# Fixed Length Hash Function

A fixed length hash function maps 2 n-bit strings to one n-bit string. This kind of a hash function maps 2n → n bits always but can be converted into variable length by using a Merkle-Damgard like transform.

In our case, we use the Discrete log to again acheive a fixed length hash function.
Using a prime $q$ & 2 generators $g$ and $h$, we get the hash $h$ by

$$h = (g^{x_1} h^{x_2}) \bmod q$$

Since finding $x_1$ & $x_2$ from $h$ is hard, breaking the hashing algorithm by finding $x' = x_1' + x_2'$ with same hash $h$ is also hard.