## Required properties:

* Minimize Hash Collisions: In the event of a hash collision, multiple passwords would generate the same hash code, rendering them interchangeable[[1]](#footnote-1).
* Pre-Image Resistant (One-Way): If a list of hashed passwords is obtained, it should not be possible to discern the password from the hash code[[2]](#footnote-2), *even if the function is known*.
* Slow: Only one valid password is required by attackers in order to compromise the hashing function’s security. As it is possible to determine an accepted password through brute-force[[3]](#footnote-3), slower hash functions are important for impeding such attacks[[4]](#footnote-4).

## sdbm Hash Function (derived from C code)[[5]](#footnote-5) :

BEGIN sdbm

hash = 0

FOR char IN str

hash = char + (LEFTSHIFT hash by 6) + (LEFTSHIFT hash by 16) - hash

ENDFOR

RETURN hash

END sdbm

hash is an unsigned long, as otherwise the bit shifts may produce negative values, complicating the function’s logic significantly.

Bit shifting and subtraction is performed on the hash code in order to vary the bits with each character. This ensures the order of the characters affects the output code.

## Test Report:

**Performance of sdbm hashing function**

We found the sdbm function to perform optimally for password hashing, producing a unique hash code for all 10150 passwords in the dataset provided.

This is an important result, as two passwords which generate the same hash code are effectively interchangeable. As this causes an affected user’s account to have multiple valid passwords, such a conflict can heavily reduce security.

Although highly effective at producing unique hash codes, the biggest flaw in the sdbm function is its speed. Our implementation was able to generate 10150 hashes in 620ms, which is too fast to impede any significant brute-force attempts. Increasing the complexity of the calculations would significantly increase the function’s security in such a situation.

1. "Network Security" Princeton University, accessed October 2, 2015, http://www.cs.princeton.edu/courses/archive/spr11/cos461/docs/rec08-net-security.pdf [↑](#footnote-ref-1)
2. Menezes, A. J., and Paul C. Oorschot. *Handbook of Applied Cryptography*. (Boca Raton: CRC Press, 1997) [↑](#footnote-ref-2)
3. Halderman, J., Waters, B., and Felten, E. *A Convenient Method for Securely Managing Passwords* (Chiba: International World Wide Web Conference Committee, 2005) [↑](#footnote-ref-3)
4. Halderman, J., Waters, B., and Felten, E. *A Convenient Method for Securely Managing Passwords* (Chiba: International World Wide Web Conference Committee, 2005) [↑](#footnote-ref-4)
5. “Hash Functions” York University, accessed October 2, 2015, http://www.cse.yorku.ca/~oz/hash.html [↑](#footnote-ref-5)