Minimální požadavky na kryptografické algoritmy

Ing. Bc. Martin Mikala
MONET+

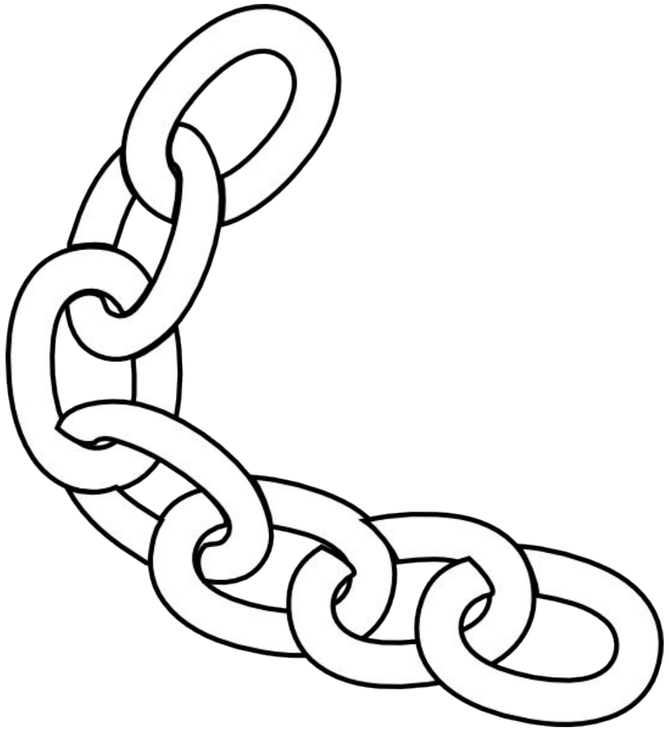
solutions by MONET +

Hlavní úkoly kryptografie

- důvěrnost (šifrování dat)
- integrita dat
- autenticita dat
- nepopiratelnost autorství

Správné použití kryptografie

- vhodný typ algoritmu
- bezpečný algoritmus
- správné parametry algoritmu
- bezchybná implementace
- korektní používání v praxi



Vhodný typ algoritmu

Typy algoritmů

- symetrický
- asymetrický
- hashovací

Příklad chybného použití

- ADOBE (2013)
- únik 10GB dat
- hesla šifrována místo hashování
  - 3DES(?) v **ECB** módu -> problém

Bezpečný algoritmus + parametry

Kryptografie se neustále vyvíjí

- objevování nových útoků
- zdokonalování starých útoků
- růst výpočetního výkonu
- dostupnost výpočetního výkonu

Nutné myslet na budoucí bezpečnost

- zašifrovaná data musí být bezpečná i například za 10 let

Hlídači bezpečných algoritmů

Nestátní organizace

- **NIST** (USA) - National Institute of Standards and Technology
  - kryptografické standardy (DES, AES, SHA-x, PQC)

- **ETSI** (EU) - European Telecommunications Standards Institute
  - např. algoritmy pro elektronické podpisy

- **IETF** - Internet Engineering Task Force
  - protokol TLS/SSL

Hlídači bezpečných algoritmů

Státní organizace

- **ANSSI** (FR) - Agence nationale de la sécurité des systèmes d'information
- **BSI** (GER) - Bundesamt für Sicherheit in der Informationstechnik
- **SK-CERT** (SK) - Slovak Computer Emergency Response Team

Národní úřad pro kybernetickou a informační bezpečnost

- příprava národních standardů, zákonů a podzákonných norem
- stanovení bezpečnostních standardů pro kritickou infrastrukturu
- osvěta a podpora vzdělání

- **Minimální požadavky na kryptografické algoritmy: doporučení kryptografické ochrany v oblasti kybernetické bezpečnosti**

NÚKIB

Minimální požadavky na kryptografické algoritmy

- verze 1.0 vydána 2018
- verze 2.0 vydána červen 2022

- seznam doporučených algoritmů
  - symetrické
  - asymetrické
  - hashovací
  - bezpečné ukládání hesel (ve verzi 2.0)

NÚKIB

MINIMÁLNÍ POŽADAVKY NA KRYPTOGRAFICKÉ ALGORITMY

doporučení kryptografické ochrany v oblasti kybernetické bezpečnosti

Minimální požadavky na kryptografické algoritmy

- schválené algoritmy
- dosluhující algoritmy (do roku 2023)
- nedoporučené algoritmy

Příklady doporučených algoritmů

Symetrické algoritmy

- Použití blokových šifer před proudovými
- Schválené obecně 128+ bitů, dosluhující 112 bitů
- Doporučená délka klíče 256 bitů

Skupiny algoritmů	Příklady algoritmu
Schválené	AES 128+ bitů
Dosluhující	3DES 112 bitů (do 10MB/klíč)
Nedoporučené	DES

Příklady doporučených algoritmů

Provozní módy blokových šifer

- Doporučení používat autentizované módy (s ochranou integrity), případně dosluhující módy v režimu Encrypt-then-MAC

Skupiny algoritmů	Příklady algoritmu
Schválené	CCM, GCM, OCB3
Dosluhující	CBC, CTR, OFB, CFB
Nedoporučené	ECB

Příklady doporučených algoritmů

Asymetrické algoritmy

- Algoritmy pro elektronické podpisy
- Algoritmy pro dohodu nad klíči a šifrování klíčů
- Řešena je hlavně délka klíčů

Skupiny algoritmů	Příklady algoritmu
Schválené	DSA, RSA, DH 3072+ bitů EC-... 256+ bitů
Dosluhující	DSA, RSA, DH 2048 bitů EC-... 224 bitů
Nedoporučené	DSA, RSA, DH 1024- bitů EC-... 192- bitů

Příklady doporučených algoritmů

Hashovací algoritmy

- Algoritmy SHA-2 nebo SHA-3
- Délka hashe 256+ bitů

Skupiny algoritmů	Příklady algoritmu
Schválené	SHA-256+ bitů SHA3-256+ bitů
Dosluhující	SHA-224 bitů SHA3-224 bitů
Nedoporučené	MD5 SHA-1

Příklady doporučených algoritmů

Algoritmy pro ukládání hesel

- Pouze schválené algoritmy
- Důraz na parametry algoritmů
- Náhodná unikátní sůl 128+ bitů
- Délka výstupu 256+ bitů

Skupiny algoritmů	Příklady algoritmu
Schválené	Argon2 Scrypt PbKDF2
Dosluhující	-
Nedoporučené	SHA-2 SHA-3 **3DES-ECB**

Nedoporučené algoritmy

"Nedoporučený" algoritmus nutně neznamená "nebezpečný"

- skupina algoritmů, kterým se doporučení nevěnuje (PQC)
- nedostatečně prozkoumané algoritmy
- algoritmy prolomené částečně
  - SHA1 × HMAC-SHA1
- algoritmy prolomené úplně

Bezchybná implementace

Postranní kanály

- Tajemství v paměti
- Časová analýza
- Odběrová analýza
- Útok zaváděním chyb

Příklad chybné implementace

- BEAST (2011)
  - protokol TLS/SSL
  - útok na bezpečný* mód CBC
  - útočník může prolomit utajení dat

Správné používání v praxi

Jednorázová tabulková šifra (OTP)

- úplně bezpečná, pokud je použita správně

- jednoduše prolomitelná v případě, že je použita špatně
    - two-time pad útok

Enigma

- na začátku zprávy 2× opakovaná třípísmenná zkratka (ABCABC)

Děkuji!

Potřebujete vyřešit kryptografii
ve vaší organizaci?

Kontaktujte nás.

www.proid.cz | info@proid.cz