
Criptografia

PID_00235158

Jordi Herrera Joancomartí
Cristina Pérez Solà

**Jordi Herrera Joancomartí**

Llicenciat en Matemàtiques per la Universitat Autònoma de Barcelona i doctor per la Universitat Politècnica de Catalunya. Els seus àmbits de recerca són la criptografia, les criptomonedes i la tecnologia *blockchain*. Ha publicat nombrosos textos doctes i més de cent articles de recerca en revistes i congressos nacionals i internacionals. Ha dirigit nou tesis doctorals i ha estat investigador principal de diversos projectes de recerca nacionals. Ha participat com a avaluador per a agències de recerca de diversos països europeus i també per a la Comissió Europea. Actualment és professor agregat del departament d'Enginyeria de la Informació i les Comunicacions a la Universitat Autònoma de Barcelona.

**Cristina Pérez Solà**

Doctora en Informàtica per la Universitat Autònoma de Barcelona i la Universitat Catòlica de Lovaina. Actualment és professora dels Estudis d'Informàtica, Multimèdia i Telecomunicacions de la Universitat Oberta de Catalunya. Els seus àmbits de recerca són les criptomonedes basades en *blockchain* i, en especial, els aspectes relacionats amb la seguretat i la privadesa d'aquestes. També està interessada en els problemes de privacitat que sorgeixen arran de l'ús de les xarxes socials i en l'adaptació de tècniques de mineria de dades a la naturalesa específica d'aquest tipus de xarxes.

L'encàrrec i la creació d'aquest recurs d'aprenentatge UOC han estat coordinats per la professora: Helena Rifà Pous

Segona edició: febrer 2021
© d'aquesta edició, FUOC, 2021
Av. Tibidabo, 39-43, 08035 Barcelona
Autoria: Jordi Herrera Joancomartí, Cristina Pérez Solà
Producció: FUOC
Tots els drets reservats

Cap part d'aquesta publicació, incloent-hi el disseny general i la coberta, no pot ser copiada, reproduïda, emmagatzemada o transmesa de cap manera ni per cap mitjà, tant si és elèctric com mecànic, òptic, de gravació, de fotocòpia o per altres mètodes, sense l'autorització prèvia per escrit del titular dels drets.

Continguts

Modul didàctic 1

Introducció a la criptografia

Cristina Pérez Solà i Jordi Herrera Joancomartí

1. Conceptes bàsics
2. Una mica d'història

Modul didàctic 2

Fonaments matemàtics

Jordi Herrera Joancomartí i Cristina Pérez Solà

1. Aritmètica modular
2. Nombres primers
3. Problemes matemàtics difícils

Modul didàctic 3

Criptografia de clau simètrica

Jordi Herrera Joancomartí i Cristina Pérez Solà

1. Criptografia de clau simètrica o compartida
2. Les xifres de flux
3. Generadors lineals de seqüència xifrant
4. Generadors no lineals
5. Les xifres de bloc
6. El criptosistema AES

Modul didàctic 4

Funcions hash

Jordi Herrera Joancomartí i Cristina Pérez Solà

1. Les funcions hash
2. Construcció de funcions hash
3. L'estàndard SHA-256
4. Aplicacions de les funcions hash

Modul didàctic 5

Criptografia de clau pública

Cristina Pérez Solà i Jordi Herrera Joancomartí

1. L'origen de la criptografia de clau pública
2. Intercanvi de claus de Diffie-Hellman
3. Xifres de clau pública

4. Signatures digitals
5. Criptografia simètrica i asimètrica
6. Implementació dels algorismes de clau pública
7. Criptografia postquàntica

Modul didàctic 6

Infraestructura de clau pública

Cristina Pérez Solà i Jordi Herrera Joancomartí

1. Entitats d'una PKI
2. Cicle de vida d'un certificat digital
3. Els estàndards X.509
4. Les normes PKCS
5. Formats de representació de dades
6. Els problemes de la PKI en desplegaments reals

Modul didàctic 7

Protocols criptogràfics

Jordi Herrera Joancomartí i Cristina Pérez Solà

1. El protocol de tres passos de Shamir
2. Esquemes de compartició de secrets
3. Signatures cegues
4. Proves de coneixement nul
5. Protocol de transferència inconscient
6. Protocol multipart segur