1. $$I(y) = \sum_{i=0}^{25} \frac{f_i(f_i-1)}{N(N-1)}$$

P[see letter i first]

P[see letter i second & saw letter i first]

where y has length N and f_i is frequency of letter i.

$$\begin{array}{ccccccccccccc} x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 & x_9 & x_{10} & x_{11} & x_{12} \\ k_0 & k_1 & k_2 & k_3 & k_4 & k_5 & k_0 & k_1 & k_2 & \cdot & \cdot & \cdot & \cdot \\ y_0 & y_1 & y_2 & y_3 & y_4 & y_5 & y_6 & y_7 & y_8 & y_9 & y_{10} & y_{11} & y_{12} \end{array}$$

$y_0 = x_0 + k_0 = x_0 + 0 = x_0$

$y_3 = x_3 + k_0 = x_3 + 0 = x_3 \leftrightarrow a$

$y_0 \; y_6 \; y_{12}$

$= x_0 + k_0, \; x_6 + k_0, \; x_{12} + k_0$

biggest IOC has $l = 6$

key probably has length 6.

IOC maximised when only see one shift, so when l is a multiple of the key length.

ABC unlikely: wrong length: IOC would be as big at $l=3$ as $l=6$.

to length 9.

ABCAEF unlikely: $k_0 = k_3 = 0 \leftrightarrow a$ so same for sample as if ABC.

0 3

ABCDEF ~~likely~~ possible key

2. (b) X plaintext

Y ciphertext

K key.

1/4 (1,0) $x \to x$

1/4 (2,0) $x \to 2x$

1/4 (3,0) $x \to 3x$

1/4 (4,0) $x \to 4x$ mod 5

(i) $\mathbb{P}[Y=2 \mid X=1] = \mathbb{P}[\text{key maps } 1 \text{ to } 2]$

$= \mathbb{P}[\text{key is } (2,0)]$

$= 1/4$

(ii) $\mathbb{P}[Y=2] = \sum_{x=0}^{4} \mathbb{P}[Y=2 \mid X=x] p_x$

$= \mathbb{P}[Y=2 \mid X=0] p_0 + \mathbb{P}[Y=2 \mid X=1] p_1 + \cdots + \mathbb{P}[Y=2 \mid X=4] p_4$

$= 0 + \frac{1}{4} p_1 + \frac{1}{4} p_2 + \frac{1}{4} p_3 + \frac{1}{4} p_4$

$= \frac{1}{4}(p_1+p_2+p_3+p_4)$

$\mathbb{P}[X=1 \mid Y=2] = \dfrac{\mathbb{P}[Y=2 \mid X=1]\,\mathbb{P}[X=1]}{\mathbb{P}[Y=2]}$

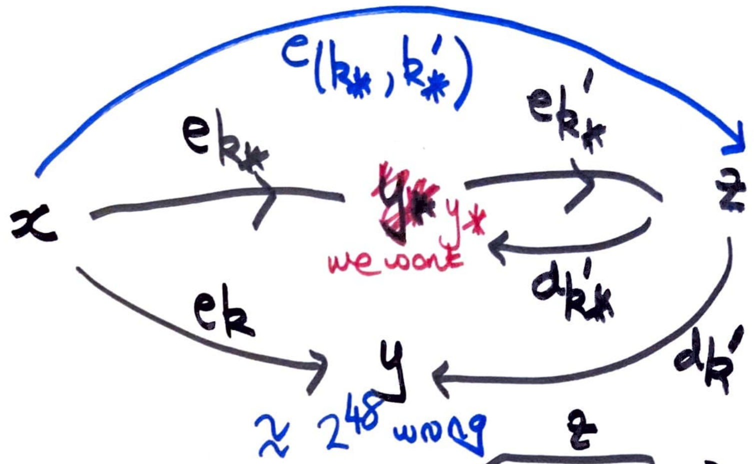
$= \frac{1}{4} p_1 \Big/ \frac{1}{4}(p_1+p_2+p_3+p_4) = \dfrac{p_1}{p_1+p_2+p_3+p_4} = \dfrac{p_1}{1-p_0}$

(iii) $\mathbb{P}[X=x \mid Y=y] = p_x$ (Perfect secrecy)

e.g. if $p_0 = p_1 = \cdots = p_4 = \frac{1}{5}$ then $\mathbb{P}[X=1 \mid Y=2] = \dfrac{1/5}{4/5} = \frac{1}{4}$

$\neq 1/5$. So no PS.

4. 2DES has block size 64
key length $56+56=112$



(i) $y_* = e_{k_*}(x) = d_{k'_*}\big[\overbrace{e_{k'_*} e_{k_*}(x)}^{z}\big] = d_{k'_*}(z)$

(ii) let $y = e_k(x) \in \mathbb{F}_{2^{64}}$
chance hit y by decrypting z with some random k' is $\frac{1}{2^{64}}$.
There are 2^{56} k, 2^{56} k' so expect
$2^{56} \times 2^{56} \times \frac{1}{2^{64}} = 2^{112-64} = 2^{48}$ collisions

(iii) $X \xrightarrow{e(k_*, k'_*)} Z$ test to see if $e(k,k')(X) = Z$ for each

of the 2^{48} candidate keys from (iii).
chance hit z with a random key
(not (k_*, k_*')) is $\frac{1}{2^{64}}$

So probably only right key passes test.

(iv) subexhaustive: used 2^{56} encs on x
$+\ 2^{56}$ decs on z
$+\ 2^{48}$ 2DES encs

$\approx 2^{58} < 2^{112} = |K|$.

hence subexhaustive

6. (c) Alice received $y = x^c$ modulo n and decrypted by calculating

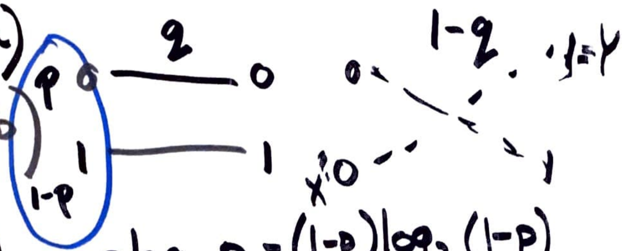
$$y^r = x^{cr} \bmod n \equiv x \bmod n$$

(i) No, since the message was encrypted using RSA

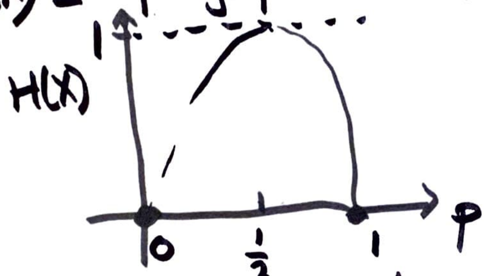
(ii) No: anyone can encrypt a message to Alice.

7. (a)

(b)



(i) $H(X) = -p\log_2 p - (1-p)\log_2(1-p)$



(ii) $\mathbb{P}[Y=0] = \mathbb{P}[Y=0 \mid X=0]p_0 + \mathbb{P}[Y=0 \mid$ [redacted] $]p_1$

$= \mathbb{P}[K=0]p + \mathbb{P}[K=1](1-p)$

$= qp + (1-q)(1-p) = r$

$\mathbb{P}[Y=1] = 1-r = (1-q)p + q(1-p)$
Exercise

$H(Y) = H(r, 1-r) = -r\log_2 r - (1-r)\log_2(1-r)$

if $p = \frac{1}{2}$ $r = q\frac{1}{2} + (1-q)\frac{1}{2} = \frac{1}{2}$

$\Rightarrow 1-r = 1/2$

$\Rightarrow H(Y) = H(1/2, 1/2) = 1.$

Exercise Show that if $q = \frac{1}{2}$ then $H(Y) = 1$.

(iii) $H(K|Y) = H(K) - \underbrace{H(Y) + H(X)}$

(iv) $q = \frac{3}{4}$ $= H\left(\frac{3}{4}, \frac{1}{4}\right) + H(p, 1-p)$
$- H(Y)$

$H(Y) \geq H(X)$ since ciphertext more random than plaintext.

$H(K|Y)$ is maximised when $H(Y) = H(X)$
so for example when $p = \frac{1}{2}$ by (i), (ii)
So $H(K|Y) \geq H(3/4, 1/4)$ with equality when $p = 1/2$.

(c) $\mathbb{P}[X=x \mid Y=y] = \mathbb{P}[X=x]$

perfect secrecy

$\Leftrightarrow$ $X=x$, $Y=y$ are independent

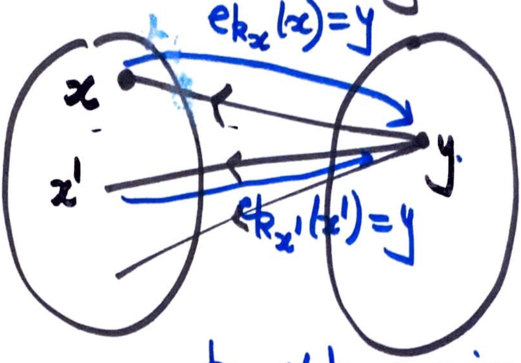
(ii) $\mathbb{P}[Y=y \mid X=x] = \mathbb{P}[K \in \mathcal{K}_{xy}]$

$\|$ independence

$\mathbb{P}[Y=y] > 0$ by practicality assumption

$\Rightarrow \mathcal{K}_{xy} \neq \emptyset$.

(iii)



$k_x \neq k_{x'}$ since different decrypts of y

$\Rightarrow |K| \geq |P|$.

(iv) No: 128 bits of key encrypt megabytes of plaintext.

$u_0 \quad u_1 \quad u_2 \quad \cdots$

8. 0 0 1 0 0 0 1 1 0 0 1 0

$k_0k_0' \quad k_1k_1' \quad k_2k_2' \quad k_3k_3' \quad k_4k_4' \quad \cdots$

(i) $u_2 = 1 \Rightarrow k_2 = k_2' = 1.$

(ii) F width 3 taps $\{1, 2, 3\}$

$$\begin{array}{ccccccccccc} k_0 & k_1 & 1 & k_3 & k_4 & 1 & 1 & k_7 & k_8 & 1 & k_{10} \\ & & k_2 & 0 & 0 & k_5 & k_6 & & & k_9 & \end{array}$$

$k_1 + k_2 + k_3 = 0 = k_4 \qquad k_2 + k_3 + k_4$

$\Rightarrow k_1 + 1 + 0 = 0 \qquad = 1 + k_3 + k_4$

$\Rightarrow k_1 = 1 \qquad \Rightarrow k_3 + k_4 = 0$

if both 1

$k_0 + k_1 + k_2 = 0 = k_3 \qquad 1 \; 1 \; 1 \; 1 \; 1 \; 1 \cdots$

$\Rightarrow k_0 + 1 + 1 = 0$

$\Rightarrow k_0 = 0. \quad \Rightarrow k_0k_1k_2 \cdots = 111 \cdots\cdots$

$\Rightarrow u_0u_1u_2 \cdots = k_0'k_1'k_2' \cdots$

$\cdots 00010$ key stream of F width 3 can't have 0001

Contradiction. Hence both 0

u_0 u_1 u_2 u_3 . . .

0 0 1 0 0 1 1 0 0 1 0

period 4

$k_0 k_1 k_2 \ldots$ 0 1 1 0 0 1 1 0 0 1 1

$k_0' k_1' k_2' \ldots$ k_0' 0 1 k_3' k_4' 1 1 k_7' k_8' 1 0

e.g. $0 = u_1 = k_1 k_1' = 1 \times k_1' = k_1'$

G invertible $\iff$ width is a tap

$\implies 3 \in T$ = taps of G.

G max period namely $2^{\text{width}} - 1 = 7$.

if 3 is only tap

$\underbrace{k_0' k_1' k_2'}$ $k_0' k_1' k_2'$ . . . is keystream period 3 ✗

if $\{1,2,3\} = T$ G = F has a keystream of period 4 ✗

~~guess~~ $T = \{1,3\}$ or $T = \{2,3\}$

$\{1,3\}$ k_0' 0 1 k_3' k_4' 1 1 k_7' k_8' 1 0

$k_0' = 0$ | 0 0 1 1 1 0 ✗

$k_0' = 1$ | 1 0 1 0 0 1 1 1 0 0 ✗

$\{2,3\}$ 0 0 1 1 0 1 1 0 1 1 . . .

consistent: $\{2,3\}$, key is 001.

2019 Q3.

$k_0 k_1 k_2 \cdots$

0 1 2 3 4 5 6 7 8 9

1 0 1 1 0 1 0 0 1 1

<u>Initialisation</u> $m = 0$ F_0 is LFSR taps $\emptyset$ width 0

$f_0 = 1$

$n = 1$ F_1 is LFSR taps $\emptyset$ width 1

$f_1 = 1$

<u>Steps</u> At step n we have an LFSR F_n correctly generating $k_0 k_1 \cdots k_{n-1}$.

<u>Step 1</u> F_1 generates $\underline{1}0$ correct for pos 1

so keep F_1, ie. $F_2 = F_1$ LFSR taps $\emptyset$ width 1.

$f_2 = f_1 = 1$ (no taps)

<u>Step 2</u> F_2 generates 100 wrong in pos 2

Update to the LFSR with tapping polynomial

$$z^{n-m} f_m + f_n$$

[Recall $f_n = 1 + \sum_{t \in T} z^t$ if taps are T.]

$$= z^{2-0} 1 + 1 = \underline{z^2 + 1}$$

and $l_2 = \max(n+1-l_1, l_1)$

$= \max(3-1, 1) = \max(2,1) = 2$

So F_3 is LFSR taps $\{2\}$ width 2 because width increased update m to 2 step number,

<u>Step 3</u> F_3 generates $\underline{10}10$ wrong in pos 3

Update to the LFSR with tapping polynomial

$$z^{3-2} f_2 + f_3 = z 1 + 1 + z^2 = 1 + z + z^2$$

and $l_3 = \max(4-2, 2) = 2$

So F_4 is LFSR taps [1,2] width 2
width did not go up so n unchanged.

Step 4 F_4 generates $\underline{10}$ 1 1 0 so
$F_4 = F_5$

Step 5 F_5 generates $\underline{10}$ 1 $\underline{10}$ 1 so
$F_5 = F_6$

Step 6 F_6 generates $\underline{10}$ 1 1 0 1 1 wrong
in pos 6 so update.

Step 8 also updates.

Exercise: compute F_7 with tapping poly
$z^{6-2} f_2 + f_6 \overset{\text{chk}}{=} 1 + z + z^2 + z^4$

Disjunctive normal form

(CNOT)	x_0	x_1	x_2	CNOT	$x_0 \wedge x_1 \wedge \neg x_2$	$\neg x_0 \wedge \neg x_1 \wedge x_2$
$\emptyset$	0	0	0	0	0	0
$\{1\}$	0	1	0	0	0	0
$\{0\}$	1	0	0	0	0	0
$\{0,1\}$	1	1	0	1	1	0
$\{2\}$	0	0	1	1	0	1
$\{1,2\}$	0	1	1	1	0	0
$\{0,2\}$	1	0	1	1	0	0
$\{0,1,2\}$	1	1	1	0	0	0

$$\text{CNOT} = (x_0 \wedge x_1 \wedge \neg x_2) \vee (\neg x_0 \wedge \neg x_1 \wedge x_2)$$
$$\underset{\text{or}}{\vee} (\neg x_0 \underset{\text{and}}{\wedge} x_1 \wedge x_2) \vee (x_0 \wedge \neg x_1 \wedge x_2)$$

is DNF of CNOT.

$$\underset{\text{notation of notes}}{=} f_{\{0,1\}} \vee f_{\{2\}} \vee f_{\{1,2\}} \vee f_{\{0,2\}}$$

Corollary of DNF Above the truth table with 3 vars x_0 x_1 x_2 has 2^3 rows so there are 2^{2^3} subsets of the rows (we had $\{\{0,1\},\{2\},\{1,2\},\{0,2\}\}$) so there are 2^{2^3} different DNFs.
Generally 2^{2^n} if n variables.

7.2 MSc.

$$\sum_{w_1,w_2\in\mathbb{F}_2} (-1)^{(w_1+k_1)(w_2+k_2)}$$

<u>Ex</u> $k_1=k_2=0 \rightsquigarrow \displaystyle\sum_{w_1,w_2\in\mathbb{F}_2}(-1)^{w_1w_2}$

$$= (-1)^{00}+(-1)^{01}+(-1)^{10}+(-1)^{11} = 1+1+1-1 = 2$$

$k_1=1=k_2 \rightsquigarrow \displaystyle\sum_{w_1,w_2\in\mathbb{F}_2}(-1)^{(w_1+1)(w_2+1)}$

$$= \underbrace{(-1)^{11}}_{-1}+\underbrace{(-1)^{10}}_{1}+\underbrace{(-1)^{01}}_{1}+\underbrace{(-1)^{00}}_{1} = 2$$

same summands in different order

Generally $\displaystyle\sum_{w_1,w_2\in\mathbb{F}_2}(-1)^{(w_1+k_1)(w_2+k_2)} = S$

$$= \sum_{v_1,v_2\in\mathbb{F}_2}(-1)^{v_1v_2} \quad \text{so same as if } k_1=k_2=0$$

$$= \sum_{w_1,w_2\in\mathbb{F}_2}(-1)^{w_1w_2}.$$

$$\sum_{(v,w)\in\mathbb{F}_2^8} (-1)^{(w_1+k_1)(w_2+k_2)} \text{ [redacted] } = \overset{\times 2\ \times 2\ \times 2\ \times 2}{\sum_{\substack{v_0,v_1,v_2,v_3\\ \times 2\ w_0,w_1,w_2,w_3\in\mathbb{F}_2}}} (-1)^{(w_1+k_1)(w_2+k_2)} = 2^6 S$$