

Funkcje skrótu

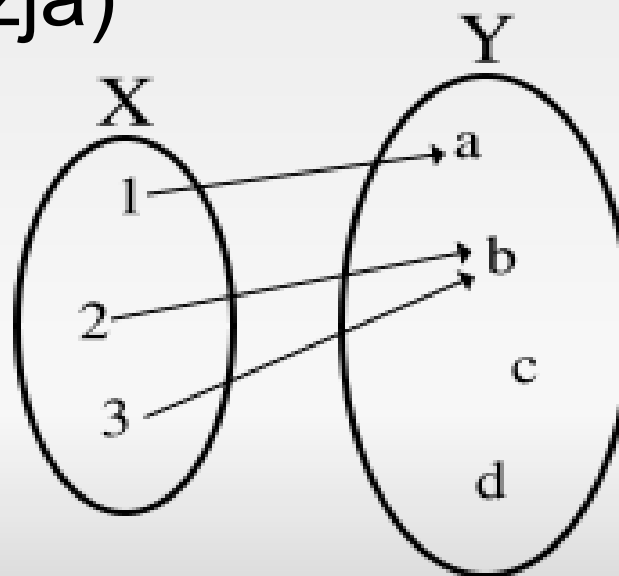
Marcin Łepicki
Politechnika Białostocka
Ochrona baz danych
Prowadząca zajęcia:
dr inż. Eugenia Busłowska

Funkcje skrótu

- Wiele nazw: funkcja skrótu, jednokierunkowa funkcja mieszająca, funkcja haszująca
- Przyporządkowuje dowolnej porcji danych krótką wiadomość o zazwyczaj stałym rozmiarze
- Ich podgrupą są kryptograficzne funkcje skrótu, mające szerokie zastosowanie w informatyce
- Nazwa "hash" wzięła się od "rozdrabniania i miksowania" i datowana jest na 1953 rok²

Funkcje skrótu

- X – zbiór możliwych wiadomości, dowolnej długości
- Y – zbiór wartości funkcji skrótu
- Może się zdażyć sytuacja, w której 2 wiadomościom przyporządkowany jest jednakowy skrót (kolizja)



Grafika za:

http://pl.wikipedia.org/wiki/Grafika:Function_illustration.svg

Kryptograficzne funkcje skrótu

- Nie istnieje dokładna definicja, ale istnieją pewne cechy, które powinna spełniać dobra kryptograficzna funkcja skrótu
 - Mając dany skrót h powinno być niemożliwym znalezienie wiadomości m takiej, że $\text{hash}(m)=h$
 - Mając daną wiadomość m_1 powinno być niemożliwym znalezienie wiadomości m_2 takiej, że $\text{hash}(m_1) = \text{hash}(m_2)$ ¹

Kryptograficzne funkcje skrótu

- Bardzo zależy nam również, by:
 - Obliczenie skrótu było proste, ale odtworzenie wiadomości lub jakichkolwiek ich cech na podstawie skrótu niemożliwe.
 - Prawdopodobieństwo, że dwie różne wiadomości będą miały ten sam skrót jest zależne wyłącznie od długości skrótu. (...) obecnie przyjmuje się od 128 do 160 bitów, co daje w przybliżeniu $3,4E+38$ do $1,46E+48$ możliwych kombinacji³

Kryptograficzne funkcje skrótu

- Tak naprawdę każdy bezpieczny algorytm szyfrujący można łatwo zmienić w bezpieczną funkcję mieszającą.
- Tworzy to jednak powolne i zbyt skomplikowane narzędzia do generowania skrótów, co bywa niepraktyczne w typowych przypadkach.
- Alternatywnie tworzone są szybkie algorytmy przetwarzające dane tak, by złożoność zależności między wejściem a wyjściem ukrywała cechy wiadomości.³

Przykłady funkcji skrót

- Wiele banalnych algorytmów, jak część danych, zliczanie bitów o danej wartości, proste operacje logiczne na danych itd.
- Popularne kryptograficzne funkcje skrótów
 - Rodzina funkcji MD (MD2, MD4, MD5)
 - Rodzina funkcji SHA (SHA-0, SHA-1, SHA-2)
 - HAVAL, WHIRLPOOL, TIGERi inne

Zastosowanie

- Tablice mieszające
- Wyznaczanie odcisków (fingerprint) wiadomości (m.in. w podpisie cyfrowym)
- Zachowywanie haseł
- Sprawdzanie spójności danych
- Protokół p2p
- Poprawianie danych generowanych przez generatory liczb pseudolosowych

Funkcja MD5

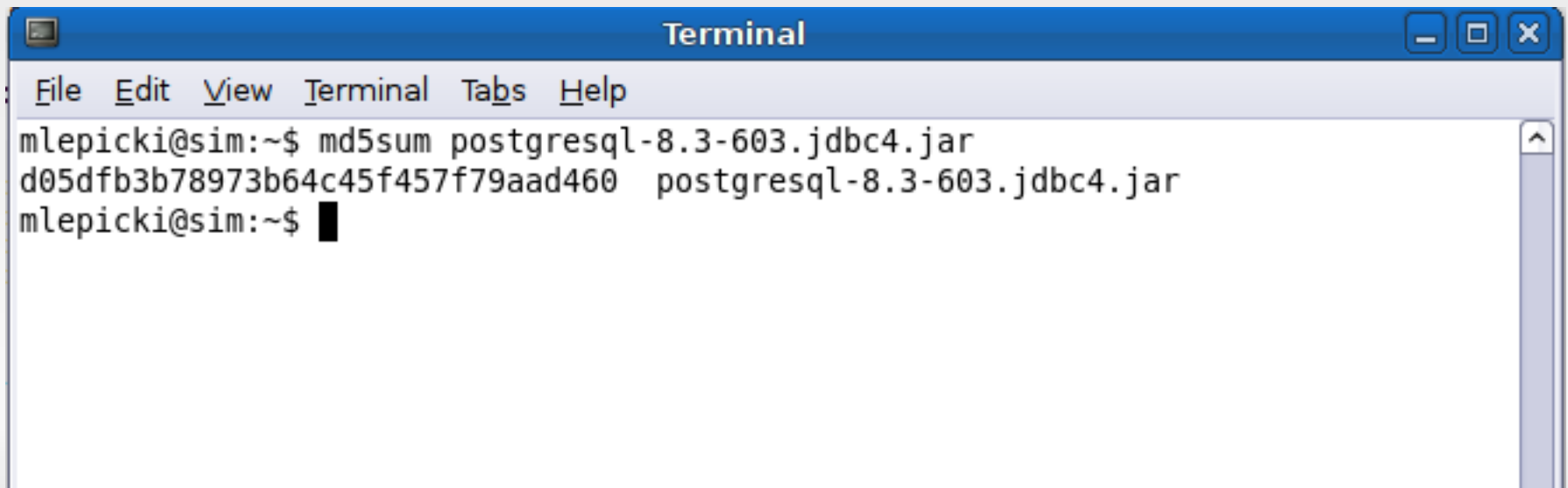
- Algorytm został opracowany przez Ronalda Rivesta. Od 2004 roku nie jest uznawana za bezpieczną, bowiem zespół chińskich badaczy z uniwersytetu Shandong znalazł sposób generowania kolidujących danych.
- Pomimo tego powszechnie używana
- Na podstawie danych generuje ciąg o długości 128-bitów

Funkcja MD5

- Działanie algorytmu (za wikipedią):
 - Doklejamy do wiadomości wejściowej bit o wartości 1
 - Doklejamy tyle zer ile trzeba żeby ciąg składał się z 512-bitowych bloków, i ostatniego niepełnego - 448-bitowego
 - Doklejamy 64-bitowy (zaczynając od najmniej znaczącego bitu) licznik oznaczający rozmiar wiadomości. W ten sposób otrzymujemy wiadomość złożoną z 512-bitowych fragmentów.
 - Ustawiamy stan początkowy na 0123456789abcdeffedcba9876543210
 - Uruchamiamy na każdym bloku (jest przynajmniej jeden blok nawet dla pustego wejścia) funkcję zmieniającą stan
 - Po przetworzeniu ostatniego bloku zwracamy stan jako obliczony skrót wiadomość
 - Funkcja zmieniająca stan wykonuje na blokach danych głównie operacje bitowe, wyznaczając sumę, iloczyn, negację, sumę wykluczającą.¹

Funkcja MD5

- Przykład: program md5sum
 - Ściągamy plik postgresql-8.3-603.jdbc4.jar, w internecie podany jest hasz wiadomości d05dfb3b78973b64c45f457f79aad460
 - Po ściągnięciu sprawdzamy plik:

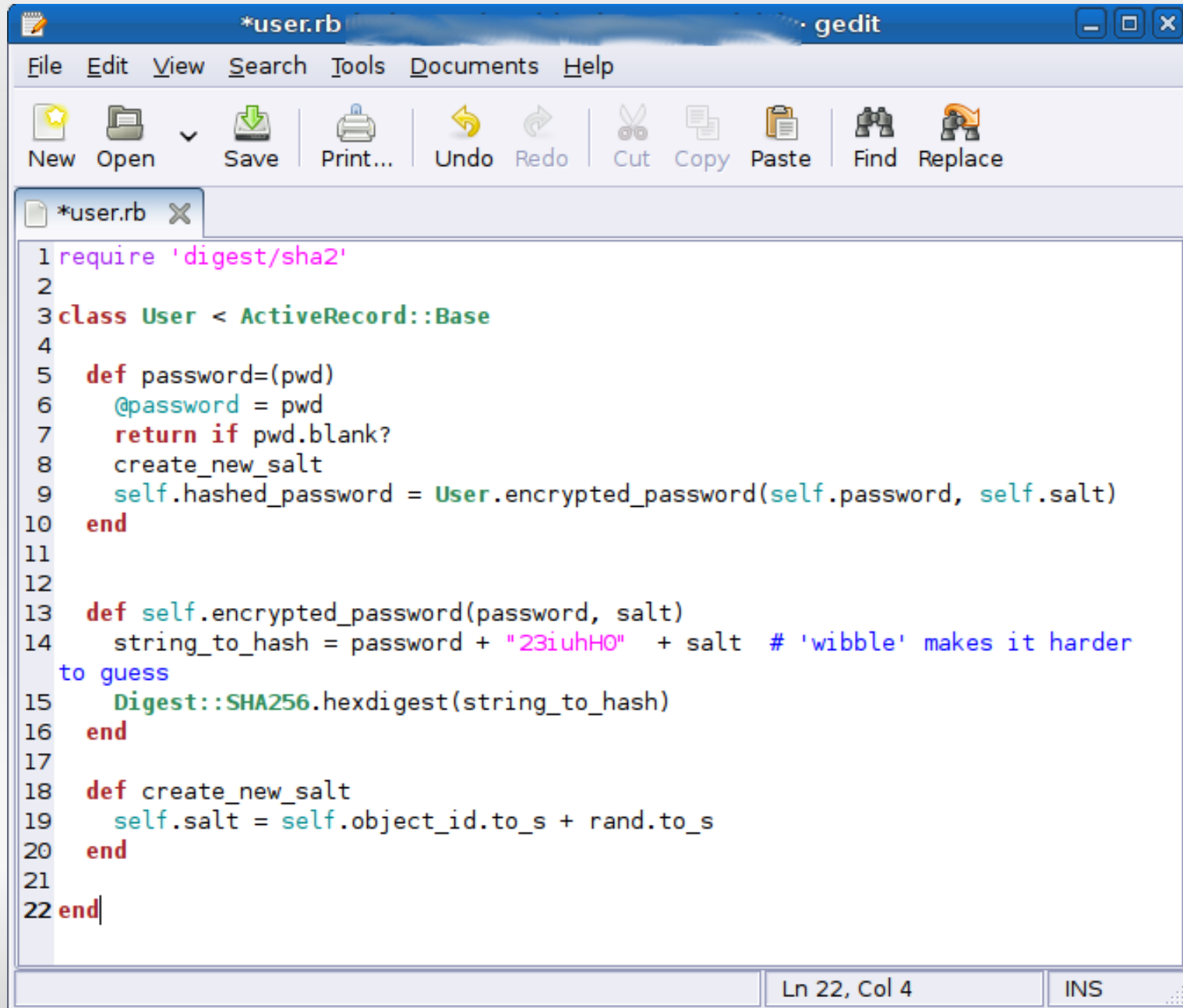


```
Terminal
File Edit View Terminal Tabs Help
mlepicki@sim:~$ md5sum postgresql-8.3-603.jdbc4.jar
d05dfb3b78973b64c45f457f79aad460 postgresql-8.3-603.jdbc4.jar
mlepicki@sim:~$ █
```

Funkcje z rodziny SHA

- Secure Hash Algorithm – rodzina funkcji zaprojektowanych przez NSA (National Security Agency)
- SHA-0 został wycofany ze względu na (nieujawnione) dane, NSA przestanie używać SHA-1 w roku 2010, zastępując go różnymi wariantami SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512)
- SHA-0 i SHA-1 generują klucz długości 160 bitów

Funkcje z rodziny SHA - przykład



```
1 require 'digest/sha2'
2
3 class User < ActiveRecord::Base
4
5   def password=(pwd)
6     @password = pwd
7     return if pwd.blank?
8     create_new_salt
9     self.hashed_password = User.encrypted_password(self.password, self.salt)
10  end
11
12
13  def self.encrypted_password(password, salt)
14    string_to_hash = password + "23iuhH0" + salt # 'wibble' makes it harder
to guess
15    Digest::SHA256.hexdigest(string_to_hash)
16  end
17
18  def create_new_salt
19    self.salt = self.object_id.to_s + rand.to_s
20  end
21
22 end
```

Ln 22, Col 4 INS

Bibliografia

1. Polska wikipedia: [Funkcja skrótu](#), [MD5](#), [SHA-1](#)
2. Angielska wikipedia: [Hash function](#), [Cryptographic hash function](#)
3. Michał Zalewski, "Cisza w sieci", wydawnictwo Helios 2005
4. Cormen T. H., Leiserson C. E., Rivest R. L., "Wprowadzenie do algorytmów", WNT 2001