

Aula 007 - Prática sobre Criptografia Assimétrica

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

Nessa aula o objetivo é compreender alguns algoritmos de *Criptografia Assimétrica*, através da execução de exemplos com OpenSSL.

Sumário

1	Criptografia Assimétrica ou Criptografia de Chave Pública	1
2	Leitura do Capítulo 4: Criptografia de Chave Pública	1
	Referências	1

1 Criptografia Assimétrica ou Criptografia de Chave Pública

Criptografia Assimétrica se refere ao tipo de Criptografia onde a chave que é utilizada para encriptar os dados é diferente da chave que é usada para decriptar os dados criptografados. Esse tipo de Criptografia é conhecido também como **Criptografia de Chave Pública**, onde são usadas uma chave pública para encriptar os dados e uma chave privada para decriptar. Existem diversos esquemas de criptografia assimétrica que estão em uso, incluindo RSA, DSA e ElGamal.

2 Leitura do Capítulo 4: Criptografia de Chave Pública

1. Faça a leitura do [Capítulo 4: Criptografia de Chave Pública](#).
2. Execute os exemplos com `openssl` via linha de comando.
3. Crie uma chave privada, uma chave pública e faça o processo de encriptação/decriptação do conteúdo de um arquivo com os algoritmos RSA, algum algoritmo de ECC e com assinatura digital.
4. 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>.