

Szkolenie: Compendium CE
Szyfrowanie i łamanie szyfrów

DOSTĘPNE TERMINY

2025-05-22 | 2 dni | Kraków / Wirtualna sala
2025-06-26 | 2 dni | Warszawa / 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

- 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



Certyfikaty:

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

Prowadzący:

Wykładowca Compendium Centrum Edukacyjnego.