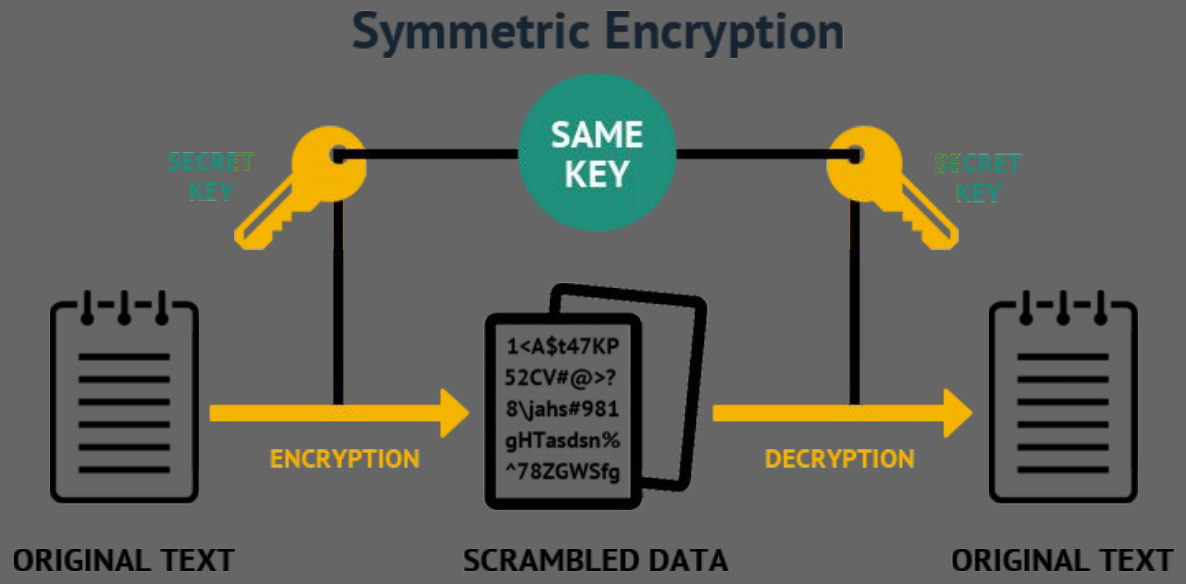
ICMC USP
SÃO CARLOS

GANESH

Criptografia Simétrica vs Assimétrica

Definições, diferenças e aplicações

Simétrica


Symmetric Encryption
SAME KEY
SECRET KEY
SECRET KEY
ENCRYPTION
DECRYPTION
1<A$t47KP
52CV#@>?
8\jahs#981
gHTasdsn%
^78ZGWSfg
ORIGINAL TEXT
SCRAMBLED DATA
ORIGINAL TEXT

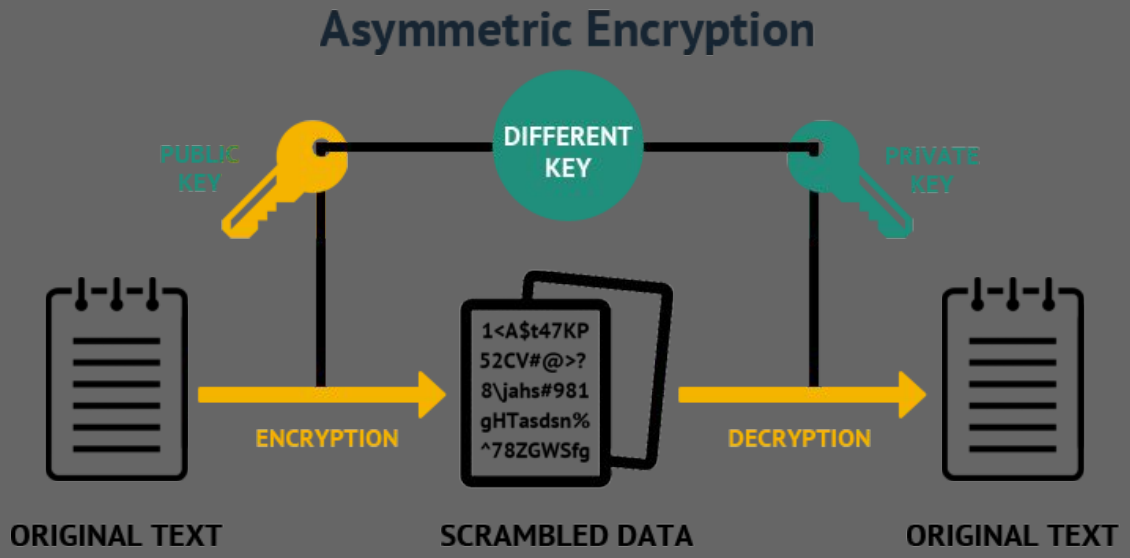
Assimétrica

Assimétrica

- Consiste de uma tripla de algs. (G, E, D)
  - G()
    - Aleatório
    - (pk, sk)
  - E(pk, m) = c
  - D(sk, c) = m

- ∀ (pk, sk) de G(), D(sk, E(pk, m)) = m

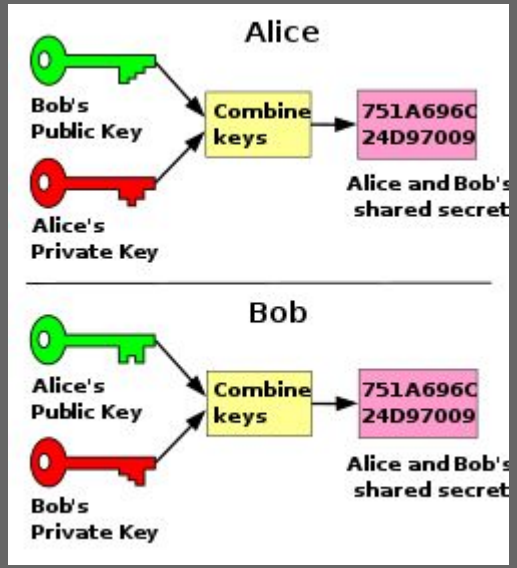
Assimétrica



Estabelecendo um segredo

- Geralmente se baseiam em problemas difíceis (NP)
  - Fatoração de inteiros (RSA e Diffie-Hellman)

- Diffie-Hellman



ICMC USP SÃO CARLOS

Ganesh

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