Introduction to Cryptography (462)
Hashing Formulas
T.J. Borrelli

Some formulas that may be helpful when dealing with hashing problems:

1. Computing the probability of a birthday collision among n people:

   $1 - \frac{_{365}\mathbf{P}_n}{365^n}$

   Where P is the permutation function.

2. Computing the number of hash outputs that must be checked before finding a collision:

   $t \approx 2^{(n+1)/2}\sqrt{ln\frac{1}{1-\lambda}}$

   ln: is the natural log function
   n: output length of hash function in bits
   λ: probability of collision