CIS 5371 Cryptography

QUIZ 11 (5 minutes only) –with answers

This quiz concerns the “birthday” attack and the Merkle-Damgård transform.

1. Use some of the following words/expressions to describe the birthday attack:
   \[ H : \{0,1\}^* \to \{0,1\}^\ell, \{0,1\}^*, y = H(x), q = \Theta(2^{\ell/2}), x_1, \ldots, x_q \in \{0,1\}^*, O(\ell \cdot 2^{\ell/2}), \text{uniformly distributed, is greater than, hash function, assume that, Let, The time taken, the values, using, hash evaluations, independent, there is a collision, arbitrary inputs, are selected, probability.} \]
   \textbf{Answer.}
   \[
   \text{Let } H : \{0,1\}^* \to \{0,1\}^\ell \text{ be a hash function. Assume that the values } y = H(x) \text{ are uniformly distributed and that } q \text{ arbitrary inputs } x_1, \ldots, x_q \in \{0,1\}^* \text{ are selected. Then the probability that there is a collision using } q = \Theta(2^{\ell/2}) \text{ hash evaluations is greater than } 1/2. \\
   \text{The time taken is } O(\ell \cdot 2^{\ell/2}).
   \]

2. A hash function is constructed based on the Data Encryption Standard (DES, which is a permutation of 64-bit strings) using the Merkle-Damgård transform. Roughly how many messages must be hashed so that we get a collision with probability greater than 1/2?
   \textbf{Answer.} \[ q = 2^{32}. \]

3. Draw a sketch of the flows of the Merkle-Damgård transform.
   \textbf{Answer.} See slides.

Mike Burmester