

Asas Kriptografi

Sinopsis:

Keselamatan data amat penting pada era siber. Salah satu mekanisme keselamatan data ialah kriptografi iaitu satu teknik yang menukarkan maklumat kepada bentuk yang tidak dapat dibaca atau difahami dengan menggunakan kekunci. Buku ini membincangkan pembangunan algoritma kriptografi yang terdiri daripada kriptografi kekunci simetri dan tak simetri. Bagi memudahkan kefahaman algoritma kekunci tak simetri, asas teori maklumat dan teori nombor juga diterangkan dalam buku ini. Selain daripada itu, algoritma cincang dan pengenalan steganografi juga dimuatkan. Buku ini sesuai digunakan oleh pelajar peringkat ijazah sarjana muda dan juga sarjana serta mereka yang ingin melakukan pembangunan perisian keselamatan data.

Asas Kriptografi

Kandungan:

Prakata

BAB 1 PENGENALAN

Keselamatan Maklumat

Tujuan Keselamatan

Serangan Keselamatan

Perkhidmatan Keselamatan

BAB 2 KRIPTOGRAFI SEPINTAS LALU

Tujuan Kriptografi

Definisi dan Terminologi

Kriptografi Klasik

Kriptografi Moden

Cerna Mesej

Tanda Tangan Digital

Protokol Umum

Sistem Hibrid

BAB 3 SEJARAH PERKEMBANGAN KRIPTOGRAFI

Sifer Purbakala

Mesin Sifer

Mesin Rotor

Sifer Enigma

Perkembangan Kriptografi Moden

BAB 4 TEORI MAKLUMAT DAN TEORI NOMBOR

Teori Maklumat

Aritmetik Modulo

Nombor Perdana dan Pembahagian Sepunya Terbesar (GCD)

Songsangan Modulo

Algoritma Euclid

Teorem Baki Cina

Logaritma Diskret

BAB 5 KRIPTOGRAFI KLASIK

Teknik Penggantian

Sifer Penyerakan

BAB 6 KRIPTOGRAFI SIMETRI

Sistem Kekunci Simetri

Kelebihan dan Kelemahan

Data Encryption Standard (DES)