NÚKIB

MINIMÁLNÍ POŽADAVKY NA KRYPTOGRAFICKÉ ALGORITMY

doporučení v oblasti kryptografické bezpečnosti

Verze 4.0, platná ke dni 5. 2. 2025

Obsah

Úvod

Podle § 26 písm. d) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „vyhláška o kybernetické bezpečnosti“) mají povinné osoby podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „zákon o kybernetické bezpečnosti“) povinnost zohlednit doporučení v oblasti kryptografických prostředků vydaná Národním úřadem pro kybernetickou a informační bezpečnost za účelem ochrany aktiv informačního a komunikačního systému. Tento dokument obsahuje zmíněná doporučení.

V případě dotazů právního charakteru se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky

Tel.: +420 541 110 777
E-mail: nckb@nukib.gov.cz

Dotazy, připomínky a podněty kryptologického charakteru můžete zasílat na e-mailovou adresu: kryptoalgoritmy@nukib.gov.cz

Upozornění:

Tento dokument obsahuje doporučení Národního úřadu pro kybernetickou a informační bezpečnost v oblasti kryptografické ochrany. Povinné osoby podle zákona o kybernetické bezpečnosti jsou na základě § 26 písm. d) vyhlášky o kybernetické bezpečnosti povinny tato doporučení zohlednit za účelem ochrany aktiv informačního a komunikačního systému.

Dokument může být měněn na základě aktuálních poznatků z oblasti kryptografické ochrany.

1 Doporučení v oblasti kryptografické bezpečnosti

Národní úřad pro kybernetickou a informační bezpečnost zde vydává seznam schválených kryptografických algoritmů (*Approved*, *Recommended*), u kterých je přesvědčen, že jsou bezpečné alespoň ve střednědobém horizontu.

Kvantově zranitelná kryptografie a příprava přechodu ke kvantově odolné kryptografii

U jednotlivých skupin algoritmů níže uvádíme, zda jsou zranitelné kvantovými algoritmy, nebo zda jsou vůči nim odolné. Důsledkem kvantové zranitelnosti schváleného algoritmu je potřeba ho v nepříliš vzdáleném horizontu nahradit vhodnou kvantově odolnou variantou.

Pro případ klasických asymetrických algoritmů (kapitola 3), proti kterým kvantová hrozba směřuje především, jsou tyto kvantově odolné varianty speciálně uvedeny v samostatné kapitole 4 tohoto dokumentu (postkvantová kryptografie).

Doporučení kryptografického charakteru k přípravě přechodu od kvantově zranitelné ke kvantově odolné kryptografii jsou uvedena a vysvětlena v příloze „Kvantová hrozba a kvantově odolná kryptografie“.

2 Symetrické algoritmy

a) Blokové šifry

1. Advanced Encryption Standard (AES) s délkou klíčů 128, 192 a 256 bitů
2. Twofish s délkou klíčů 128 až 256 bitů
3. Camellia s délkou klíčů 128, 192 a 256 bitů
4. Serpent s délkou klíčů 128, 192 a 256 bitů

b) Proudové šifry

1. SNOW 2.0, SNOW 3G s délkou klíčů 128 a 256 bitů
2. ChaCha20 s délkou klíče 256 bitů a se zatížením klíče[1] menším než 256 GB

Doporučujeme preferovat:

- Použití blokových šifer před proudovými.
- V případě blokových šifer: AES, Camellia a Serpent (v uvedeném pořadí).
- Délku klíče 256 bitů.

Kvantová zranitelnost a kvantová odolnost:

- Všechny šifry s délkami klíčů 128 bitů a 192 bitů jsou kvantově zranitelné.
- Všechny šifry s délkou klíče 256 bitů jsou kvantově odolné.

c) Módy autentizovaného šifrování

1. CCM
2. EAX
3. OCB1 a OCB3, doporučujeme preferovat OCB3 před OCB1
4. GCM s inicializačním vektorem dlouhým 96 bitů a s tagem dlouhým 128 bitů
5. ChaCha20 + Poly1305 se zatížením klíče menším než 256 GB
6. Složená schémata typu „Encrypt-then-MAC“

Upozornění:

- Schválené módy šifrování musí používat blokové šifry uvedené v kapitole 2 písm. a).
- Složená schémata typu „Encrypt-then-MAC“ musí k výpočtu MAC používat pouze módy pro ochranu integrity uvedené v kap. 2 písm. e) a k šifrování pouze módy šifrování uvedené v kap. 2 písm. d), nebo v případě šifrování disků i módy uvedené v kap. 2 písm. f). Zároveň tato schémata nesmí pro šifrování a pro výpočet MAC používat stejný klíč.
- Inicializační vektor musí být součástí vstupu pro výpočet MAC.
- Při použití módu GCM se pro daný klíč nesmí opakovat hodnota inicializačního vektoru. Nejpozději po 2^{32} hodnotách inicializačního vektoru musí dojít k výměně klíče.

[1] Zatížení klíče je maximální objem dat, který smí být zašifrován týmž klíčem.

d) Módy šifrování pro složená schémata typu „Encrypt-then-MAC“

1. CTR
2. OFB
3. CBC (rovněž CBC-CS)
4. CFB

Upozornění:

- Módy CBC a CFB musí být použity s náhodným, pro útočníka nepředpověditelným, inicializačním vektorem.
- Při použití módu OFB se pro daný klíč nesmí opakovat hodnota inicializačního vektoru.
- Při použití módu CTR se pro daný klíč nesmí opakovat hodnota čítače.
- Samostatné použití módů šifrování mimo schémata typu „Encrypt-then-MAC“ není schváleno.

e) Módy pro ochranu integrity (Message Authentication Code – MAC)

1. HMAC pouze s hašovací funkcí z kapitoly 5
2. CMAC
3. KMAC
4. GMAC s inicializačním vektorem dlouhým 96 bitů a s tagem dlouhým 128 bitů
5. EMAC[2]
6. UMAC[2]

Upozornění:

- Při použití módu GMAC se pro daný klíč nesmí opakovat hodnota inicializačního vektoru. Nejpozději po 2^{32} hodnotách inicializačního vektoru musí dojít k výměně klíče.
- Při použití módu UMAC se pro daný klíč nesmí opakovat hodnota inicializačního vektoru.
- U všech výše uvedených algoritmů musí být délka tagu alespoň 96 bitů, pokud není uvedeno jinak.

f) Módy pro šifrování disků

1. XTS – délka jednotky dat (sektoru) nesmí přesáhnout 2^{20} bloků šifry (v případě šifry se 128bitovým blokem je to zhruba 16 MB)
2. EME2

Kvantová odolnost: Všechny schválené módy symetrické kryptografie jsou kvantově odolné, pokud jsou kvantově odolné symetrické šifry a hašovací funkce, které jsou v nich použity.

[2] Algoritmy EMAC a UMAC jsou v praxi vzácné a do budoucna uvažujeme o jejich odebrání ze seznamu schválených algoritmů. Pokud je používáte, prosíme o sdělení této informace na adresu kryptoalgoritmy@nukib.gov.cz.

3 Klasické asymetrické algoritmy

a) Klasické algoritmy pro digitální podpis

1. Digital Signature Algorithm (DSA) s délkou klíčů 3072 bitů a více, s délkou parametru cyklické podgrupy 256 bitů a více
2. Elliptic Curve Digital Signature Algorithm (EC-DSA) s délkou klíčů 256 bitů a více
3. Rivest-Shamir-Adleman Probabilistic Signature Scheme[3] (RSA-PSS) s délkou klíčů 3072 bitů a více
4. Elliptic Curve Schnorr Signature Algorithm (EC-Schnorr) s délkou klíčů 256 bitů a více

Kvantová zranitelnost: Všechny schválené klasické algoritmy pro digitální podpis jsou kvantově zranitelné.

b) Klasické algoritmy pro ustanovení klíčů[4]

1. Diffie-Hellman (DH) s délkou klíčů 3072 bitů a více, s délkou parametru cyklické podgrupy 256 bitů a více
2. Elliptic Curve Diffie-Hellman (ECDH) s délkou klíčů 256 bitů a více
3. Elliptic Curve Integrated Encryption System – Key Encapsulation Mechanism (ECIES-KEM) s délkou klíčů 256 bitů a více
4. Provably Secure Elliptic Curve – Key Encapsulation Mechanism (PSEC-KEM) s délkou klíčů 256 bitů a více
5. Advanced Cryptographic Engine – Key Encapsulation Mechanism (ACE-KEM) s délkou klíčů 256 bitů a více
6. Rivest Shamir Adleman – Optimal Asymmetric Encryption Padding (RSA-OAEP) s délkou klíčů 3072 bitů a více
7. Rivest Shamir Adleman – Key Encapsulation Mechanism (RSA-KEM) s délkou klíčů 3072 bitů a více

Doporučení: U kryptografie na bázi eliptických křivek doporučujeme preferovat délku klíčů 384 a více bitů.

Kvantová zranitelnost: Všechny schválené klasické algoritmy pro ustanovení klíčů jsou kvantově zranitelné.

[3] Algoritmus RSA-PSS je někdy ekvivalentně označován RSASSA-PSS.

[4] „Ustanovení klíčů“ (*key establishment*) považujeme za nejobecnější pojem, který v sobě zahrnuje všechny metody, jakými mohou komunikující strany získat sdílený klíč, a spadají pod něj jak „dohoda na klíči“ (*key agreement*), tak „šifrování klíčů“ (*key wrapping*, *key encapsulation*).

4 Kvantově odolné asymetrické algoritmy (postkvantová kryptografie)

Přechod k náhradě kvantově zranitelné kryptografie bude mimořádně náročný. Proto doporučujeme se seznámit s podrobnějšími vysvětleními a doporučeními uvedenými v příloze „Kvantová hrozba a kvantově odolná kryptografie“.

a) Samostatný postkvantový algoritmus pro ustanovení klíčů

1. ML-KEM-1024

ML-KEM-1024 je standardizovaná verze algoritmu Kyber-1024 (též označovaného jako CRYSTALS-Kyber úrovně 5). Pro samostatné použití je nutná implementace dle standardu NIST (FIPS 203)[5].

b) Hybridní kvantově odolná kryptografie pro ustanovení klíčů

Kombinuje jeden z následujících postkvantových algoritmů KEM/Encryption:

1. ML-KEM-1024/Kyber-1024, ML-KEM-768/Kyber-768
2. FrodoKEM-1344, FrodoKEM-976
3. mceliece8192128, mceliece6688128, mceliece460896, mceliece8192128f, mceliece6688128f, mceliece460896f

s některým z klasických algoritmů pro ustanovení klíčů z kapitoly 3 písm. b), a to takovým způsobem, že bezpečnost hybridní kombinace zůstane zachována i v případě, kdy bude jedna z jejích složek prolomena.

Doporučení: V hybridní kombinaci je možné použít jak standardizovaný algoritmus ML-KEM, tak původní algoritmus Kyber. Nicméně doporučujeme preferovat ML-KEM a do budoucna předpokládáme schválení pouze této standardizované verze.

c) Samostatný postkvantový algoritmus digitálního podpisu pro ochranu integrity firmware a software

1. LMS
2. XMSS

Použití těchto algoritmů doporučujeme pouze pro ochranu integrity firmwaru a softwaru.

[5] https://csrc.nist.gov/pubs/fips/203/final

d) Samostatný postkvantový algoritmus digitálního podpisu pro obecné použití

1. ML-DSA-87
2. SLH-DSA

ML-DSA-87 je standardizovaná verze algoritmu CRYSTALS-Dilithium úrovně 5 (viz standard NIST FIPS 204)[6]. SLH-DSA je standardizovaná verze algoritmu SPHINCS+.

Upozornění: Pro samostatné použití algoritmu SLH-DSA schvalujeme bezpečnostní úrovně NIST 3 a 5 (viz standard NIST FIPS 205)[7].

e) Hybridní kvantově odolná kryptografie pro digitální podpis

Kombinuje jeden z následujících postkvantových algoritmů pro digitální podepisování:

1. ML-DSA/CRYSTALS-Dilithium
2. SLH-DSA/SPHINCS+
3. Falcon

s některým ze schválených klasických algoritmů pro digitální podpis z kapitoly 3 písm. a), a to takovým způsobem, že bezpečnost hybridní kombinace zůstane zachována i v případě, kdy bude jedna z jejích složek prolomena.

Upozornění: Pro ML-DSA v hybridní kombinaci schvalujeme varianty ML-DSA-87 a ML-DSA-65. Pro SLH-DSA v hybridní kombinaci schvalujeme bezpečnostní úrovně 3 a 5 dle standardu NIST FIPS 205[7]. Konkrétní varianty Falconu budou upřesněny v návaznosti na vývoj standardizace tohoto algoritmu.

[6] https://csrc.nist.gov/pubs/fips/204/final
[7] https://csrc.nist.gov/pubs/fips/205/final

5 Algoritmy hašovacích funkcí

a) Hašovací funkce SHA-2

1. SHA-256
2. SHA-384
3. SHA-512
4. SHA-512/256

b) Hašovací funkce SHA-3

1. SHA3-256
2. SHA3-384
3. SHA3-512
4. SHAKE128
5. SHAKE256

c) Ostatní hašovací funkce

1. Whirlpool
2. BLAKE2

Upozornění: Všechny schválené hašovací funkce musí mít délku výstupu alespoň 256 bitů. Doporučujeme však preferovat délku výstupu alespoň 384 bitů.

Kvantová zranitelnost a kvantová odolnost:

- Všechny schválené hašovací funkce s délkou výstupu 384 bitů nebo větší jsou kvantově odolné.
- Všechny schválené hašovací funkce s délkou výstupu 256 bitů nebo menší jsou kvantově zranitelné.

6 Algoritmy pro bezpečné ukládání hesel

1. Argon2 s volenou funkcí Argon2id a parametry alespoň
   i) t = 1, m = 2^{21} (2 GiB of RAM), p = 4
   ii) t = 3, m = 2^{16} (64 MiB of RAM), p = 4 pro prostředí s omezenou pamětí
2. scrypt s parametry alespoň N = 131072 (2^{17}), r = 8 a p = 1
3. PBKDF2
   i) HMAC-SHA-256 s počtem iterací alespoň 600 000
   ii) HMAC-SHA-512 s počtem iterací alespoň 210 000

Upozornění:

- Musí být použita sůl náhodně vygenerovaná pro každé heslo.
- Délka soli musí být alespoň 128 bitů (16B).
- Délka výstupu (tagu) musí být alespoň 256 bitů (32B).

Doporučení:

- Velikost parametrů je vhodné volit jako maximální možnou prakticky použitelnou pro danou aplikaci.
- Doporučujeme preferovat Argon2 s výše uvedenými parametry.

Kvantová odolnost: Všechny schválené algoritmy pro ukládání hesel jsou kvantově odolné, pokud jsou kvantově odolné symetrické šifry a hašovací funkce, které jsou v nich použity.

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
26. 11. 2018	1.0	Odbor bezpečnosti informačních a komunikačních technologií, NÚKIB	Vytvoření dokumentu
8. 6. 2022	2.0	Odbor bezpečnosti informačních a komunikačních technologií, NÚKIB	Revize dokumentu, algoritmy pro ukládání hesel
1. 7. 2023	3.0	Odbor bezpečnosti informačních a komunikačních technologií, NÚKIB	Revize dokumentu, kvantově odolná kryptografie, příloha
5. 2. 2025	4.0	Národní úřad pro kybernetickou a informační bezpečnost	Revize dokumentu a přílohy, postkvantové standardy NIST, KMAC, aktualizace parametrů u algoritmů pro ukládání hesel, odebrání dosluhujících algoritmů