Odporúčania pre kryptografické algoritmy

Odporúčania pre kryptografické algoritmy			
Číslo verzie	**1.0**	**Platnosť od**	**08.10. 2025**

Obsah

Úvod

Tento dokument poskytuje odporúčania pre výber a používanie kryptografických algoritmov s dôrazom na vysokú úroveň bezpečnosti, odolnosť voči kvantovým hrozbám a dodržiavanie aktuálnych štandardov. Pre symetrické šifrovanie sa odporúča používať moderné a overené algoritmy s dostatočnou dĺžkou kľúča. V prípade asymetrických algoritmov sa odporúča zvoliť riešenia poskytujúce primeranú úroveň odolnosti voči súčasným aj budúcim výpočtovým možnostiam. V oblasti post kvantovej kryptografie je vhodné zohľadniť algoritmy navrhnuté na odolnosť voči budúcim možným kvantovým útokom. Všetky odporúčané algoritmy by mali byť implementované s použitím bezpečných knižníc a podľa najnovších bezpečnostných odporúčaní. Všetky šifrovacie algoritmy uvedené v tomto dokumente považujeme za dostatočne kvalitné. Pokiaľ je to z hľadiska konkrétnej aplikácie možné, odporúčané sú najväčšie dĺžky kľúčov ktoré dané algoritmy podporujú.

Symetrické algoritmy

Odporúčanie pre symetrické algoritmy:

Pri používaní symetrických algoritmov, či už blokových alebo prúdových, odporúčame používať kľúče s dĺžkou minimálne 256 bitov, aby bola zabezpečená vysoká odolnosť aj v budúcnosti voči kvantovým útokom.

Použitie 192 alebo 128 bitových kľúčov je možné, avšak efektívna bezpečnosť v takom prípade klesá, najmä pri potenciálnych kvantových hrozbách.

Preferujeme blokové šifry pred prúdovými, pretože poskytujú vyššiu odolnosť proti rôznym typom útokov a umožňujú flexibilnejšie využitie v rôznych bezpečnostných režimoch.

Blokové šifry

Odporúčané dĺžky kľúčov sú aktuálne najväčšie podporované dĺžky pre dané algoritmy.

Advanced Encryption Standard (AES) [1] s dĺžkou kľúča 256 bitov
Camellia s dĺžkou kľúča 256 bitov [2]
Twofish s dĺžkou kľúča 256 bitov
Serpent s dĺžkou kľúča 256 bitov

Prúdové šifry

Odporúčané dĺžky kľúčov sú aktuálne najväčšie podporované dĺžky pre dané algoritmy.

ChaCha20 [3] **s dĺžkou kľúča 256 bitov** a obmedzením využitia kľúča na menej než 256 GB dát
SNOW 3G [4] **s dĺžkou kľúča 256 bitov**

Dôvod výberu:

Groverov kvantový algoritmus (Lov Grover -1996) umožňuje hľadanie kľúčov ľubovoľného kryptografického systému hrubou silou, ktorý je však tiež podstatne menej efektívny než Shorov algoritmus. Dôsledkom je, že za bezpečné voči Groverovmu algoritmu považujeme iba tie blokové a prúdové šifry, ktoré majú kľúče dlhé 256 bitov alebo viac.

Asymetrické algoritmy

Asymetrické algoritmy sú najviac ohrozené nástupom kryptograficky relevantných kvantových počítačov. V akademickej sfére, odbornej a štátnej sfére existuje konsenzus, že kryptograficky relevantná kvantová výpočtová technika s vysokou pravdepodobnosťou spôsobí stav, kedy šifrovanie, ktoré dnes bežne používame na výmenu kľúča alebo elektronický podpis, nebude viac dostatočne bezpečné (Odporúčanie Komisie z 11. 4. 2024 o Pláne koordinovaného vykonávania prechodu na post-kvantovú kryptografiu)[1].

Asymetrické kryptografické algoritmy sa z hľadiska rezistencie na hrozby kryptograficky relevantných kvantových počítačov rozdeľujú do kategórie:

- klasické, kvantovo nerezistentné, ktoré sa neodporúča použiť samostatne, alebo už iba dočasne ako dosluhujúce,
- kvantovo rezistentné, t.j. PQC algoritmy, ktoré je možné použiť samostatne, alebo aj v kombinácii s klasickým asymetrickým algoritmom v hybridnej schéme.

Klasické asymetrické algoritmy

Klasické asymetrické algoritmy, ktorých bezpečnosť závisí od faktorizácie prvočísiel (RSA) alebo na počítaní diskrétnych logaritmov nad konečnými poľami alebo eliptických kriviek (DH/ECDH, DSA/ECDSA) nie je možné považovať za bezpečné pre budúce použitie, pretože nie sú odolné voči kvantovým útokom a ich bezpečnosť bude s najväčšou pravdepodobnosťou pri dostupnosti kryptograficky relevantného (dostatočne výkonného) kvantového počítača prelomená.

Post kvantové algoritmy

Prechod na kvantovo odolnú kryptografiu predstavuje novú výzvu a je potrebné sa s ňou dôkladne oboznámiť. Post kvantové algoritmy sú navrhnuté tak, aby poskytovali odolnosť proti kvantovým výpočtom a zabezpečovali bezpečnú výmenu kľúčov aj digitálne podpisy aj v ére kvantových technológií.

Pri výbere odporúčaných algoritmov sme vychádzali z najnovších uznávaných štandardov a dobrej praxe.

Samostatné použitie – výmena kľúčov

ML-KEM-768 Level 3 [5]
ML-KEM-1024 Level 5 [5]

[1] https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography

Hybridná kvantovo odolná kryptografia – výmena kľúčov

ML-KEM-1024 / Kyber-1024, ML-KEM-768 / Kyber-768
Predbežne: **FrodoKEM-1344, FrodoKEM-976**
Predbežne: **McEliece** (varianty 8192128, 6688128, 460896 a ich modifikované verzie)

Kombinujú sa s klasickými algoritmami pre výmenu kľúčov. Bezpečnosť hybridu je zachovaná aj pri prelomení jednej z častí. Preferuje sa ML-KEM.

Samostatné použitie – digitálny podpis (integrita firmvéru / softvéru)

LMS [6]
XMSS [6]

Odporúča sa, keďže oba algoritmy sú založené na OTS (one-time signature) schéme, kde je možné privátny kľúč použiť len raz.

Samostatné použitie – digitálny podpis (všeobecné použitie)

ML-DSA-87 Level 5 [7]
SLH-DSA [8]

Hybridná kvantovo odolná kryptografia – digitálny podpis

Hybridný prístup je definovaný ako výber aspoň dvoch rôznych schém, z ktorých je jedna kvantovo odolná a druhá je klasická. Naviac sa odporúča použitie pred-zdieľaného kľúča ako jedného zo vstupov do funkcie na odvodenie kľúča.

ML-DSA / CRYSTALS-Dilithium [9] (varianty ML-DSA-87 a ML-DSA-65)
SLH-DSA / SPHINCS+ [10] (úrovne 3 a 5)
Predbežne: **FN-DSA / Falcon** [11] (varianty budú určené po štandardizácii)

Záver

Všetky odporúčania uvedené v tomto dokumente sú v súlade s aktuálnymi štandardmi NIST pre kvantovo odolnú kryptografiu (stav Round 3, NIST PQC Standardization).

Algoritmy **CRYSTALS-Kyber** (ML-KEM-1024 / Kyber-1024, ML-KEM-768 / Kyber-768), **CRYSTALS-Dilithium** (ML-DSA-87 / ML-DSA-65) a **SPHINCS+** (SLH-DSA, úrovne 3 a 5) sú štandardizované NIST a odporúčané pre produkčné použitie.

Algoritmy **FrodoKEM** a **McEliece** sú momentálne v procese štandardizácie a ešte nie sú oficiálne schválené NIST. Ich použitie je zatiaľ experimentálne.

Hybridné schémy kombinujú klasické a kvantovo odolné algoritmy, čím zabezpečujú zachovanie bezpečnosti aj pri prelomení jednej z častí.

Tento prístup umožňuje postupný prechod na kvantovo odolnú kryptografiu s ohľadom na aktuálne štandardy a bezpečnostné odporúčania NIST.

Algoritmy digitálneho odtlačku (hash funkcie)

SHA-2

SHA-384 [12]
SHA-512 [12]

SHA-3

SHA3-384 [13]
SHA3-512 [13]
SHAKE256 [13]

Ostatné

BLAKE2 [14] (s výstupom ≥ 384 bitov)

Odporúčanie:
Všetky schválené algoritmy digitálneho odtlačku funkcie by mali mať výstup aspoň 256 bitov, ale pre kvantovú odolnosť odporúčame dĺžku minimálne 384 bitov.
Funkcie s výstupom 384 bitov a viac sú považované za kvantovo odolné, zatiaľ čo tie s 256 bitmi alebo menej sú kvantovo zraniteľné.

Dôvod výberu:
BHT-algoritmus (Brassard, Høyer a Tapp - 1997) vychádzajúci z Groverovho algoritmu znižuje náročnosť hľadania kolízií hašovacích funkcií v porovnaní s klasickými algoritmami hľadajúcimi kolízie na báze narodeninového paradoxu. Za bezpečné voči útoku zmieneným kvantovým algoritmom dnes považujeme iba tie hašovacie funkcie, ktorých výstupy sú dlhé aspoň 384 bitov.
Ostatné algoritmy digitálneho odtlačku, napríklad SHA-256 alebo SHA3-256, sú pri kvantových útokoch menej bezpečné a preto sa neodporúčajú pre kritické aplikácie. Stačí nahradiť hašovacie funkcie s dĺžkou výstupu 256 bitov hašovacími funkciami s dĺžkou výstupu 384 bitov.

Algoritmy digitálneho odtlačku pre heslá

Argon2

Argon2 [15] s použitím variantu Argon2id a parametrami minimálne:

1) t = 1, m = 2^{21} (2 GiB RAM), p = 4

2) t = 3, m = 2^{16} (64 MiB RAM), p = 4 pre prostredia s obmedzenou pamäťou

scrypt

scrypt [16] s parametrami minimálne: N = 131072 (2^{17}), r = 8, p = 1

PBKDF2

PBKDF2 [17]

1) **HMAC-SHA-256** s počtom iterácií aspoň 600 000

2) **HMAC-SHA-512** s počtom iterácií aspoň 210 000

Upozornenie:

- Pre každé heslo musí byť použitá náhodne vygenerovaná soľ (salt) zvlášť.
- Dĺžka soli musí byť minimálne 128 bitov (16 B).
- Dĺžka výstupu (tagu) musí byť minimálne 256 bitov (32 B).

Odporúčanie:

- Parametre je vhodné voliť čo najvyššie, aké sú prakticky použiteľné pre danú aplikáciu.
- Odporúča sa uprednostniť Argon2 s vyššie uvedenými parametrami.

Kvantová odolnosť:

Všetky schválené algoritmy na ukladanie hesiel sú kvantovo odolné, pokiaľ sú kvantovo odolné symetrické šifry a algoritmy digitálneho odtlačku, ktoré v nich používajú.

Generovanie náhodných postupností

Ak pseudonáhodný generátor využíva niektoré náhodné procesy v zariadení, je potrebné aby vzorkovaná veličina nadobúdala hodnoty v dostatočne veľkom rozsahu. Generátory náhodných postupností bitov založené na softvéri musia vykonávať kryptografický postprocesing vygenerovaných náhodných postupností podľa odporúčaní NIST SP800-90 [18] [19] [20] alebo BSI AIS 20/31 [21].

Záver

Odporúčané kryptografické algoritmy poskytujú vysokú úroveň bezpečnosti pre ochranu informácií a dát a sú vybrané s ohľadom na aktuálne odporúčania NIST. Pre symetrické šifry sa odporúča používať moderné algoritmy s kľúčom minimálne 256 bitov, ako AES, Twofish alebo ChaCha20, a pre hašovacie funkcie SHA-2, SHA-3 či BLAKE2 s výstupom ≥384 bitov, aby bola zachovaná kvantová odolnosť. Klasické asymetrické algoritmy, ako RSA, DSA alebo ECDSA, nie sú vhodné pre budúce použitie, a preto sa odporúča prechod na štandardizované post kvantové algoritmy, ako ML-KEM, ML-DSA a SLH-DSA. Experimentálne algoritmy (FrodoKEM, McEliece) používať len v špecifických prípadoch kde nie je možné použiť schválené verzie. Hybridné schémy kombinujú klasické a kvantovo odolné algoritmy, čím zabezpečujú dodatočnú úroveň bezpečnosti kombináciou klasického overeného algoritmu a nového post kvantového prístupu. Implementácia všetkých odporúčaných riešení by mala vždy využívať overené knižnice a aktuálne bezpečnostné postupy.

Poznámka:

Zmena kryptografických algoritmov je časovo a technicky náročný proces, ktorý si vyžaduje dôkladné plánovanie, alokáciu dostatočných kapacít pre vývoj a testovanie, a po implementácii aj vykonanie penetračných testov na overenie bezpečnosti.

Pri vývoji aplikácií preto odporúčame vytvoriť takú softvérovú architektúru, ktorá umožňuje ľahkú výmenu kryptografického algoritmu. Takáto implementácia typicky:

- *umožňuje simultánne využívanie viacerých algoritmov pre potreby plynulého prechodu,*
- *ukladá spolu s kľúčovým materiálom, zašifrovanými údajmi či hashom aj typ použitého algoritmu,*
- *má modulárnu architektúru, ktorá umožňuje ľahko meniť zoznam podporovaných kryptografických algoritmov*

Pri dodávaní aplikácií odporúčame zdokumentovať všetky miesta, kde sa kryptografické algoritmy nachádzajú a ich typy. Odberateľom odporúčame vždy požadovať od dodávateľa takýto zoznam.

Odkazy

[1] FIPS 197-upd1 PDF: Advanced Encryption Standard (AES), NIST, 9. máj 2023

[2] ISO/IEC 18033-3:2010 Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers, ISO/IEC, 2010

[3] RFC 8439, ChaCha20 and Poly1305 for IETF Protocols, IETF, jún 2018

[4] 3GPP TS 35.216: Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 2: SNOW 3G specification, 3GPP, september 2006

[5] FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, NIST, august 2024

[6] SP 800-208, Recommendation for Stateful Hash-Based Signature Schemes, NIST, október 2020

[7] FIPS 204, Module-Lattice-Based Digital Signature Standard, NIST, august 2024

[8] FIPS 205, Stateless Hash-Based Digital Signature Standard, NIST, august 2024

[9] FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA), NIST, august 2024

[10] FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA), NIST, august 2024

[11] FIPS 206, Standard: Digital Signature Based on Structured Lattices, NIST, v príprave

[12] FIPS 180-4, Secure Hash Standard (SHS), NIST, august 2015

[13] FIPS 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, NIST, august 2015

[14] RFC 7693: The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC), IETF, november 2015

[15] RFC 9106, Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications, IETF, september 2021

[16] RFC 7914: The scrypt Password-Based Key Derivation Function, IETF, august 2016

[17] NIST SP 800-132: Recommendation for Password-Based Key Derivation: Part 1: Storage Applications, NIST, december 2010

[18] SP 800-90A Rev. 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, NIST, jún 2015

[19] SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation, NIST, január 2018

[20] SP 800-90C, Recommendation for Random Bit Generator (RBG) Constructions, NIST, júl 2024

[21] AIS 20 / AIS 31, Evaluation of random number generators, BSI, september 2011