FNV Hash Function

draft-eastlake-fnv-18.txt

Glenn Fowler, Landon Curt Noll, Kiem-Phong Vo,
Donald Eastlake <d3e3e3@gmail.com>, Tony Hansen
FNV: Fowler, Noll, Vo – Hash Function

• FNV is a widely used, simple, non-cryptographic hash function with good dispersion.

• Purpose of this document:
  • To lead to a stable, permanent FNV reference document in the form of an RFC.
  • To provide FNV reference code.

• NOT the purpose of this document:
  • To list lots of hash functions.
  • To select the “best” hash function.
FNV: Fowler, Noll, Vo – Hash Function

• FNV-1a Pseudo-code:
  • hash = offset_basis
    for each octet_of_data to be hashed
      hash = hash xor octet_of_data
      hash = hash * FNV_Prime
    return hash

• Values of FNV_Prime and default values of offset_basis are specified for hash lengths of 32, 64, 128, 256, 512, and 1024 bits.
FNV: Fowler, Noll, Vo – Hash Function

• The FNV_Prime for a 2**s bit FNV hash is defined as:
  • When s is an integer and 4 < s < 11, then FNV_Prime is the smallest prime p of the form:
    • 256**int((5 + 2**s)/12) + 2**8 + b
  • where b is an integer such that:
    • 0 < b < 2**8
    • The number of one-bits in b is 4 or 5
    • and where ( p mod (2**40 - 2**24 - 1) ) > (2**24 + 2**8 + 2**7).
  • An FNV_Prime will have only 6 or 7 one bits in its binary representation.
FNV: Fowler, Noll, Vo – Hash Function

• Example FNV_Primes:
  • 32-bit: 0x01000193
  • 64-bit: 0x000001000000001B3

• If a hash function of a different number of bits k < 1024 is required, xor folding is recommended:
  • Assume FNV_S is the smallest FNV hash larger than k.
  • \( \text{temp} = \text{FNV}_S \) (input data)
  • \( k\)-bit-hash = (temp xor temp\( \gg k \)) & (2**k – 1)
FNV: Fowler, Noll, Vo – Hash Function

• Widely used:
  • IEEE Std 802.1Qbp-2014
  • RFC 7357 and RFC 7873
  • Used in DNS servers, the Twitter service, database indexing hashes, major web search / indexing engines, netnews history file Message-ID lookup functions, anti-spam filters, a spellchecker programmed in Ada 95, flatalsembler's open source x86 assembler - user-defined symbol hashtree, non-cryptographic file fingerprints, computing Unique IDs in DASM (DTN (Delay Tolerant Networking) Applications for Symbian Mobile-phones), Microsoft's hash_map implementation for VC++ 2005, the realpath cache in PHP 5.x (php-5.2.3/TSRM/tsrm_virtual_cwd.c), and many other uses.

• Has a good web site but no stable document
  • http://isthe.com/chongo/tech/comp/fnv/index.html
Next Step(s)

- Suggest that SECDISPATCH recommend AD Sponsored
End

draft-eastlake-fnv-18.txt

Glenn Fowler, Landon Curt Noll, Kiem-Phong Vo, Donald Eastlake <d3e3e3@gmail.com>, Tony Hansen