

Aula 006 - Prática sobre Criptografia Simétrica

Prof. Rogério Aparecido Gonçalves *Universidade Tecnológica Federal do Paraná (UTFPR)*

Nesta aula são introduzidos conceitos, teoria e aspectos práticos sobre Criptografia Simétrica. Com foco nos elementos mais relevantes para o contexto da tecnologia *blockchain*. Será utilizado o OpenSSL por linha de comando com alguns exemplos de algoritmos implementados.

Sumário

1	Criptografia Simétrica	1
2	Leitura do Capítulo 3: Criptografia Simétrica	2
	Referências	2

1 Criptografia Simétrica

Criptografia é a ciência de tornar a informação segura na presença de adversários. Cifradores ou Cifras são algoritmos usados para encriptar/criptografar ou decryptar/descriptar/descriptografar dados, de modo que, se interceptados por um adversário, os dados não tenham sentido para ele sem serem decodificados, o que requer uma chave secreta. A Figura 1 apresenta um modelo básico de Criptografia Simétrica, na qual uma única chave secreta é utilizada para criptografar e descriptografar os dados.

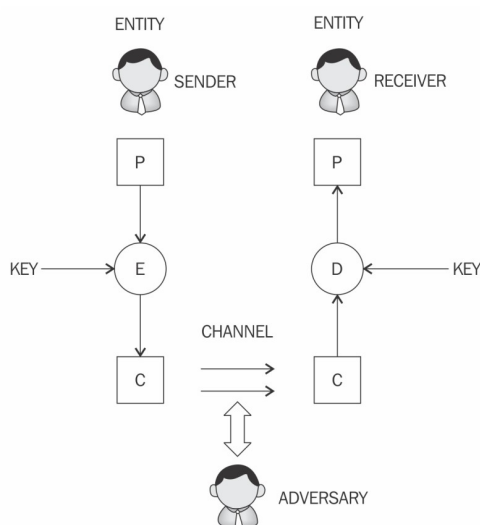


Figure 1: Criptografia

2 Leitura do Capítulo 3: Criptografia Simétrica

1. Faça a leitura do [Capítulo 3: Criptografia Simétrica](#).
2. Execute os exemplos com `openssl` via linha de comando.
3. Faça um relatório simples sobre a execução e os resultados obtidos.

Referências

Imran, Bashir. 2018. *Mastering Blockchain : Distributed Ledger Technology, Decentralization, and Smart Contracts Explained, 2nd Edition*. Packt Publishing. <https://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=1789486&lang=pt-br&site=eds-live&scope=site>.