1. Let variables x1, x2, x3, etc represent each bit, and go through procedure algebraically. The output will be in terms of the individual bits. This is in addition to each bit having a value. So, each bit would have a numeric value, 0 o 1, and a symbolic value.
2. Use variable length words, but never truncate. See if this helps in the final answer. May be able to use the otherwise “lost” information.
3. Use matrices to represent values. Maybe matrix operations could be substituted.
4. Get hash of “” (nothing). Is this useful? Get has of 1. Is this useful?
5. Devise a very simple hash routine..not secure or long. But useful as tool. One loop, few operations, etc. Practice finding inverse, solutions, collisions, breaking preimage resistance, etc. Then scale up gradually.
6. Use Fourier analysis to analyze message before and after hashing. Before and after nonce? At points in the process?