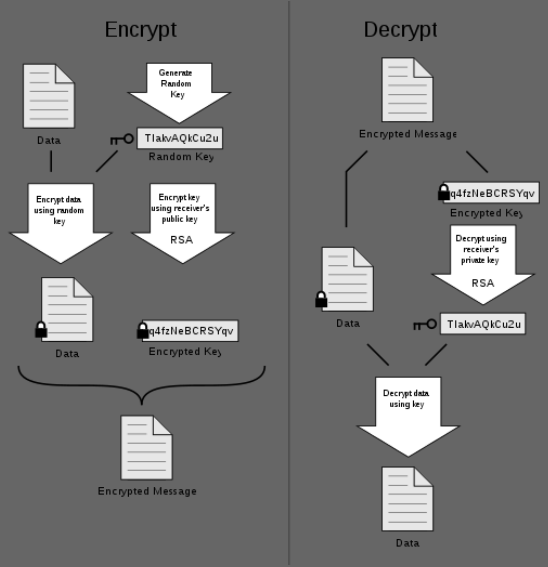
ICMC USP
SÃO CARLOS

GANESH

Aplicações de Criptografia

Comunicação Segura

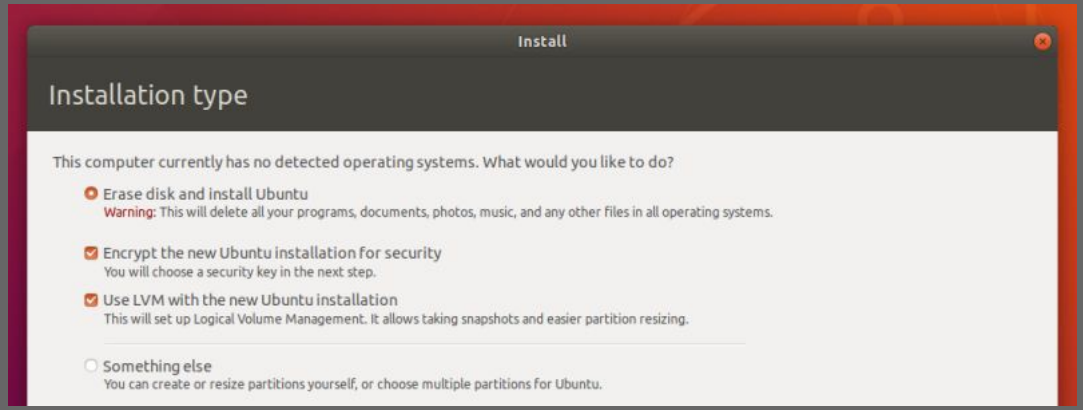
- Criptografia de chave privada
- Criptografia de chave pública (assimétrica)
  - OpenPGP, S/MIME
- Encriptação fim-a-fim
  - Whatsapp



Armazenamento

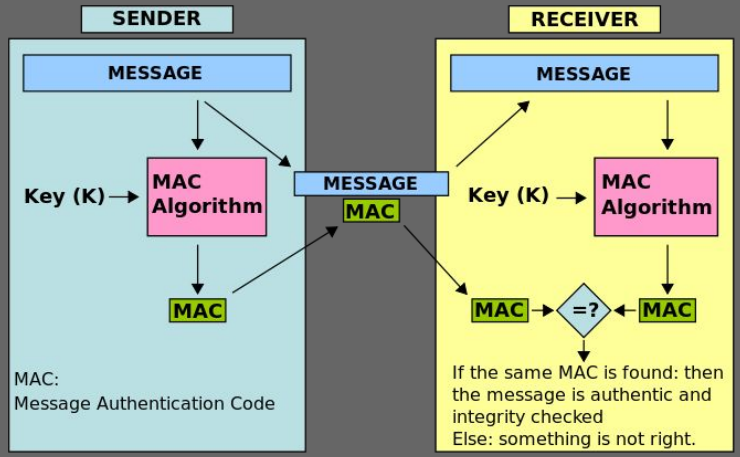
- SHA-n
- MD5
- Cifras de Bloco

- Verificação de senha
- Encriptação de disco



Autenticação

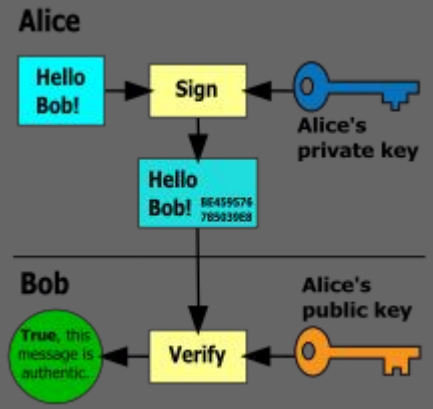
- Autenticação de mensagem
  - MAC, HMAC



- SSL/TLS
- SSH

Assinaturas Digitais

- Autenticação
  - JupiterWeb
- Não repúdio



Criptomoedas

- Transações financeiras
- Unidades adicionais
- Verificação

- Bitcoin
- Blockchain

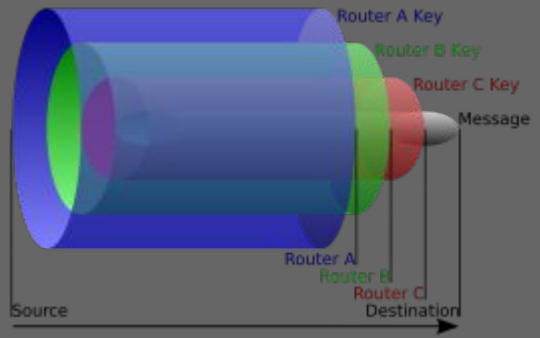
Threshold Cryptosystems

- Encriptação com Chave Pública

- Chave Privada é dividida entre um grupo
  - Precisa-se de mais de uma chave privada para decriptar a mensagem

Redes anônimas

- Tor (The onion router)
- Onion routing



Secure multi-party computation

- Função computada em conjunto
- Inputs privados

ICMC USP SÃO CARLOS

Ganesh

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