UNIVERSITA'DEGLI STUDI DI ENNA "KORE"
Corso di Laurea In Ingegneria Telematica Classe L9

CORSO DI SICUREZZA NEI SISTEMI INFORMATICI
III ANNO CFU 6 I SEMESTRE A.A. 2010/2011
Docente Ing. Conti Vincenzo

- Introduzione al corso
- Attacchi alla sicurezza
- Meccanismi di sicurezza
- Tecniche di crittografia
- Modello ci cifratura simmetrico classico
- Tecniche di sostituzione
- Cifratura a blocchi
- Algoritmo DES (Data Encryption Standard)
- Lo standard AES (Advanced Encryption Standard)
- Sviluppi della cifratura simmetrica
- Doppio e triplo DES
- Modalità di funzionamento della cifratura a blocchi
- Crittografia a chiave pubblica
- Algoritmo RSA
- Gestione delle chiavi
- Applicazioni della sicurezza

Testo di riferimento

Crittografia e sicurezza delle reti – William Stallings – McGraw-Hill Editore