Collision Resistant Hash Function:

A Hash Function is said to be collision resistant if it is infeasible for any probabilistic polynomial time algorithm to find a collision in H i.e, for any two different inputs x and y H(x) is not the same as H(y).

A Hash Function (Gen,H) is collision resistant if for all polynomial time adversaries A:

$$\Pr[\text{Output of Hash-game} = 1] \leq \text{negl}(n)$$

For a positive integer N, and q<= sqrt(2N) elements $y_1, y_2, .., y_q$ are choen uniformly and independently at random from a set of size N. Then the probability that there exist i,j with $y_i = y_j$ is at least q(q-1)/4N.

$$\text{coll}(q, N) \geq \frac{q(q-1)}{4N}.$$

Fixed Length Hash Function

Let P be a polynomial time algorithm that on input 1^n output a cyclic group of order q (length of q is n) and generator g

Gen: Run $P(1^n)$ to obtain (G,q,g). select uniformly at random an element h from G. Output s(G,q,g,h)

H: On input x_1 and x_2 each of length n, H returns an n-bit hash.

If the discrete logarithm problem is considered hard, then the above is a fixed length collision resistant hash function.

$H^s(x_1, x_2) = g^{x1}.h^{x2} \bmod q$

Here x1 and x2 will be in the range 0 to q-1.