Generátory pseudonáhodných čísel

Používané generátory, testování, proudové šifry

Generátory pseudonáhodných čísel

- Další generátory
- Testování generátorů
- Proudové šifry
- Slabiny
  - Pro kryptografii výhodné hardwarové generátory náhodných čísel

Blum, Blum and Shub

- Považován za bezpečný
- Parametry
  - N = p * q (p, q velká prvočísla, konguentní k 3 mod 4)
  - X0 = x2 mod N
- Xi = xi-12 mod N
- Xi = xi-1(2i)mod ((p-1)(q-1))
  - Není potřeba počítat postupně!
- Vhodné pro generování proudových šifer, ale pomalé!

Testování generátorů

- Potřeba testovat kvalitu generátorů

„Jak kvalitně se generovaná posloupnost čísel blíží náhodné?“

- Stanovena pravidla pro generování pseudonáhodných posloupností
- Sestavy statistických testů

Kritéria BSI

- Německý federální úřad pro informační bezpečnost
  - Kritéria kvality deterministických generátorů

- Kritéria
  - K1 - Nízká pravděpodobnost stejných úseků po sobě
  - K2 - Neodlišitelné statistickými testy od náhodné posloupnosti
  - K3 - Z žádné části nelze zjistit předchozí nebo následující znaky
  - K4 - Z vnitřního stavu generátoru (parametrů) nelze odvodit předchozí znaky ani stavy generátoru
    - K4 pro použití v kryptografii nutné!

Statistické testy

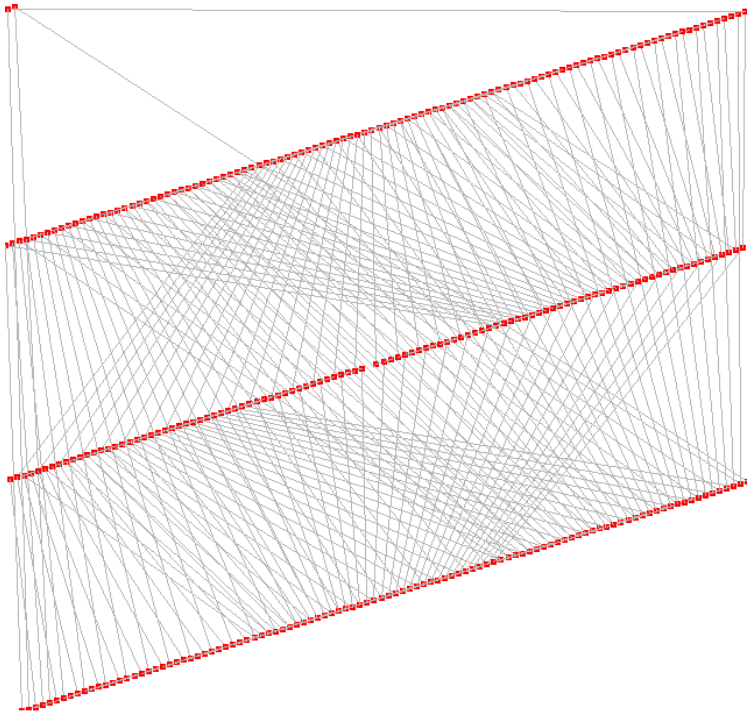
- Různé sestavy testů, empiricky potvrzena jejich vypovídací hodnota
- Testování hypotézy
  - Shoduje se vygenerovaná posloupnost s náhodným rovnoměrným rozdělením?
- BSI – 5 testů
- NIST – 16 testů

Statistické testy

- Frekvenční test (monobits)
  - Počet 0 a 1 v celé posloupnosti by měl být „stejný“
  - Počet 0 a 1 v části posloupnosti (M-bitů) by měl být M/2
- Runs test
  - Zjišťuje množství a délku posloupností samých 0 nebo 1
  - Porovnává s náhodnou posloupností
  - Možné porovnávat i v blocích délky M
- Poker test
  - Vyjádření posloupnosti jako celá čísla – rozdělení na pětice
  - Rozdělení na kategorie – počet stejných hodnot ve skupině?
  - Chi-kvadrát test shody s očekávanými hodnotami

Spektrální test

- Diskrétní fourierova transformace
  - Zjištění periodicity posloupnosti (opakované vzory blízko sebe)
  - Zaměřuje se na maximální hodnoty DFT



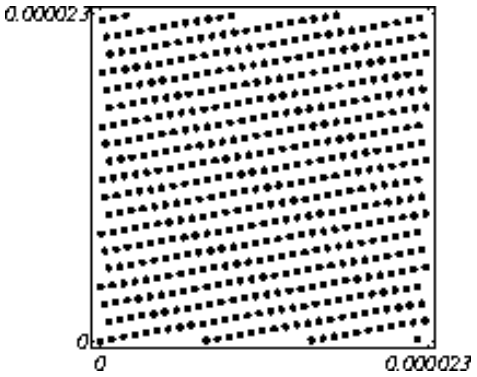
Lineární kongruenční g. n. č.

Spektrální test

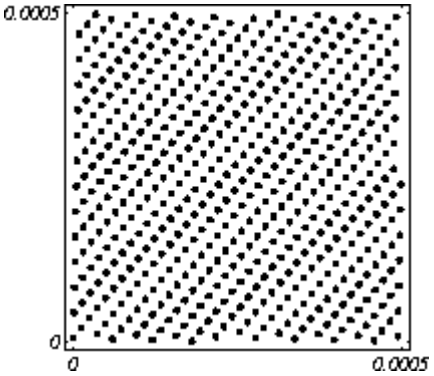
- LCG(m, a, b, y0)

$$y_{n+1} \equiv a y_n + b \ (mod\ m)$$

- Maple
  - LCG(1012-11, 427419669081, 0, 1)



- ANSI C rand() function
  - LCG(231, 1103515245, 12345, 12345)



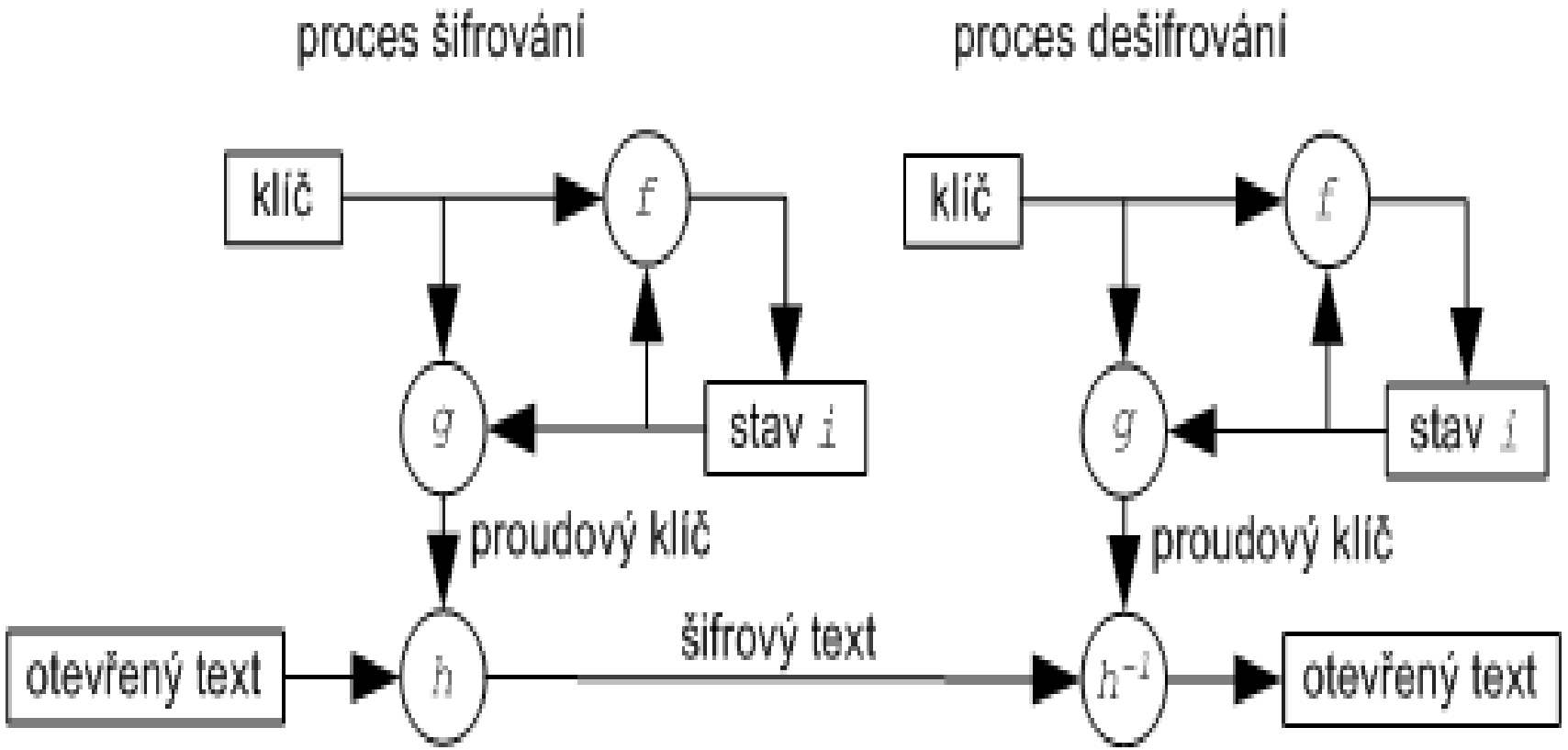
Proudové šifry

- Podobné Vernamově šifře
- Z klíče se pomocí posloupnosti pseudonáhodných čísel vygeneruje posloupnost klíčů
- Každým klíčem je zakódován pouze jeden znak

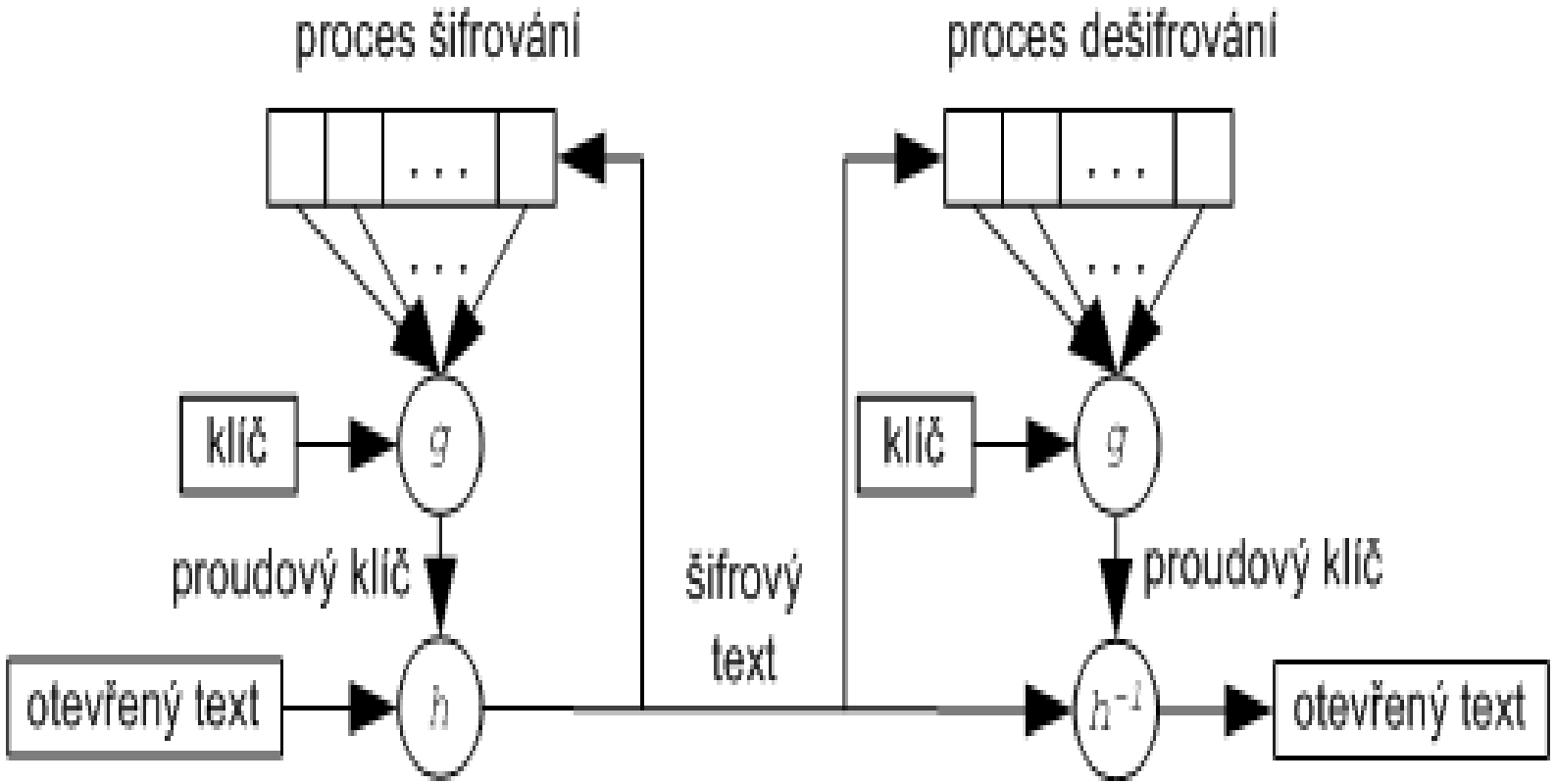
- Synchronní
  - Když je ztracen jeden bit, ztraceny i všechny ostatní

- Samo-synchronizační
  - Když je ztracen bit, ztraceno jen dalších n-bitů

Proudové šifry - synchronní



Proudové šifry - asynchronní



Slabiny generátorů a šifer

- Pro proudové šifry – znovupoužití klíče
  - E(A) = A xor C
  - E(B) = B xor C
- Windows 2000
  - Ze stavu generátoru lze odhadnout předchozí i následující stavy
  - Odhaleno 2007
- Debian OpenSSL
  - Změna v roce 2006 – podle překladače redundantní kód
  - Dramaticky snížilo entropii generovaných hodnot
  - Odhaleno 2008

GSM šifra A5

- Používá se pro spojení mezi telefonem a základovou stanicí (jinde nešifrováno)
- Klíč uložen na SIM kartě
- Verze A5/1
- A5/2
- A5/3 = KASUMI
  - Složitější šifra

GSM šifra A5/1

- Kvalitní ale slabá šifra už od začátku – krátké klíče
- Původně tajná

- Kombinace tří registrů o velikostech 19,22,23
  - Nepravidelné časování

- Triviální útok vyžaduje 240 výpočtů
  - Odhadnout první dva gen., poté vypočítat hodnotu třetího

- Výpočet tabulek klíčů – uskutečněn
  - Tabulka komprimovaná na velikosti 2TB v prosinci 2009

GSM šifra A5/3 = KASUMI

- Upravená šifra MISTY
  - Složitější šifra

- 128 bitový klíč rozdělený na 16 bloků
- Pro UMTS, GPRS a nové technologie

- 2010 nalezen algoritmus, který zvládne 1 dual-core PC během 2 h.

Použité zdroje

- Random numbers
  - http://www.mathworks.com/moler/random.pdf
- Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)
  - http://csrc.nist.gov/publications/nistpubs/800-90/SP800-90revised_March2007.pdf
- Tester generátorů pseudonáhodných čísel
  - http://tomasolivka.wz.cz/files/Generator_Tester.pdf
- NIST statistické testy
  - http://csrc.nist.gov/groups/ST/toolkit/rng/stats_tests.html

Použité zdroje

- Využití proudových šifer v současnosti
  - http://access.feld.cvut.cz/view.php?cisloclanku=2009080001
- Differential Cryptanalysis in Stream Ciphers
  - http://eprint.iacr.org/2007/218.pdf
- Cryptanalysis of the Random Number Generator of the Windows Operating Systém
  - http://eprint.iacr.org/2007/419.pdf
- Debial OpenSSL bug
  - http://digitaloffense.net/tools/debian-openssl/

Použité zdroje

- Intercepting GSM traffic
  - http://www.blackhat.com/presentations/bh-europe-08/Steve-DHulton/Whitepaper/bh-eu-08-steve-dhulton-WP.pdf
- Subverting the security base of GSM
  - https://har2009.org/program/attachments/119_GSM.A51.Cracking.Nohl.pdf
- A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony
  - http://eprint.iacr.org/2010/013.pdf