Тема №4: Описание на хеш функция

Факултет "Артилерия, ПВО и КИС"



Изготвил: Явор Стоянов Ботов

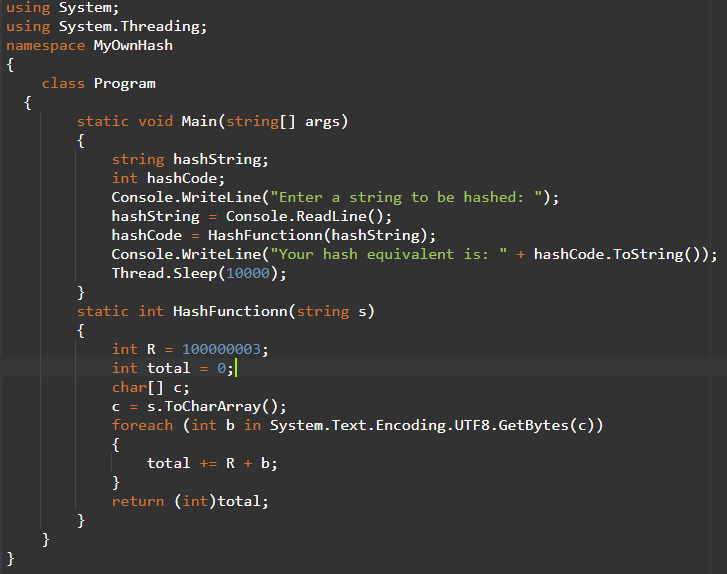
Факултетен Номер: 1187632

Пълно описание на темата:

Като познавате принципите на построение на хеш функциите, предложете свой собствен вариант на хеш функция. Обосновете характеристиките й. Посочете предимствата й. Представете код и изпълним файл на хеш функцията и тестови резултати.

Програма и използван език: Visual studio & C#

Изпълним код:



Характеристики:

За всеки елемент E който искам да хеширам, се изчислява коефициентът (R+b);  
Използва ASCII таблица, всеки символ ползва елементи от таблицата;  
Използва пермутации (колкото по голям е низа за хеширане, варианта за пермутация се увеличава, единственото ограничение е в integer размера от – до 0 и от 0 до + (int32));  
32-битов хеш защото генерираното число е integer. В програмирането int=32bit;

Предимства:  
Задейства се еднопосочно;  
(R+ b) гарантира, че всички фактори са нечетни;  
Избягва се резултата от хеширането да стане 0;

Недостатъци:   
Големината на хеш-а;  
Не приема “null” като стойност за ключа( null: не е стойност, нито е “unique”);  
Няколко различни input-а могат да генерират един и същ output;

Алгоритъм:

Дефинираме входяща стойност “Total”, която ще бъде нашата цел за хеширане.

Всеки един знак от входящият стринг представлява променлива “b”, а големината на стринга е съвкупност от всички “b“-та. За всяка една променлива “b”се взима числената й стойност от ASCII таблицата. Това гарантира уникалност на всеки един от знаците в стринга (независимо дали е числен или не).   
Дефинираме константна стойност “R”, която представлява 10 цифрено число, след което на всяка една итерация алгоритъмът придобива следният вид:

Total += R + b

Стойността на R гарантира, че изходният код ще бъде винаги число в диапазона -2,147,483,648 до 2,147,483,647.( Integral numeric types (C# reference)).

При изчисление на хеш функцията това би изглеждало по този начин:

Total =(R +b)+(R+b)+ (R +b)+(R+b)+….

В зависимост от големината на входящия стринг се определя и дължината на хеширащото уравнение. Пример:

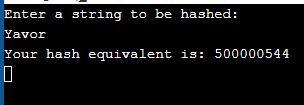
Входящ стринг: Yavor

|  |  |  |
| --- | --- | --- |
| **b** | ASCII | R = 100000003; (R+b) |
| Y | 89 | 100 000 092 |
| a | 97 | 100 000 100 |
| v | 118 | 100 000 121 |
| o | 111 | 100 000 114 |
| r | 114 | 100 000 117 |

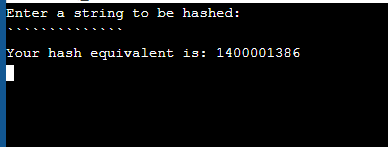
Total = 500 000 544

Изходният хеш представлява 32 битово кодирано число.То е еднопосочно. Може да се ползва навсякъде където се налага хеширането на чувствителна ифнормация.

Пример с входящи и изходящи данни:



Фигура 1 5 елемента



Фигура 2 14 елемента

Сравнения:

С MD5 – заради линейната векторна идентичност на генерираните хешове с MD5 не е за предпочитане той да се ползва за записване на чувствителна информация в база данни. Принципа на генериране на примерния хеш който предлагам аз има ниско ниво на колизия заради големият диапазон от възможности на крайния изходен код. От друга страна минус на този тип решение е лесната проследяемост на алгоритъма което би довело до бързо разпознаване на принципа на действие. Това е ниско ниво на хеширане тъй като работи само с числени стойности.