Praktická kryptografie pro správce i vývojáře a post-quantum kryptografie

Kód kurzu: GOC161

Třídenní kurz seznamuje posluchače praktickou cestou s principy a vlastnostmi aktuálně používaných šifrovacích, podpisových a hash algoritmů, jako jsou AES, ML-KEM, ML-DSA, RSA, SHA256, SHA1, ECDSA, ECDH, RC4 a dalších, také problémů generování náhodných čísel, důvody pro nejnovější post-quantum algoritmy, stejně se základy technologie digitálních certifikátů a protokolů vyšší úrovně jako je TLS/SSL, Kerberos, nebo DPAPI, šifrováním disků (například BitLocker) a databází, ukládáním šifrovacích klíčů a hesel na webových serverech, v databázcích a prohlížečích a trezorech hesel, probírají se i časová razítka. Školení a příklady je prováděno na platformě Windows, ale všechny technologie jsou obecně platné a otevřeně standardní. Certifikátům a PKI se detailně věnuje navazující školení.

Pro koho je kurz určen

- Kurz je určen jak správcům IT tak i vývojářům, návrhářům systémů a aplikací, kteří se chtějí orientovat v aktuálních technologiích a trendech.

Co vás na kurzu naučíme

- Porozumnět principům kryptografie a vidět je v aktuálně používaných algoritmech
- Chápat bezpečnostní a výkonové limity starších i aktuálních šifrovacích a hash algoritmů
- Na aktuálních technologiích porozumnět použití nejmodernějších algoritmů i těch starších v případě nutné kompatibility
- Umět si navrhnout zabezpečení databáze, datových disků i disků operačního systému, šifrování komunikace klient-server
- Dokázat zabezpečit šifrovací klíče a hesla na webových serverech, v databázích, při přenosu mezi uživatelem a serverem, využívat vícefaktorové ověřování
- Zvolit správně sílu a parametry PKI kryptografií a porozumnět souvisejícím technologiím, jako jsou časová razítka

Předpokládané vstupní znalosti

- Znalosti v rozsahu kurzů uvedených v sekcích
- Předchozí kurzy
- a
- Související kurzy
- Dobrá znalost technologií TCP/IP a DNS

Osnova kurzu

- Základy matematiky pro kryptografii, XOR, modulo, polynomy, náhodná čísla a další
- Kombinace a permutace, náročnost algoritmů a work-factor, aktuální výpočetní možnosti
- Hesla versus hash funkce a CRC kontrolní součty
- Historické okénko, Ceasar, Vernam a jejich kamarádi, transpoziční a substituční šifry, tabulky
- Symetrické algoritmy a asymetrické algoritmy, časové náročnosti, výpočetní výkon a síla proti bruteforce
- AES, ML-KEM, ML-DSA, RC4, DES a 3DES (TDEA), bloky a proudy, vliv délky textu, režimy ECB, CBC, CFB, OFB, CTR, CCM, GCM a další jejich mutace
- MD2, MD5, MD4, SHA1, SHA 2 (SHA256, SHA384, SHA512), SHA3, HMAC, náhodná čísla
- Útoky typu brute-force, dictionary, rainbow table, password guessing, offline password/hash analysis a jejich praktická (ne)proveditelnost
- Historické a aktuální praktické příklady aplikace symetrických algoritmů na TLS/SSL, Kerberos, NTLM, BitLocker, DPAPI, ukládání a přenos hesel, trezory na hesla (KeePass) a další
- Asymetrická kryptografie RSA a ECDSA a ML-DSA, digitální podpis a jeho kombinace s hash algoritmy
- Domluva šifrovacích klíčů, RSA Key Exchange a (EC)DH Key Agreement a ML-KEM
- Kombinace algoritmů symetrických, asymetrických, hash a domluvy klíčů v reálných technologiích TLS/SSL, IPSec, VPN, (P)EAP/TLS, WiFi WPA/2 apod.
- Návrh zabezpečení dat v databázích, při jejich přenosu a při přístupu k datům

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved

- Technologie ověřování uživatelských "hesel", formy přihlašovacích údajů, vícefaktorové a biometrické metody, jejich vhodnost a vlastnosti
- Návrh bezpečného přihlašování do webových i GUI aplikací
- Návrh metod ukládání a izolace dat pomocí kryptografických metod
- Hardware zařízení jako jsou čipové karty, tokeny a HSM (hardware security moduly), jejich bezpečnost a (ne)izolace klíčů
- Optimalizace výkonu a rychlosti za použití přiměřeně bezpečných algoritmů

Příprava k certifikačním zkouškám

- Kurz není přímo přípravou na žádnou certifikační zkoušku, ale je může být vhodnou formou k doplnění základních znalostí obecných bezpečnostních technologií.

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved