

# Praktická kryptografia pre správcov a vývojárov a post-quantum kryptografia

Kód kurzu: GOC161

Trojdnňový kurz zoznamuje poslucháčov praktickou cestou s princípmi a vlastnosťami aktuálne používaných šifrovacích, podpisových a hash algoritmov, ako sú AES, ML-KEM, ML-DSA, RSA, SHA256, SHA1, ECDSA, ECDH, RC4 a ďalších, tiež problémov generovania náhodných čísel, dôvody pre a protokolov vyššej úrovne ako je TLS/SSL, Kerberos, alebo DPAPI, šifrovaním diskov (napríklad BitLocker) a databáz, ukladaním šifrovacích kľúčov a hesiel na webových serveroch, v databázach a prehliadačoch a trezoroch hesiel, preberajú sa aj časové pečiatky. Školenia a príklady je vykonávané na platforme Windows, ale všetky technológie sú všeobecne platné a otvorene štandardné. Certififikátum a PKI se detailně věnuje navazující školení.

| Pobočka    | Dní | Katalógová cena | ITB |
|------------|-----|-----------------|-----|
| Praha      | 3   | 17 100 Kč       | 30  |
| Brno       | 3   | 17 100 Kč       | 30  |
| Bratislava | 3   | 750 €           | 30  |

Všetky ceny sú uvedené bez DPH.

## Termíny kurzu

| Dátum                                                                                         | Dní | Cena kurzu | Typ výučby    | Jazyk výučby | Lokalita         |
|-----------------------------------------------------------------------------------------------|-----|------------|---------------|--------------|------------------|
|  18.11.2026  | 3   | 17 100 Kč  | Teleprezenčný | CZ/SK        | GOPAS Praha      |
|  18.11.2026  | 3   | 17 100 Kč  | Teleprezenčný | CZ/SK        | GOPAS Brno       |
|  18.11.2026 | 3   | 750 €      | Teleprezenčný | CZ/SK        | GOPAS Bratislava |

Všetky ceny sú uvedené bez DPH.

## Pre koho je kurz určený

Kurz je určený ako správcom IT, tak aj vývojárom, návrhárom systémov a aplikácií, ktorí sa chcú orientovať v aktuálnych technológiách a trendoch.

## Čo vás na kurze naučíme

- Porozumieť princípom kryptografie a vidieť ju v aktuálne používaných algoritmoch
- Chápať bezpečnostné a výkonové limity starších i aktuálnych šifrovacích a hash algoritmov
- Na aktuálnych technológiách chápať použitie najmodernejších algoritmov aj tých starších v prípade nutnej kompatibility
- Vedieť si navrhnuť zabezpečenia databázy, dátových diskov aj diskov operačného systému, šifrovanie komunikácie klient-server
- Dokázať zabezpečiť šifrovacie kľúče a heslá na webových serveroch, v databázach, pri prenose medzi užívateľom a serverom, využívať multifaktorové overovanie
- Zvoliť správne silu a parametre PKI kryptografie a porozumieť súvisiacim technológiám, ako jsou časové pečiatky

## Predpokladané vstupné znalosti

- Znalosti v rozsahu kurzov uvedených v sekciách
- **Predchádzajúce**
- **kurzy**
- a
- **Súvisiace**
- **kurzy**
- Dobrá znalosť technológií TCP/IP a DNS

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

**GOPAS Brno**  
Nové sady 996/25  
602 00 Brno  
Tel.: +420 530 513 590  
[info@gopas.cz](mailto:info@gopas.cz)

**GOPAS Bratislava**  
Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 902 903 132  
[info@gopas.sk](mailto:info@gopas.sk)



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

# Praktická kryptografia pre správcov a vývojárov a post-quantum kryptografia

## Osnova kurzu

- Základy matematiky pre kryptografiu, XOR, moduly, polynómy, náhodné čísla a ďalšie
- Kombinácia a permutácie, náročnosť algoritmov a work-factor, aktuálne výpočtové možnosti
- Heslá versus hash funkcie a CRC kontrolné súčty
- Historické okienko, Ceasar, Vernay a ich kamaráti, transpozíčné a substitučné šifry, tabuľky
- Symetrické algoritmy a asymetrické algoritmy, časové náročnosti, výpočtový výkon a sila proti bruteforce
- AES, ML-KEM, ML-DSA, RC4, DES a 3DES (TDEA), bloky a prúdy, vplyv dĺžky textu, režimy ECB, CBC, CFB, OFB, CTR, CCM, GCM a ďalšie ich mutácie
- MD2, MD5, MD4, SHA1, SHA 2 (SHA256, SHA384, SHA512), SHA3, HMAC, náhodné čísla
- Útoky typu brute-force, dictionary, rainbow table, password Guessing, offline password/hash analysis a ich praktická (ne)uskutočniteľnosť
- Historické a aktuálne praktické príklady aplikácie symetrických algoritmov na TLS/SSL, Kerberos, NTLM, BitLocker, DPAPI, ukladanie a prenos hesiel, trezory na heslá (KeePass) a ďalšie
- Asymetrická kryptografia RSA a ECDSA a ML-DSA, digitálny podpis a jeho kombinácia s hash algoritmami
- Dohoda šifrovacích kľúčov, RSA Key Exchange a (EC)DH Key Agreement a ML-KEM
- Kombinácia algoritmov symetrických, asymetrických, hash a dohody kľúčov v reálnych technológiách TLS/SSL, IPSec, VPN, (P)EAP/TLS, WiFi WPA/2 a pod.
- Návrh zabezpečenia dát v databázach, pri ich prenose a pri prístupe k dátam
- Technológia overovania používateľských "hesiel", formy prihlasovacích údajov, multifaktorové a biometrické metódy, ich vhodnosť a vlastnosti
- Návrh bezpečného prihlasovania do webových aj GUI aplikácií
- Návrh metód ukladania a izolácie dát pomocou kryptografických metód
- Hardware zariadenia ako sú čipové karty, tokeny a HSM (hardware security moduly), ich bezpečnosť a (ne)izolácia kľúčov
- Optimalizácia výkonu a rýchlosti s použitím primerane bezpečných algoritmov

## Príprava k certifikačným skúškam

Kurz nie je priamo prípravou na žiadnu certifikačnú skúšku, ale môže byť vhodnou formou na doplnenie základných znalostí všeobecných bezpečnostných technológií.

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

**GOPAS Brno**  
Nové sady 996/25  
602 00 Brno  
Tel.: +420 530 513 590  
[info@gopas.cz](mailto:info@gopas.cz)

**GOPAS Bratislava**  
Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 902 903 132  
[info@gopas.sk](mailto:info@gopas.sk)



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