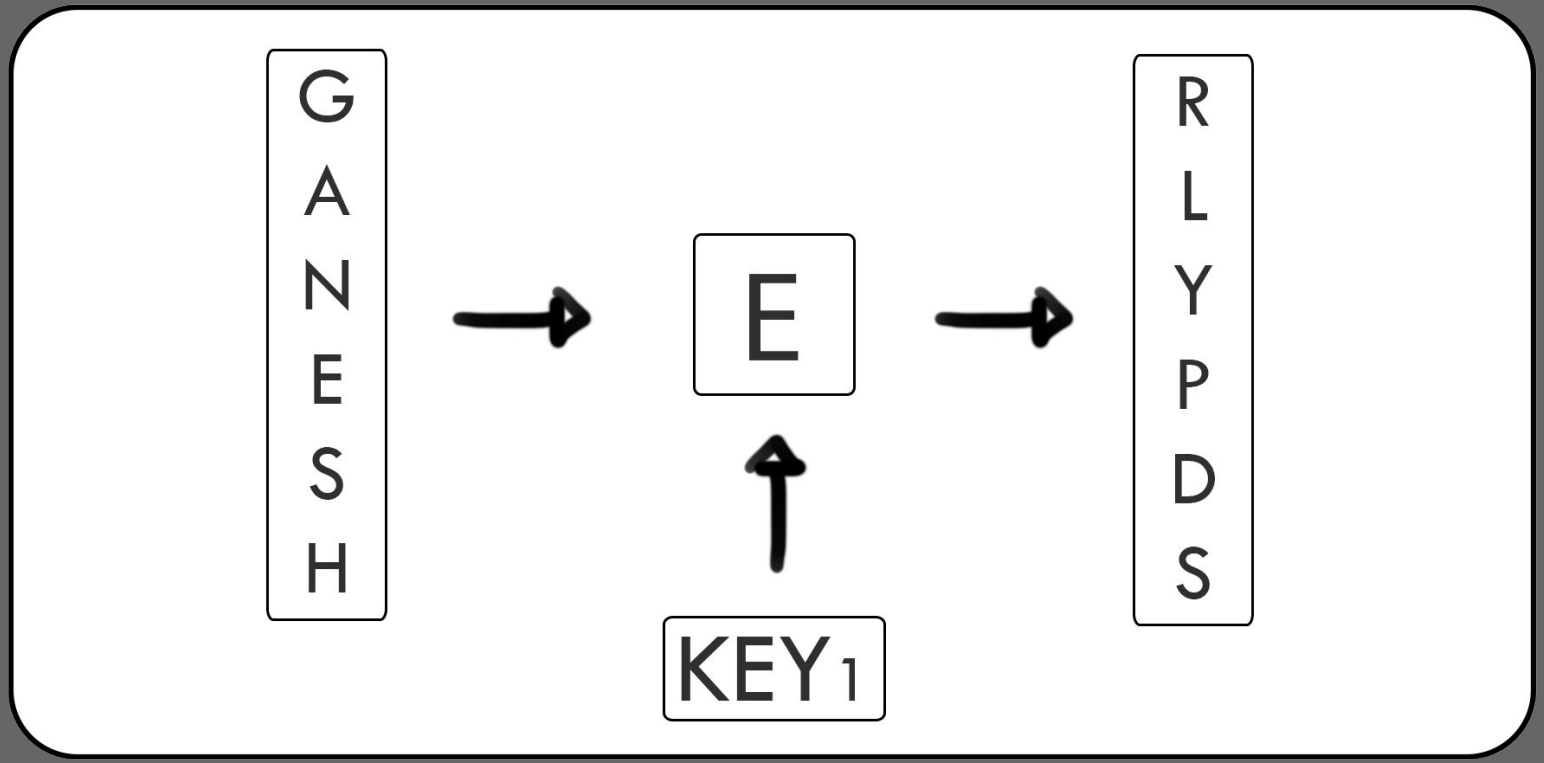
- Confidencialidade
- Autenticação
- Integridade
- Não repúdio
- Anonimidade

Criptografia

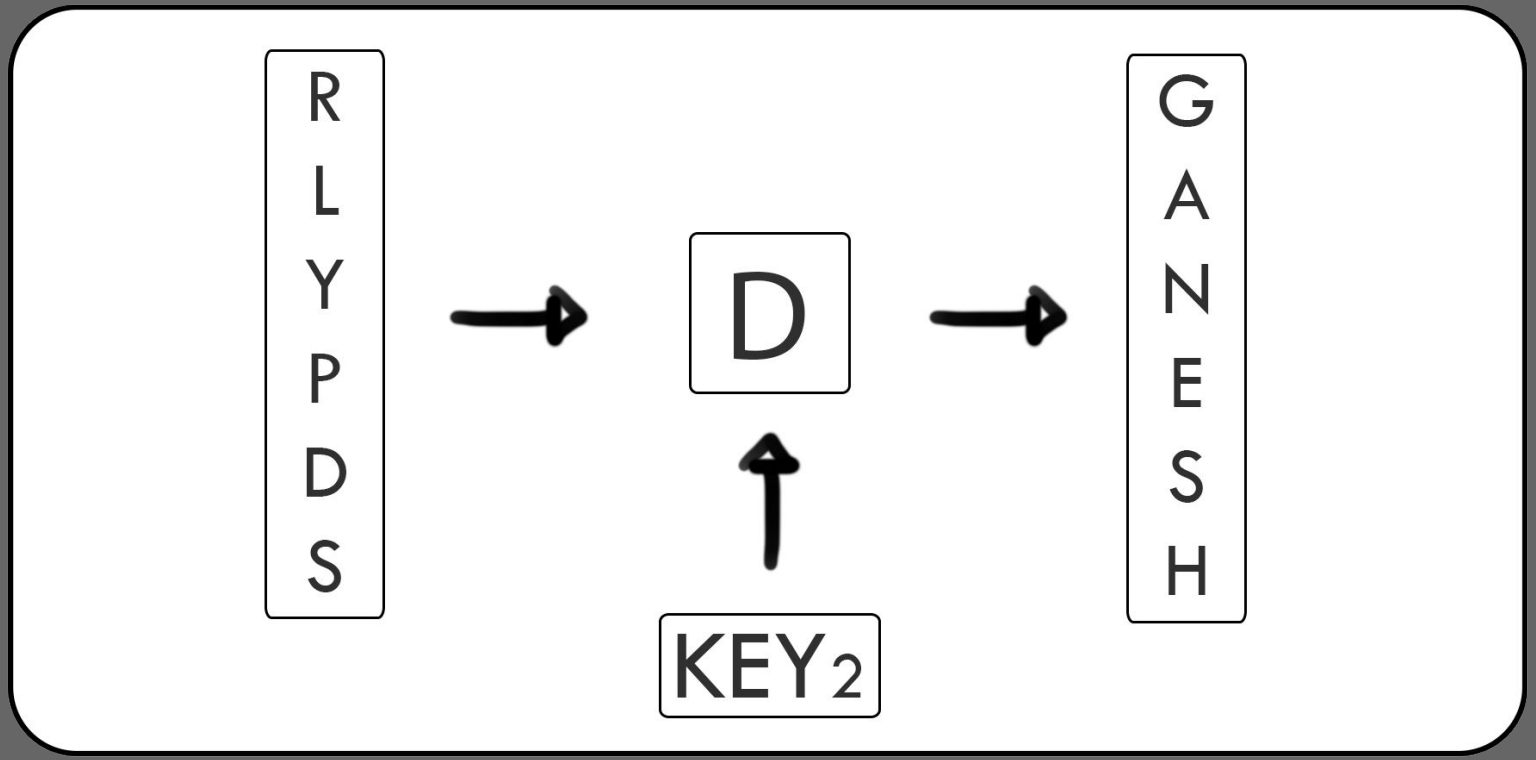


- Plaintext (planotexto) = m
- Ciphertext (cifrotexto) = c
- Chave = k
- Funções
- Simétrica vs. Assimétrica

Encripta

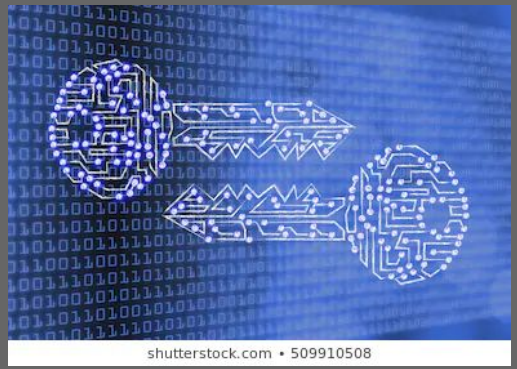


Decripta



Criptografia é:

- Uma excelente ferramenta
- A base de vários mecanismos de segurança



Criptografia não é:

- A solução para todos os problemas
  - SW Bugs, Eng Rev, Protocolos, Eng Social
- Confiável, a não ser que seja implementada e utilizada corretamente (WEP)
- Algo que você deva tentar inventar por você mesmo.

Roteiro

- Criptografia clássica
  - Cifras de Substituição
  - Cifras de Transposição
  - CIfras de Rotores
- Criptografia Moderna
  - One-Time Pad
  - Stream Cipher
- Ataques

Roteiro

- Kahoot!
- Challs
  - http://ctf.ganeshicmc.com/
- Dúvidas
  - Google Meets
  - Comentários no Youtube
  - Telegram

GANESH

Grupo de Segurança da Informação
ICMC / USP - São Carlos, SP
http://ganesh.icmc.usp.br/
ganesh@icmc.usp.br