Hašovací funkce - nejaktuálnější téma kryptologie

Jiří Hörner, Václav Rozhoň, Martin Vančura

Gymnázium Pelhřimov & Gymnázium Jana Valeriána Jirsíka ČB

21. června 2012

Program

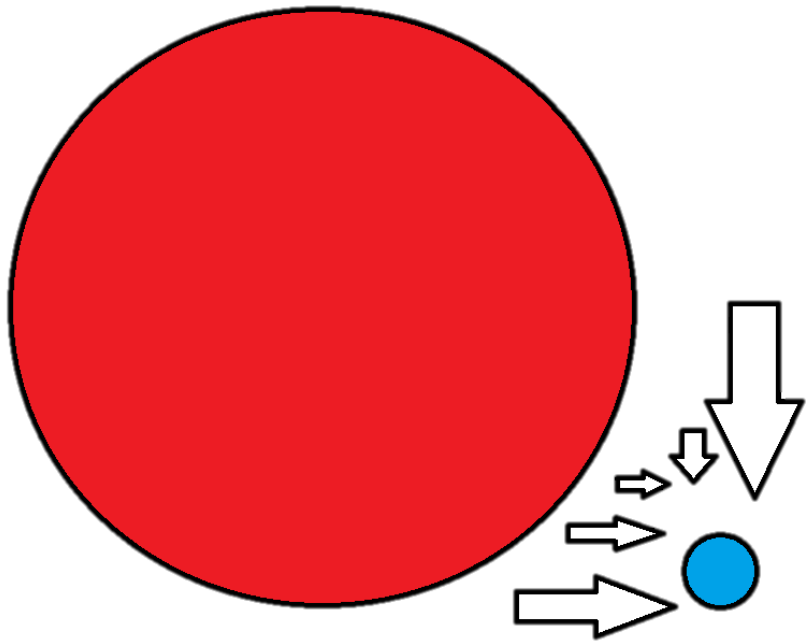
1. Hašovací funkce
2. Využití hašovacích funkcí
3. Nový standard SHA-3

Program

1. Hašovací funkce
2. Využití hašovacích funkcí
3. Nový standard SHA-3

Definice hašovací funkce

- na hašovací funkce jsou kladeny 4 základní požadavky:
  - jednocestnost
  - bezkoliznost
  - odolnost vůči hledání druhého vzoru
  - náhodné orákulum



Narozeninový paradox

Kolik hostů musí být na párty, aby s pravděpodobností 50%

- měli 2 z nich narozeniny ve stejný den?

Narozeninový paradox

Kolik hostů musí být na párty, aby s pravděpodobností 50%

- měli 2 z nich narozeniny ve stejný den?

  odpověď: 23 hostů

- měl někdo jiný narozeniny ve stejný den jako já?

Narozeninový paradox

Kolik hostů musí být na párty, aby s pravděpodobností 50%

- měli 2 z nich narozeniny ve stejný den?

  odpověď: 23 hostů

- měl někdo jiný narozeniny ve stejný den jako já?

Narozeninový paradox

Kolik hostů musí být na párty, aby s pravděpodobností 50%

- měli 2 z nich narozeniny ve stejný den?

  odpověď: 23 hostů

- měl někdo jiný narozeniny ve stejný den jako já?

  odpověď: 257 hostů

Narozeninový paradox

Kolik hostů musí být na párty, aby s pravděpodobností 50%

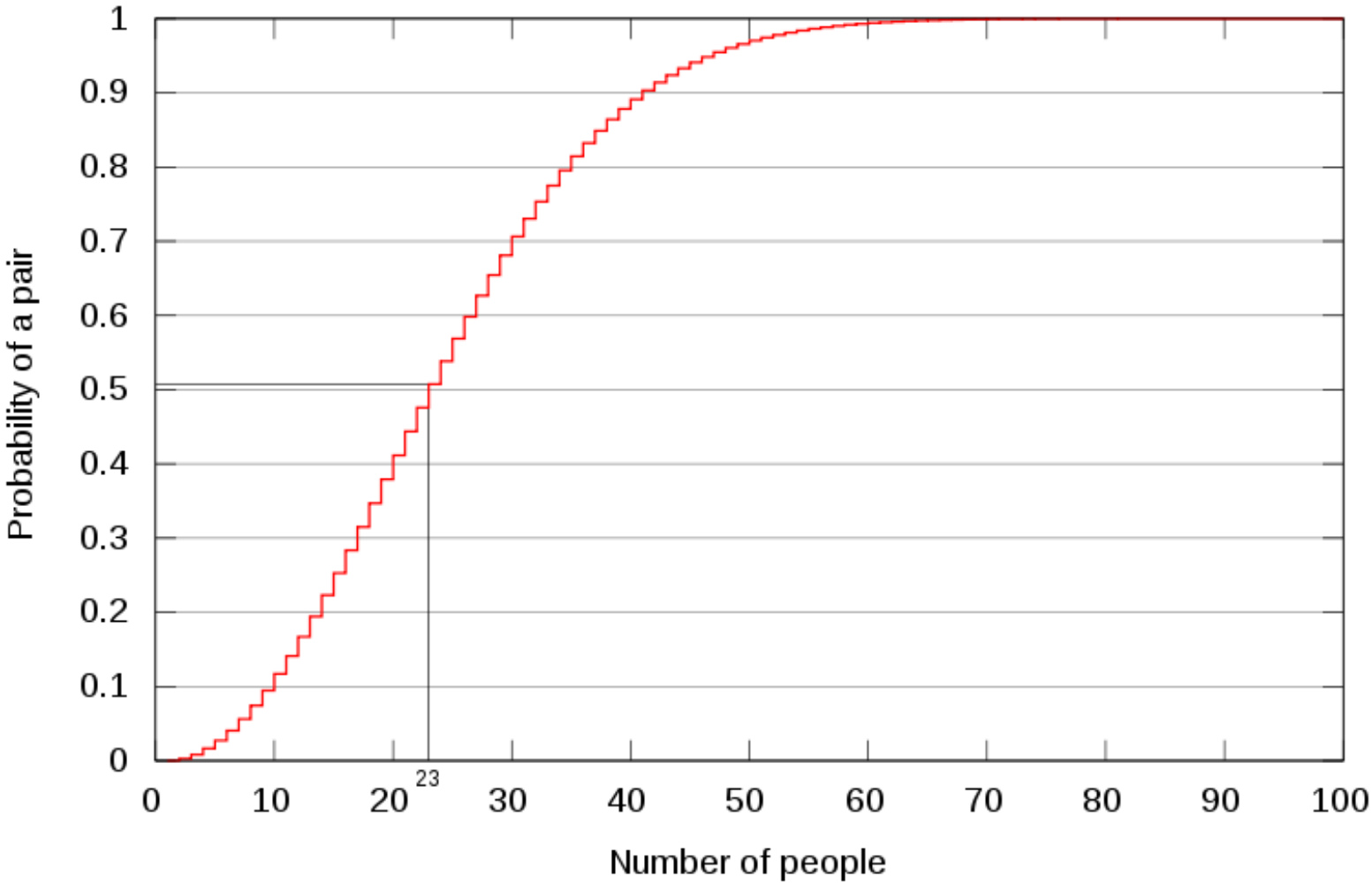
- měli 2 z nich narozeniny ve stejný den?

  odpověď: 23 hostů

- měl někdo jiný narozeniny ve stejný den jako já?

  odpověď: 257 hostů

Narozeninový paradox



Prolomení hašovací funkce

- funkce je prolomená, pokud lze jednoduše hledat:
  - kolize
  - druhé vzory
- pokud dojde k prolomení hašovací funkce, lze ji ještě využít na jiné aplikace

****

CONTRACT
At the price of **$176,495** Alf Blowfish
sells his house to Ann Bonidea ...

****

CONTRACT
At the price of **$276,495** Alf Blowfish
sells his house to Ann Bonidea ...

- H. Dobbertin – metoda nalézání kolizí u algoritmu MD4 (1996)
- teoretická možnost podstrčení falešného dokumentu (stejný haš)

Program

1 Hašovací funkce

2 Využití hašovacích funkcí

3 Nový standard SHA-3

Ukládání přihlašovacích hesel

- místo hesel se ukládají jejich haše
- přihlašování do systému = výpočet haše a jeho porovnání s uloženým
- haše neodhalují hesla, z nichž jsou vypočteny

Autentizace

- hašováním zpracovává nejen zprávu M, ale i tajný klíč K
- průkaz znalosti při autentizaci entit
- značení HMAC-SHA-1(M,K)

Kontrola integrity

- neporušenost zprávy lze kontrolovat neporušeností jejího hašovacího kódu
- CRC (*Cyclic redundancy check*)
- kontrolní součet

Program

1 Hašovací funkce

2 Využití hašovacích funkcí

3 Nový standard SHA-3

Nový standard SHA-3

- 2005 - nalezení trhlin v hašovacím standardu SHA-1
- nový standard SHA-2 je příliš pomalý
- 2007 - vyhlášena soutěž o novou hašovací funkci $\Rightarrow$ SHA-3
- dva programy s českými spoluautory

EDON-R

- jeden z nejrychlejších hašovacích algoritmů
- spoluautoři Vlastimil Klíma, Aleš Drápal
- bylo zjištěno, že není zaručena jednocestnost $\Rightarrow$ nedostala se do užšího výběru

BMW

- Blue Midnight Wish (dříve Blue Wish)
- velice rychlý
- spoluautorem Vlastimil Klíma
- dostala se do užšího výběru 14 algoritmů

Další výběr

- prosinec 2010 - výběr pěti finalistů
- spekulace o objektivitě
- prosinec 2012 - vyhlášení vítěze

64 bitový procesor, 256 bitový hašový kód, rychlost v cyklech/byte		
1	Blue Midnight Wish	7.55
2	Skein	7.6
3	Shabal	8.03
4	BLAKE	8.19
5	Keccak	10
6	CubeHash	11
7	SIMD	11
8	Luffa	13.4
9	SHA-256	15.34
10	JH	16.8
11	Grøstl	22.2
12	Hamsi	25
13	SHAvite-3	26.7
14	Fugue	28
15	ECHO	28.5

64 bitový procesor, 512 bitový hašový kód, rychlost v cyklech/byte		
1	Blue Midnight Wish	3.88
2	Skein	6.1
3	Shabal	8.03
4	BLAKE	9.29
5	CubeHash	11
6	SIMD	12
7	SHA-512	12.59
8	JH	16.8
9	Keccak	20
10	Luffa	23.2
11	Hamsi	25
12	Grøstl	30.5
13	SHAvite-3	38.2
14	ECHO	53.5
15	Fugue	56