Use DLP to build a fixed length collision resistant hash function

Based on DLP, two values can be hashed as

$$y = (g^{x1}.h^{x2})modP$$

Where g,h are primes in the Zp group and through this two values are hashed into a single value. In other words, the function hashes 2n bits to n bits.

The hash function first splits it into two halves and then generates the hash.

The arguments for generate and verify mode are also handled.

The code has been explained in the comments present in the script wherever necessary.