NÚKIB

MINIMÁLNÍ POŽADAVKY NA KRYPTOGRAFICKÉ ALGORITMY

doporučení v oblasti kryptografické bezpečnosti

Verze 3.0, platná ke dni 1. 7. 2023

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.cz

Dotazy, připomínky a podněty kryptologického charakteru můžete zasílat na e-mailovou adresu: kryptoalgoritmy@nukib.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 vydává tato doporučení.

(1) Kategorie kryptografických algoritmů podle omezení doby své použitelnosti

Z hlediska doby použitelnosti rozlišujeme následující kategorie algoritmů:

Schválené kryptografické algoritmy (*Approved, Recommended, Future*) jsou algoritmy, u kterých jsme přesvědčeni, že jsou bezpečné alespoň ve střednědobém horizontu.

Kvantově odolná kryptografie s veřejnými klíči (*Quantum Safe Cryptography*) jsou kryptografické mechanismy s veřejnými klíči, u kterých jsme přesvědčeni, že budou v blízké budoucnosti vhodné k náhradě kvantově zranitelné kryptografie.

Dosluhující kryptografické algoritmy (*Legacy*) jsou algoritmy, u kterých doporučujeme přestat s jejich používáním do roku 2023. A dále doporučujeme nově zavádět pouze takové kryptografické systémy, které obsahují pouze schválené kryptografické algoritmy (a neobsahují dosluhující).

(2) 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 nutné ho v nepříliš vzdáleném časovém horizontu nahradit vhodnou kvantově odolnou kryptografií. Ta je stručně uvedena v kapitole 5 tohoto dokumentu.

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“.

(3) Symetrické algoritmy

a) Schválené blokové a proudové šifry

1. Advanced Encryption Standard (AES) s využitím délky klíčů 128, 192 a 256 bitů
2. Twofish s využitím délky klíčů 128 až 256 bitů
3. Camellia s využitím délky klíčů 128, 192 a 256 bitů
4. Serpent s využitím délky klíčů 128, 192 a 256 bitů
5. SNOW 2.0, SNOW 3G s využitím délky klíčů 128 a 256 bitů
6. ChaCha20 s délkou klíče 256 bitů a se zatížením klíče menším než 256 GB

Poznámka: Zatížení klíče je maximální objem dat, který smí být zašifrován týmž klíčem.

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.

b) Dosluhující blokové a proudové šifry

1. Triple Data Encryption Standard (3DES) s využitím délky klíčů 112 bitů, omezené použití jen se zatížením klíče menším než 10 MB, postupně přecházet na AES. Doporučeno použití jedinečného klíče pro každou zprávu.
2. Blowfish s využitím minimální délky klíčů 128 bitů, omezené použití jen se zatížením klíče menším než 10 GB.
3. Kasumi s využitím délky klíčů 128 bitů, omezené použití jen se zatížením klíče menším než 10 GB.

Kvantová zranitelnost: Všechny dosluhující šifry jsou kvantově zranitelné.

c) Schválené módy autentizovaného šifrování

1. CCM
2. EAX
3. OCB1 a OCB3, doporučujeme preferovat OCB3 před OCB1
4. GCM s noncí dlouhou 96 bitů a s tagem dlouhým 128 bitů, nejpozději po 2^{32} hodnotách nonce musí dojít k výměně klíče
5. ChaCha20 + Poly1305 se zatížením klíče menším než 256 GB
6. Složená schémata typu „Encrypt-then-MAC“

Poznámky:

- Schválené módy šifrování musí používat schválené blokové šifry.
- Schémata typu „Encrypt-then-MAC“ musí používat k šifrování pouze šifrovací módy uvedené v odstavci d) a k výpočtu MAC pouze schválené módy pro ochranu integrity.
- Inicializační vektor (nebo nonce) musí být součástí vstupu pro výpočet MAC.

d) Módy šifrování

Jejich samostatné použití je dosluhující, ale schválené je jejich použití ve složených schématech typu „*Encrypt-then-MAC*“.

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

Poznámky:

- Pro použití v rámci schváleného složeného schématu typu *Encrypt-then-MAC* musí tyto módy používat pouze schválené blokové šifry.
- 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.
- V případě použití CBC módu k šifrování bez ochrany integrity je třeba ověřit odolnost proti útoku na padding CBC módu.

e) Schválené 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

f) Schválené módy pro ochranu integrity

1. HMAC se schválenou hašovací funkcí
2. EMAC
3. CMAC
4. UMAC s délkou tagu 64 bitů

Kvantová odolnost: Všechny schválené módy symetrické kryptografie jsou kvantově odolné, pokud jsou použity s kvantově odolnou blokovou šifrou nebo kvantově odolnou hašovací funkcí.

g) Dosluhující módy pro ochranu integrity

1. HMAC-SHA1
2. CBC-MAC-X9.19, omezené použití jen se zatížením menším než 10^9 MAC

Kvantová zranitelnost a kvantová odolnost: Z uvažovaných módů je kvantově odolný pouze CBC-MAC-X9.19 za podmínky, že používá šifru s délkou klíče 256 bitů (šifry s délkou klíčů 128 bitů a 192 bitů jsou kvantově zranitelné).

(4) Klasické asymetrické algoritmy

a) Schválené klasické algoritmy pro technologii digitálního podpisu

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

Kvantová zranitelnost: Všechny schválené klasické algoritmy pro technologii digitálního podpisu jsou kvantově zranitelné.

b) Dosluhující klasické algoritmy pro technologii digitálního podpisu

1. Digital Signature Algorithm (DSA) s využitím délky klíčů 2048 bitů, délky parametru cyklické podgrupy 224 bitů
2. Elliptic Curve Digital Signature Algorithm (EC-DSA) s využitím délky klíčů 224 bitů
3. Rivest-Shamir-Adleman Probabilistic Signature Scheme (RSA-PSS) s využitím délky klíčů 2048 bitů
4. Elliptic Curve Schnorr Signature Algorithm (EC-Schnorr) s využitím délky klíče 224 bitů

Kvantová zranitelnost: Všechny dosluhující klasické algoritmy pro technologii digitálního podpisu jsou kvantově zranitelné.

c) Schválené klasické algoritmy pro procesy dohod na klíči a šifrování klíčů

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

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

Kvantová zranitelnost: Všechny schválené klasické algoritmy pro procesy dohod na klíči a šifrování klíčů jsou kvantově zranitelné.

d) Dosluhující klasické algoritmy pro procesy dohod na klíči a šifrování klíčů

1. Diffie-Hellman (DH) s využitím délky klíčů 2048 bitů, délky parametru cyklické podgrupy 224 bitů
2. Elliptic Curve Diffie-Hellman (ECDH) s využitím délky klíčů 224 bitů
3. Elliptic Curve Integrated Encryption System – Key Encapsulation Mechanism (ECIES-KEM) s využitím délky klíčů 224 bitů
4. Provably Secure Elliptic Curve – Key Encapsulation Mechanism (PSEC-KEM) s využitím délky klíčů 224 bitů
5. Advanced Cryptographic Engine – Key Encapsulation Mechanism (ACE-KEM) s využitím délky klíčů 224 bitů
6. Rivest Shamir Adleman – Optimal Asymmetric Encryption Padding (RSA-OAEP) s využitím délky klíčů 2048 bitů
7. Rivest Shamir Adleman – Key Encapsulation Mechanism (RSA-KEM) s využitím délky klíčů 2048 bitů

Kvantová zranitelnost: Všechny dosluhující algoritmy pro procesy dohod na klíči a šifrování klíčů jsou kvantově zranitelné.

(5) Kvantově odolná kryptografie s veřejnými klíči

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) Hybridní kvantově odolná kryptografie pro ustanovení klíčů

Kombinuje schválený klasický algoritmus pro dohody na klíči a ustanovení klíčů (odst. 2(4)c) s jedním z následujících post-kvantových algoritmů KEM/Encryption:

Kyber-1024, Kyber-k768, FrodoKEM-1344, FrodoKEM-976, mceliece8192128, mceliece6688128, mceliece460896, mceliece8192128f, mceliece6688128f, mceliece460896f.

Tyto hybridní kombinace klasické a post-kvantové kryptografie lze považovat za schválené.

b) Samostatný post-kvantový algoritmus pro ustanovení klíčů

CRYSTALS-Kyber úrovně 5 implementovaný dle standardu NIST.

Vzhledem k tomu, že standard NIST bude publikován až v roce 2024, není toto řešení zatím schváleno. K tomu dojde až pro implementace dle standardu NIST.

Poznámka: Kyber-1024 je jiný název pro CRYSTALS-Kyber úrovně 5.

c) Samostatný post-kvantový algoritmus digitálního podpisu pro ochranu integrity firmware a software

1. LMS
2. XMSS

Samostatné použití těchto algoritmů pro ochranu integrity firmware a software lze považovat za schválené.

d) Samostatný post-kvantový algoritmus digitálního podpisu s obecným použitím

CRYSTALS-Dilithium úrovně 5 implementovaný dle standardu NIST.

Vzhledem k tomu, že standard NIST bude publikován až v roce 2024, není toto řešení zatím schváleno. K tomu dojde až pro implementace dle standardu NIST.

Poznámka: Pro CRYSTALS-Dilithium úrovně 5 se též používá název Dilithium 5.

e) Hybridní kvantově odolná kryptografie pro technologii digitálního podpisu

Kombinuje schválený klasický algoritmus pro technologii digitálního podpisu (odst. 2(4)a) s některým z následujících post-kvantových algoritmů pro digitální podepisování: Dilithium,

SPHINCS+, Falcon. Jejich konkrétní varianty budou doporučeny v návaznosti na další průběh jejich standardizace.

(6) Algoritmy hašovacích funkcí

a) Schválené hašovací funkce SHA-2

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

b) Schválené hašovací funkce SHA-3

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

c) Ostatní schválené hašovací funkce

1. Whirlpool
2. BLAKE2

Doporučení:
U schválených hašovacích funkcí doporučujeme preferovat délku výstupu 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.

d) Dosluhující hašovací funkce

1. SHA-2 s délkou výstupu 224 bitů (SHA-224, SHA-512/224)
2. SHA3-224
3. RIPEMD-160

Kvantová zranitelnost: Všechny dosluhující hašovací funkce jsou kvantově zranitelné.

(7) Algoritmy pro bezpečné ukládání hesel

a) Schválené algoritmy

1. Argon2 s volenou funkcí Argon2id a parametry alespoň
   i) t=1, m=2^{21} (2 GiB of RAM)
   ii) t=3, m=2^{16} (64 MiB of RAM) pro prostředí s omezenou pamětí
2. Scrypt s parametry alespoň N=32768 (2^{15}), r=8, a p=1
3. PBKDF2 s počtem iterací alespoň 100 000 a schválenou hašovací funkcí SHA-2

Poznámky:

- 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.

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
26. 11. 2018	1.0	Odbor bezpečnosti informačních a komunikačních technologií	Vytvoření dokumentu
8. 6. 2022	2.0	Odbor bezpečnosti informačních a komunikačních technologií	Revize dokumentu, algoritmy pro ukládání hesel
1. 7. 2023	**3.0**	**Odbor bezpečnosti informačních a komunikačních technologií**	**Revize dokumentu, kvantově odolná kryptografie, příloha**