1. **The random variable Z where Z=X+Y, where X and Y are also (not necessarily independent) random variables.**

   a. **Establish that H(Z|X) = H(Y|X)**
   b. **Establish that if X and Y are independent H(Z|X) = H(Y) and show that H(Y) ≤ H(Z) and H(X) ≤ H(Z)**
   c. **Give an example where H(Y) > H(Z)**

$H(Z,Y|X)$
$= H(Z|Y) + H(Y|X,Z)$
$= H(Y|X) + H(Z|Y,X)$
$=$

a) $H(Z|X) = -\sum_x \sum_z p(x,z) \log_2 p(z|x)$ $\quad z = x+y$

$= -\sum_x \sum_{z=x+y} p(x, x+y) \log_2 \frac{p(x+y|x)}{p(y|x)}$ $\quad p(X+Y=x+y \mid X=x)$

$= -\sum_x \sum_y p(x,y) \log_2 p(y|x) = H(Y|X)$

b) $H(Z|X) = H(Y|X) = H(Y)$

↑ if x & y are independent

$\Rightarrow$ Note $H(Y|X) \le H(Y) = H(Z|X) \le H(Z)$

$\Rightarrow H(Y) \le H(Z)$

$\Rightarrow$ Note: as in a) $H(Z|Y) = H(X|Y)$

if x & y independent

$H(Z|Y) = H(X|Y) = H(X)$

$\Rightarrow H(X|Y) \le H(X) = H(Z|Y) \le H(Z)$

$H(X) \le H(Z)$.

c) x & y are dependent

$y \in \{0,1\}$ w/ $p(Y=0) = p(Y=1) = 1/2 \Rightarrow H(Y) = 1$ b.t.

Let $X = Y$ (dependent)

$\Rightarrow Z = X + Y$ where $+ = XOR$

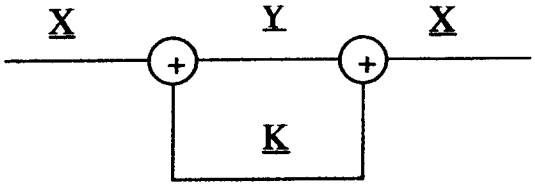
$\Rightarrow Z = 0$ w.p. probability 1 $\Rightarrow H(Z) = 0$

$H(Z) < H(Y)$

2. *Effect of key correlation on security.* The following diagram for a cryptographic system was described in class, except now $\underline{X} = [X1, X2]$, $\underline{K} = [K1, K2]$, $\underline{Y} = [Y1, Y2]$ are vectors, where all X1, X2, K1, K2, Y1 and Y2 are bits and $\underline{Y} = \underline{X} + \underline{K}$ where '+' is a component-wise XOR.

   a. If K1 and K2 are independent and each equally likely to be 0 or 1 show that the system is perfectly secure, namely show that $I(\underline{X};\underline{Y}) = 0$.

   b. If the key bits are always equal, namely K=[0,0] or [1,1] (with equal probability), is the system perfectly secure? Justify your answer.



(+5) a) $I(\underline{X};\underline{Y}) = I(X_1 X_2; Y_1 Y_2)$

$= I(X_1; Y_1 Y_2) + I(X_2; Y_1 Y_2 | X_1)$ (A)

$= I(X_1; Y_1) + I(X_1; Y_2 | Y_1) + I(X_2; Y_1 | X_1) + I(X_2; Y_2 | X_1 Y_1)$

Note: If $X_1 \& X_2$ are independent of each other and independent of $K_1 \& K_2$

$I(X_1; Y_2 | Y_1) = 0$, $I(X_2; Y_1 | X_1) = 0$

$I(X_2; Y_2 | X_1 Y_1) = I(X_2; Y_2)$

$I(X, Y) = \underbrace{I(X_1; Y_1)}_{0 \text{ by class}} + \underbrace{I(X_2; Y_2)}_{0 \text{ by class}} = 0$

(+5) b) Note in (A) $I(X_2; Y_2 | X_1 Y_1)$

$Y_1 = X_1 + K \rightarrow$ if X_1, Y_1 known $\Rightarrow K$ is known

$Y_2 = X_2 + K$

$\Rightarrow I(X_2; Y_2 | X_1 Y_1) = 1$

System is <u>not</u> perfectly secure.

3. Consider a discrete memoryless source with the probability distribution of P = (p, 1-p) for 0 and 1, respectively.

(a) Suppose $X^n=(x_1,\ldots,x_n)$ is an observed sequence of this source with m ($0\le m\le n$) elements equal to 0. Let Q be the probability mass function $Q=\left(\frac{m}{n},\frac{n-m}{n}\right)$.

Show that the probability mass function $\Pr(X^n)=2^{-n[D(Q\|P)+H(Q)]}$

(b) The sequence $X^n=(x_1,\ldots,x_n)$ in part a) with exactly m zeros is called a sequence of type Q. Let T_Q denote the set of all these sequences with exactly m zeros. Using part a) and the fact that $|T_Q|\le 2^{nH(Q)}$ to find an upper bound on $\Pr\{T_Q\}$.

(c) Describe intuitively the meaning of this inequality, and discuss what occurs asymptotically when $n\to\infty$

a) X^n has m 0's out of n $\Rightarrow P(X^n)=p^m(1-p)^{n-m}$

Note: $D(Q\|P)+H(Q)=\sum_{x\in\{0,1\}} Q(x)\log_2\frac{Q(x)}{P(x)}+\sum -Q(x)\log_2 Q(x)$

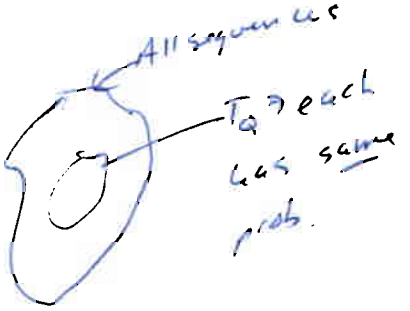
$=\sum_x Q(x)\log\frac{1}{P(x)}=-\sum_x Q(x)\log P(x)$

$=-\frac{m}{n}\log p+-\frac{(n-m)}{n}\log(1-p)$

Note $2^{-n(D(Q\|P)+H(Q))}=2^{-n\left\{-\frac{m}{n}\log_2 p+\frac{n-m}{n}\log_2(1-p)\right\}}$

$=2^{\log_2 p^m+\log_2(1-p)^{n-m}}=p^m(1-p)^{n-m}$

b)



$\Pr\{T_Q\}=|T_Q|P(X^n)$

$\le 2^{nH(Q)}\,2^{-n(D(Q\|P)+H(x))}$

$\Rightarrow \Pr\{T_Q\}\le 2^{-nD(Q\|P)}$

c) Note as $n\to\infty$ Q and P get close $\Rightarrow D(Q\|P)\to 0$

$\Rightarrow \Pr\{T_Q\}\to 1$ as