Criptografia

PID_00235158

Jordi Herrera Joancomartí
Cristina Pérez Solà

Universitat Oberta de Catalunya

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 docents 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

Av. Tibidabo, 39-43, 08035 Barcelona
Autoria: Jordi Herrera Joancomartí, Cristina Pérez Solà
Producció: FUOC

Continguts

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