

1.

log(a,b) = log(a) + log(b) p(X=x) = ∑x p(X=x,Y=y) p(a,b) = p(a|b)\*p(b)

H(X,Y) = -∑x∑y (p(x,y)\*log2(p(x,y)))

= -∑x∑y (p(x,y)\*log2(p(x|y)\*p(y)))

= (-∑x∑y (p(x,y)\*log2(p(x|y)))) + (-∑x∑y(p(x,y)\*log2(p(y))))

= (-∑x∑y (p(x|y)\*p(y)\*log2(p(x|y)))) + (-∑x∑y(p(x,y)\*log2(p(y))))

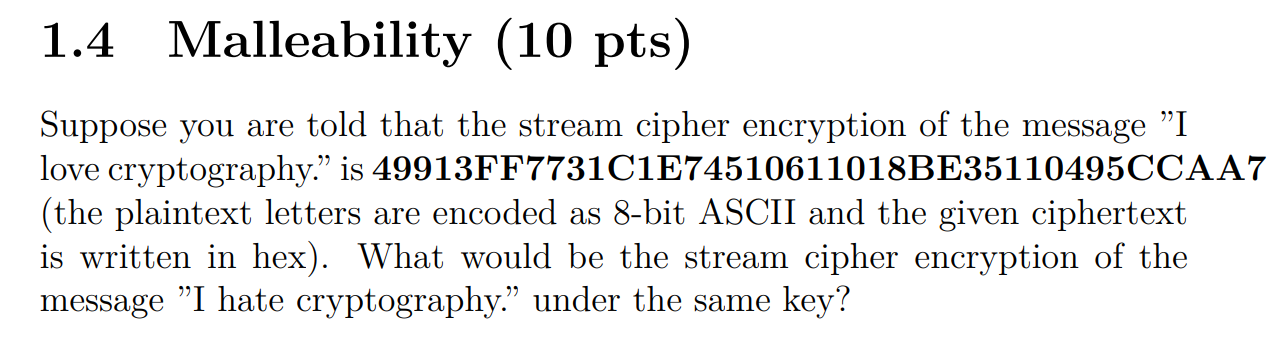
= (-∑y(p(y))∑x(p(x|y)\*log2(p(x|y)))) + (-∑y(p(y)\*log2(p(y))))

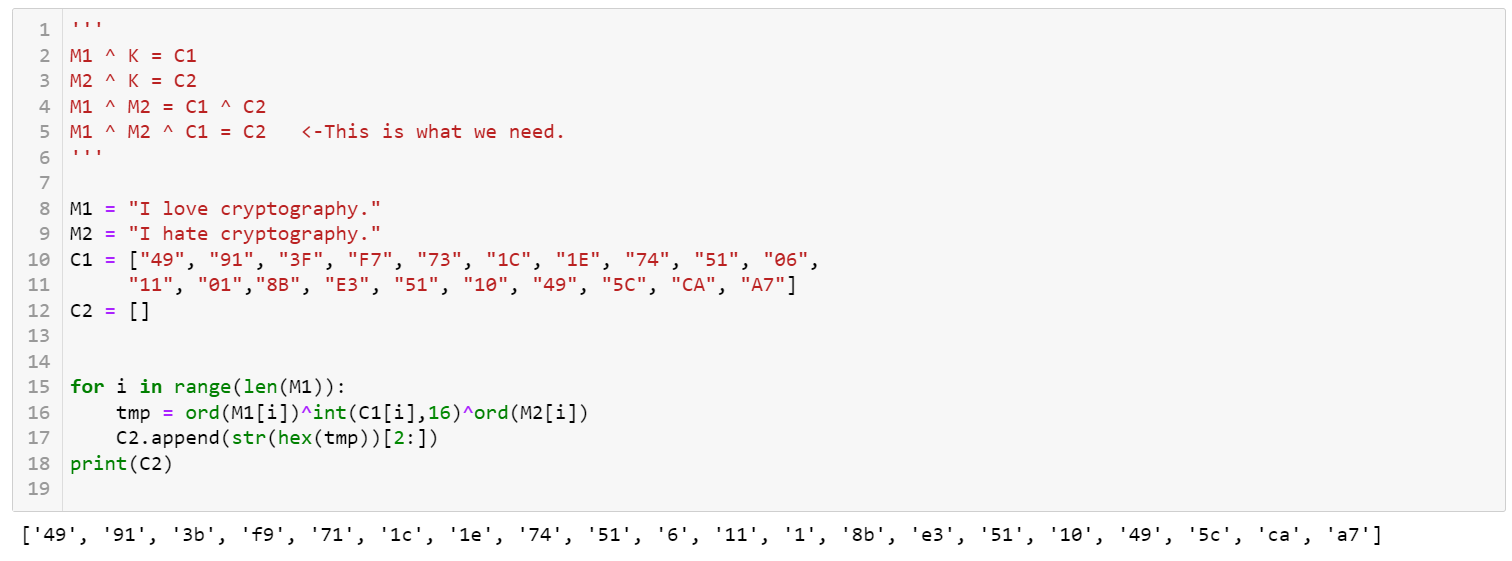
= H(X|Y) + H(Y)

2.

結合1.可知 H(Y) + H(X|Y) ≤ H(X) + H(Y)，故變成證明H(X|Y) ≤ H(X)

因為H(X|Y)表示「給了Y的資訊後, X剩下的資訊量」，所以他必少於或等於「X本身的資訊量」H(X)





I hate cryptography. -> 49913BF9711C1E74510611018BE35110495CCAA7