FICHA DE NOVO COMPONENTE CURRICULAR
DA PÓS-GRADUAÇÃO *STRICTO SENSU* - UFPE

NOME DO PROGRAMA:	Programa de Pós-graduação em Engenharia Elétrica - PPGEE
CENTRO:	Centro de Tecnologia e Geociências - CTG

DADOS DO COMPONENTE			
NOME DO COMPONENTE:	Criptografia		
CARGA HORÁRIA:	60 hs	**TIPO DE COMPONENTE:**	(X) disciplina ( ) atividade
		COMPONENTE FLEXÍVEL:	( ) sim (X) não
EMENTA:	01. Conceitos preliminares e criptografia pré-contemporânea; 02. Segurança incondicional e computacional; 03. Conceitos de teoria da informação: Equivocação e distância de unicidade. 04. Conceitos de criptografia simétrica: confusão e difusão. 05. LFSR's. 06. Sistemas criptográficos DES e AES. 07. Modos de operação. 08. Ataques a sistemas criptográficos simétricos: Meet-in-the-Middle. 09. Conceitos de criptografia assimétrica. 10. Problema do logaritmo discreto (LD) e algoritmos rápidos para cálculo do LD: Algoritmos de colisão (Pollard rho e babystep-giantstep), Pohlig-Hellman, cálculo de índice. 11. Sistemas criptográficos: Algoritmo da Mochila, RSA, Diffie-Hellman, Elgamal, Elíptico. 12. Função de Hash e assinatura digital. 13. blockchain e suas aplicações.		
REFERÊNCIAS:	[1] J. L. Massey, Cryptography: Fundamentals and Applications, Editores: V. C. da Rocha Jr. and R. D. Lins, 1999. Disponível em CD. [2] C. Paar and J. Pelzl, Understanding Cryptography, Springer, 2010. [3] Jeffrey Hoffstein and Jin Pipher and Joseph H. Silverman, "An Introduction to Mathematical Cryptography", 2º Edição, Springer, 2014. [4] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 2001 (quinta impressão). [5] N. Koblitz, A Course in Number Theory and Cryptography, 2º Edição, Springer-Verlag, 2012. [6] William Stallings, "Cryptography and Network Security: Principles and Practice", 8º Edição, Pearson, 2022. [7] Jonathan Katz e Yehuda Lindell, "Introduction to Modern Cryptography", 2º Edition, CRC Press, 2014.		