

Criptografia avançada

Llorenç Huguet Rotger

Josep Rifà Coma

Juan Gabriel Tena Ayuso

PID_00185087

Material docent de la UOC

Llorenç Huguet Rotger**Josep Rifà Coma****Juan Gabriel Tena Ayuso**

L'encàrrec i la creació d'aquest material docent han estat coordinats per la professora Helena Rifà Pous per al programa del Màster Interuniversitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions –MISTIC– (2012)



Primera edició: febrer 2012

© Llorenç Huguet Rotger, Josep Rifà Coma, Juan Gabriel Tena Ayuso

Tots els drets reservats

© d'aquesta edició, FUOC, 2012

Av. Tibidabo, 39-43, 08035 Barcelona

Disseny: Manel Andreu

Realització editorial: Eureka Media, SL

Dipòsit legal: B-3.167-2012



Els textos i imatges publicats en aquesta obra estan subjectes –llevat que s'indiqui el contrari– a una llicència de Reconeixement-NoComercial-SenseObraDerivada (BY-NC-ND) v.3.0 Espanya de Creative Commons. Podeu copiar-los, distribuir-los i transmetre'ls públicament sempre que en citeu l'autor i la font (FUOC. Fundació per a la Universitat Oberta de Catalunya), no en feu un ús comercial i no en feu obra derivada. La llicència completa es pot consultar a <http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.ca>

Continguts

Mòdul didàctic 1

Cossos finits

Llorenç Huguet Rotger, Josep Rifà Coma, Juan Gabriel Tena Ayuso

1. Existència i propietats dels cossos finits
2. Bases de cossos finits
3. Computació en cossos finits

Mòdul didàctic 2

Elements de criptografia

Llorenç Huguet Rotger, Josep Rifà Coma, Juan Gabriel Tena Ayuso

1. Criptosistemes simètrics o de clau privada
2. Criptosistemes de clau pública
3. Criptografia quàntica i postquàntica

Mòdul didàctic 3

Protocols criptogràfics

Llorenç Huguet Rotger, Josep Rifà Coma, Juan Gabriel Tena Ayuso

1. Protocols de gestió i distribució de claus
2. Protocols d'autenticació
3. Transaccions electròniques segures: diners electrònics
4. Protocols de transferència inconscient
5. Esquemes llindar i repartiment de secrets
6. Votacions electròniques

Mòdul didàctic 4

Criptografia amb corbes el·líptiques

Llorenç Huguet Rotger, Josep Rifà Coma, Juan Gabriel Tena Ayuso

1. Corbes i punts racionals
2. Geometria de les corbes el·líptiques
3. Corbes el·líptiques sobre cossos finits
4. L'ús de les corbes el·líptiques en criptografia
5. Criptografia i protocols criptogràfics basats en corbes el·líptiques
6. ECC estàndards i aplicacions

Mòdul didàctic 5

Pairings i les seves aplicacions

Llorenç Huguet Rotger, Josep Rifà Coma, Juan Gabriel Tena Ayuso

1. *Pairings* en corbes el·líptiques
2. Atacs basats en *pairings*
3. Criptografia basada en la identitat

