

$$(1) P[M = m | C = c] = \frac{P[M = m \wedge C = c]}{P[C = c]} \quad (\text{definition of conditional probability})$$

$$(2) P[M = m \wedge C = c] = P[M = m \wedge K = m \oplus c] \quad (M = m \wedge C = c \text{ and } M = m \wedge K = m \oplus c \text{ are equivalent}) \\ = P[M = m] \cdot P[k = m \oplus c] \quad (K \text{ is independent of } M, \text{ so you can multiply these two}) \\ = P[M = m] \cdot 2^{-n} \quad (K \text{ is randomly chosen})$$

$$(3) P[C = c] = \sum_m P[M = m \wedge C = c] \\ = \sum_m P[M = m] \cdot 2^{-n} \quad (\text{by the result obtained in 2}) \\ = 1 \cdot 2^{-n} \quad (\sum_m P[M = m] = 1) \\ = 2^{-n} \quad (\text{that is, each } c \text{ is equally likely})$$

$$(4) P[M = m | C = c] = \frac{P[M = m \wedge C = c]}{P[C = c]} \\ = \frac{P[M = m] \cdot 2^{-n}}{2^{-n}} \quad (\text{by the result obtained in 2 and 3}) \\ = P[M = m]$$

