NAME

sdlh − Shamir Discrete Logarithm Hash Function

SYNOPSIS

sdlh [-256] [-v] [-key keyfile] files

DESCRIPTION

sdlh prints the hash value computed on the input bytes that are stored in a file or piped in from stdin. The message is converted into a long integer x as in PKCS#1-OS2IP.

hash(x) = gˆx mod n

The length of the hash value will depend on the modulus used for hashing.
Without the option -key the hash key (modulus and generator) is read from a config file .hashkey in the user's home directory. If the config file does not exist and the option -key is not used, the hash value cannot be generated and an error message is printed to stdout.

If no file arguments are given, stdin is used and the message can be piped into the program.

A user's hash key (hashmodulus and generator) can be generated with the program **sdlh-generate-hashkey**.

OPTIONS

−256 The hash value has a fixed length of 256 bits.

−v Turn on verbose mode (default is off). Prints information about the User ID of the hash key file used (hashmodulus, generator). The length of the hash value in bits is appended to the hash value.

−key file
Reads the modulus and generator from a file.

NOTES

Full documentation https://senderek.ie/sdlh
https://www.metzdowd.com/pipermail/cryptography/2003-May/004642.html
https://www.metzdowd.com/pipermail/cryptography/2003-May/004781.html

FILES

$HOME/.hashkey
A user's default hash key (hashmodulus and generator) can be generated with the program **sdlh-generate-hashkey**. It must be stored in the user's home directory.

BUGS

Please report bugs to innovation@senderek.ie

AUTHORS

sdlh is written by Ralf Senderek <innovation@senderek.ie>.

COPYRIGHT

SEE ALSO

sdlh-generate-hashkey, pcp2, pcp2-protect-privatekey, pcp2-generate-rsakeys