

Opleiding : Inleiding tot cryptografie

Praktijkcursus - 3d - 21u00 - Ref. CYP

Prijs : 2100 € V.B.



4,2 / 5

Deze cursus presenteert de verschillende cryptografische technieken en hun belangrijkste toepassingen. Symmetrische en asymmetrische encryptie, hashing, de meest gebruikte algoritmen en sleutelbeheermethodes worden in detail uitgelegd.



Pedagogische doelstellingen

Aan het einde van de training is de deelnemer in staat om:

- ✓ De woordenschat van cryptologie beheersen: algoritme, hash, sleutel, etc.
- ✓ Leer over de meest gebruikte algoritmen in cryptologie
- ✓ Methoden identificeren voor het uitwisselen, beheren en certificeren van openbare sleutels
- ✓ Symmetrische en asymmetrische versleutelingstools gebruiken

Doelgroep

Beveiligingsmanagers, ontwikkelaars, projectmanagers.

Voorafgaande vereisten

Geen speciale kennis vereist.

Opleidingsprogramma

1 Inleiding

- Geschiedenis van de eerste versleutelde documenten.
- Cryptografische diensten.
- Wiskundige concepten.
- Cryptografische beveiliging en aanvalstechnieken.

DEELNEMERS

Beveiligingsmanagers, ontwikkelaars, projectmanagers.

VOORAFGAANDE VEREISTEN

Geen speciale kennis vereist.

VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vakkennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, ... De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

2 Streamcijfers

- Presentatie van het concept.
- Lineair feedbackstroomregister (LFSR): details over hoe het werkt, Galois LFSR, toepassingen.
- Andere vormen van stream encryptie: RC4, SEAL.

3 Blokcijfers

- Presentatie van het concept.
- De verschillende vormen: Electronic CodeBook (ECB), Cipher-Bloc Chaining (CBC), Cipher FeedBack (CFB), etc.
- Vergelijking van stroom- en blokversleuteling.
- Data Encryption Standard (DES).
- Triple DES (3DES): presentatie, werkprocedures.
- Geavanceerde Encryptie Standaard (AES).
- Aanvullende algoritmen: IDEA, RC5, SAFER.

4 Asymmetrische encryptie

- Het RSA-algoritme in detail. Veiligheid en sleutelgrootte. Aanvallen en de RSA-uitdaging. Praktische toepassingen.
- ElGamal encryptie. ElGamal in DSA.

5 Hash-functies

- Concept en doelstellingen.
- Algoritmische principes. Wiskundige eigenschappen.
- Praktische rechtvaardigingen voor de verschillende eigenschappen.
- Hashbeveiliging en -lengte.
- Eenvoudig (Unkeyed) en veilig (Keyed) hashen: blokvercijfering. MD4-functie.
- Geavanceerde aanvallen op hashfuncties.
- Technische presentatie van hashfuncties: SHA-1, SHA-256 en SHA-512. MD5. Haval. RIPEMD-128...

6 Integriteit en authenticatie

- Presentatie. CBC-MAC-standaarden. HMAC.
- Elektronische handtekening. DSA en RSA handtekening.

7 Sleutelbeheer

- Sleuteluitwisseling met symmetrische en asymmetrische encryptie. Details van uitwisselingen.
- Diffie-Hellman algoritme. Man-in-the-middle aanval.
- Beheer van openbare sleutels en certificering.
- Intrekken, vernieuwen en archiveren van sleutels.
- X509-formaat certificaten, PKIX-standaard.
- Sleutelbeheerinfrastructuur (PKI).

8 Vertrouwde derde partijen

- Presentatie en standaarden. Architecturen.
- Certificeringsinstantie. Kerberos.

PEDAGOGISCHE EN TECHNISCHE MIDDELEN

- De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
- Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
- Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

TOEGANGSMODALITEITEN EN TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

KLAS OP AFSTAND

2026 : 23 maa., 27 mei, 28 sep., 23 nov.

PARIS LA DÉFENSE

2026 : 23 maa., 27 mei, 28 sep., 23 nov.