

# PROGRAMMA DEL CORSO DI SICUREZZA INFORMATICA

## SETTORE SCIENTIFICO

ING-INF/05

## CFU

4

## DESCRIZIONE

- 1 - CONCETTI BASE DI SICUREZZA
- 2 - SERVIZI E MECCANISMI DI SICUREZZA
- 3 - CRITTOGRAFIA SIMMETRICA
- 4 - CRITTOGRAFIA SIMMETRICA: TECNICHE DI SOSTITUZIONE E DI TRASPOSIZIONE
- 5 - CIFRATURA A BLOCCHI
- 6 - LA CIFRATURA DES: DATA ENCRYPTION STANDARD
- 7 - LA CIFRATURA AES - ADVANCED ENCRYPTION STANDARD
- 8 - LA CRITTOGRAFIA MULTIPLA
- 9 - MODALITA' DI FUNZIONAMENTO DELLA CIFRATURA A BLOCCHI
- 10 - SEGRETEZZA E CRITTOGRAFIA SIMMETRICA
- 11 - CRITTOGRAFIA ASIMMETRICA
- 12 - L'ALGORITMO RSA
- 13 - GESTIONE DELLE CHIAVI E SCAMBIO DIFFIE-HELLMAN
- 14 - AUTENTICAZIONE DEI MESSAGGI
- 15 - CODICI MAC E FUNZIONI HASH
- 16 - L'ALGORITMO SHA-512
- 17 - GLI ALGORITMI HMAC E CMAC
- 18 - LE FIRME DIGITALI
- 19 - LA SICUREZZA INFORMATICA

20 - LA SICUREZZA INFORMATICA AZIENDALE

21 - NORMATIVE A PROTEZIONE DEI DATI E DELLA SICUREZZA INFORMATICA

22 - LA TUTELA GIURIDICA DEI DATI PERSONALI E LE MISURE DI PROTEZIONE DELLE PUBBLICHE AMMINISTRAZIONI

23 - LA TUTELA DELLE COMUNICAZIONI INFORMATICHE E TELEMATICHE E LE MODALITA' DI INTERCETTAZIONE

24 - SISTEMI E TECNOLOGIE DI PROTEZIONE