

Family of uniform hash functions

The notion of pairwise independence says that, for any $x_1 \neq x_2$ and $c_1, c_2 \in Z_p$, we have that

$$\Pr_{h \in H}[h(x_1) = c_1 \wedge h(x_2) = c_2] = \Pr_{h \in H}[h(x_1) = c_1] * \Pr_{h \in H}[h(x_2) = c_2]$$

In other words, the joint probability is the product of the two individual probabilities. Show that the family of hash functions $H = \{h_{ab}(x) = ((ax + b) \bmod p) \bmod m : a \in Z_p^*, b \in Z_p\}$ (seen in class) is "pairwise independent", where p is a sufficiently large prime number ($m + 1 \leq p \leq 2m$).

SOLUTION