Szkolenie: Compendium CE

Szyfrowanie i łamanie szyfrów

DOSTĘPNE TERMINY

2026-11-04 | 2 dni | Warszawa / Wirtualna sala
2026-12-02 | 2 dni | Kraków / Wirtualna sala

Cel szkolenia:

Handel elektroniczny, e-banking, podpis elektroniczny a nawet alarmy samochodowe nie mogą się obejść bez szyfrowania. Obecnie praktycznie każda przeglądarka WWW jest wyposażona w tak silne mechanizmy kryptograficzne jakimi kilkadziesiąt lat temu nie dysponowało nawet wojsko. Równocześnie co chwilę ukazują się nowe informacje o złamaniu tego czy innego szyfru, producenci prześcigają się w długościach kluczy i sile szyfrowania. Celem szkolenia ilustrowanego przykładami praktycznymi jest omówienie podstawowych zasad współczesnej kryptografii, jej silnych i słabych stron oraz możliwości ataków na systemy kryptograficzne.

Plan szkolenia:

- Cele i środki kryptografii
  - Komu jest potrzebna kryptografia?
  - Czy kryptografia to tylko szyfrowanie?
  - Szyfrowanie, kodowanie, enkrypcja, integralność, terminologia
- Historia kryptografii
  - Czasy starożytne
  - Średniowiecze
  - XIX-XX wiek
  - Czasy najnowsze
  - Kryptografia, polityka, terroryści
- Podstawy warsztatu kryptograficznego
  - Reguła Kerckhoffa
  - Szyfry przeszłości (Cezar, Vigenere i inne)
  - Szyfr jednorazowy (OTP)
  - Podstawowe typy ataków na szyfry
- Współczesny warsztat kryptograficzny
  - Magiczny XOR
  - Szyfry blokowe vs strumieniowe

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Tryby pracy szyfrów blokowych
- Funkcje skrótu i kontrola integralności
- Szyfry symetryczne vs asymetryczne
- Liczby losowe w kryptografii

- Szyfry blokowe
  - DES, DES-X, 3DES
  - AES
- Funkcje skrótu
  - MD5
  - SHA-1
  - SHA-2
- Szyfry asymetryczne
  - RSA
  - ElGamal
  - Krzywe eliptyczne (ECC)
- Algorytmy, protokoły
  - Algorytm a protokół
  - SSL, TLS
  - SSH
  - IPSec, ISAKMP, ESP
- Systemy kryptograficzne
  - Algorytmy, klucze, zaufanie
  - PGP
  - X.509
  - Ciphire
- Problemy kryptografii
  - Snake-oil security
  - Security through obscurity
  - Jak rozpoznać „złą kryptografię”?

Wymagania:

Podstawowa znajomość Windows, popularnych programów pocztowych oraz biurowych.

Poziom trudności



Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

Certyfikaty:

Uczestnicy szkolenia "**Szyfrowanie i łamanie szyfrów**" otrzymują **certyfikat** wystawiony imiennie oraz na firmę, sygnowany przez **Compendium - Centrum Edukacyjne**.

Prowadzący:

Wykładowca Compendium Centrum Edukacyjnego.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001