Hash Function For My Own Use

As we know the hash function is function which is used to map the data to such data structure which have access time O(1) means we can access the data in just constant time so that during the processing the data the access and storage time take constant computational time, that not all it is also use for cryptographic encryption for maintaining the Integrity of data during transmission process.

The function which I suggest is as follow:

F(x)= (x0 \* N0+ x1 \* N1+ x2 \* N2+ x3 \* N3+ x4 \* N4+ x5 \* N5+…...) %M

Where

X is an integer or string.

X0, X1....... is the digit or character at the 0th and So on positions.

N is any prime number which is larger so that encryption range increase

M is the round off for maximum memory size slot M.

The Hash function must satisfy below three property's:

1. One way: Can’t be reversed

It states that if we have function H(X) where H is hashing function and X is an input number then

let h=H(X)

Then it hard to reverse it and find X.

In an above function F(X) from the analysis you can see that the function is contain the polynomial equation which is of the power Since number h can be form from multiplication of number then it's hard to find and try all the combination for that particular h to find x requires knowledge of the F(X) which if not available then it quit be irreversible.

2.Output does not reveal information on input

It’s related to first Property such that the output is not going to reveal the information about input but if we think the h is a number from that we can’t predict any polynomial equation such that ir give the output as same.

3.Hard to find Collisions.

Collision in the term of the hash function meaning that the it impossible to find X, Y such that the h1=h2 which is quit be possible in above case.

An example is as follow:

For string Aa and BB is as the show below:

"Aa" = 'A' \* 31 + 'a' = 2112  
"BB" = 'B' \* 31 + 'B' = 2112

Which can be solve by again hashing with the number other that N=32.

And replace the hash with another.

For that data we key=any other than that.