Relatório de Conteúdo Programático

Grau: Graduação Presencial

Òrgão: TEP - DEPARTAMENTO DE ENGENHARIA DE PRODUÇÃO

Nome: SEGURANCA DA INF I - INT A CRIPTOLOGIA Código: TEP04069

Característica: CO - Comum Status: Desativada

Carga Horaria Total: 60h Estagio: 0h Teorica: 60h Pratica: 0h

Período de vigência: 1º período de 1995 até a presente data.

Conteúdo Programático:

1. SISTEMAS CRIPTOGRÁFICOS CLÁSSICOS
SUBSTITUIÇÃO E TRANSPOSIÇÃO
CIFRA PLAYFAIR
VERNAM E A CHAVE DE UMA SÓ VEZ (CHUSV)
CRIPTOGRAFIA ALGÉBRICA
SHANNON: UMA NOVA PERSPECTIVA

2. SISTEMAS SIMÉTRICOS MODERNOS
DES / NOVO DES / IDEA / RC5 / AES
GERENCIAMENTO DE CHAVES
MODOS DE OPERAÇÃO PARA CIFRAS DE BLOCO

3 - SISTEMAS ASSIMÉTRICOS OU DE CHAVE PÚBLICA
MATEMÁTICA NECESSÁRIA
O PARADÍGMA DA CHAVE PÚBLICA
O RSA
A MOCHILA (" KNAPSACK ")
O SISTEMA DE EL GAMAL
O SISTEMA DE MC ELIECE
CONTRIBUIÇÕES BRASILEIRAS
O SISTEMA DE OKAMOTO
ASSINATURA DIGITAL
CONDENSAÇÃO (" HASHING ")
AUTENTICAÇÃO

4 - ALGORÍTMOS DE FLUXO E GERADORES DE PSEUDO-ALEATÓRIOS
O GERADOR DE MARSAGLIA
GERADORES CONGRUENCIAIS LINEARES E NÃO LINEARES
REGISTRADORES DE DESLOCAMENTO: LINEARES E NÃO LINEARES
GERADOR DE BLUM - BLUM E SHUB
USO DE CIFRAS DE BLOCOS COMO GERADORES DE PSEUDO-ALEATÓRIOS

5 - TÓPICOS VARIADOS
HOMOFONIA / ALEATORIZAÇÃO / PROTOCOLOS CRIPTOGRÁFICOS / COMPARTILHAMENTO DE SEGREDOS / TIPOS DE
CRIPTOANÁLISE / CRIPTOFONIA / NORMAS TEMPEST / NORMAS TÉCNICAS : ABNT-ISO / TESES BRASILEIRAS / PATENTES

Gerado em: 28/05/2019 - 19:55

Relatório de Conteúdo Programático

Ementa:

SISTEMAS CLÁSSICOS. REGISTRADORES DE DESLOCAMENTO. NOÇÕES DE TEORIA DA INFORMAÇÃO. CÓDIGOS DE HUFFMAN. O DES: PADRÃO DE CRIPTOGRAFIA. CRIPTOGRAFIA DE CHAVE PÚBLICA. O SISTEMA RSA. NOÇÕES DE TEORIA DOS NÚMEROS. O SISTEMA DE MC ELIECE. O SISTEMA DA MOCHILA (KNAPSACK). ESQUEMAS DE LIMIAR.

Bibliografia Básica:

1 - CRIPTOGRAFIA:
MÉTODOS E ALGORÍTMOS
DANIEL B. CARVALHO (EDITORA BOOK EXPRESS LTDA. - RIO-2000)
2 - APPLIED CRYPTOGRAPHY
B. SCHNEIER
WILLEY - N. YORK - 1996

Bibliografia Complementar:

NÃO DISPONÍVEL.

Gerado em: 28/05/2019 - 19:55