NAME

sdlh-generate-hashkey − Key generation for the Shamir Discrete Logarithm Hash Function

SYNOPSIS

sdlh-generate-hashkey [-size numrandombytes]

DESCRIPTION

sdlh-generate-hashkey generates two large strong prime numbers P and Q and finds a generator value of maximum order for the group mod(P*Q).

The hashmodulus and generator values are stored in a file "./hashkey" together with a User ID string to form a valid hashkey that can be used with **sdlh** or **pcp2**.

OPTIONS

−size numrandombytes

The number of random bytes taken from /dev/random are used to find a strong prime. For every probable prime P that can be found the value (P-1)/2 is checked. If this value is also prime, P is regarded as a strong prime number. The number of random bytes (roughly) defines the size of the hash modulus.
The minimum number of random bytes is 85 and the maximum number is 128. If the user provides a size that is outside this range then no hashkey is generated.

NOTES

Full documentation: https://senderek.ie/sdlh

BUGS

Please report bugs to innovation@senderek.ie

AUTHORS

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

COPYRIGHT

SEE ALSO

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