	Key length	# of Keys
rectangular transposition		
ADFGVX		
homophonic		
Vernam	p & q	$26^p \cdot 26^q = 26^{p+q}$
Vigenere -8 · 3.2 bits	8	26^8

		# of Keys	# of ~~plaintext~~ cyphertext ~~cypertext~~ length r
Vernam	p & q	$26^p \cdot 26^q = 26^{p+q}$	26^r
homophonic	n	25^n	$(25 \cdot n)^r$
ADFGVX	key 2n 6x6 square	$(2n)!$ $36 \cdot 35 \cdot 34 \cdots 11$	6^r
rectangular transposition	n	$n!$	26^r
playfair	5x5 square	$\frac{25!}{25}$	25^r

$$H(K) = H(C) - H(M)$$

Vigenere

$$H(K) = \log_2 26^8 = 8 * 4.7$$

$$H(C) = \log_2 (26^N) = N * 4.7$$

$$H(M) = 3.2N$$

$$8 \cdot 4.7 = N * 4.7 - N * 3.2$$

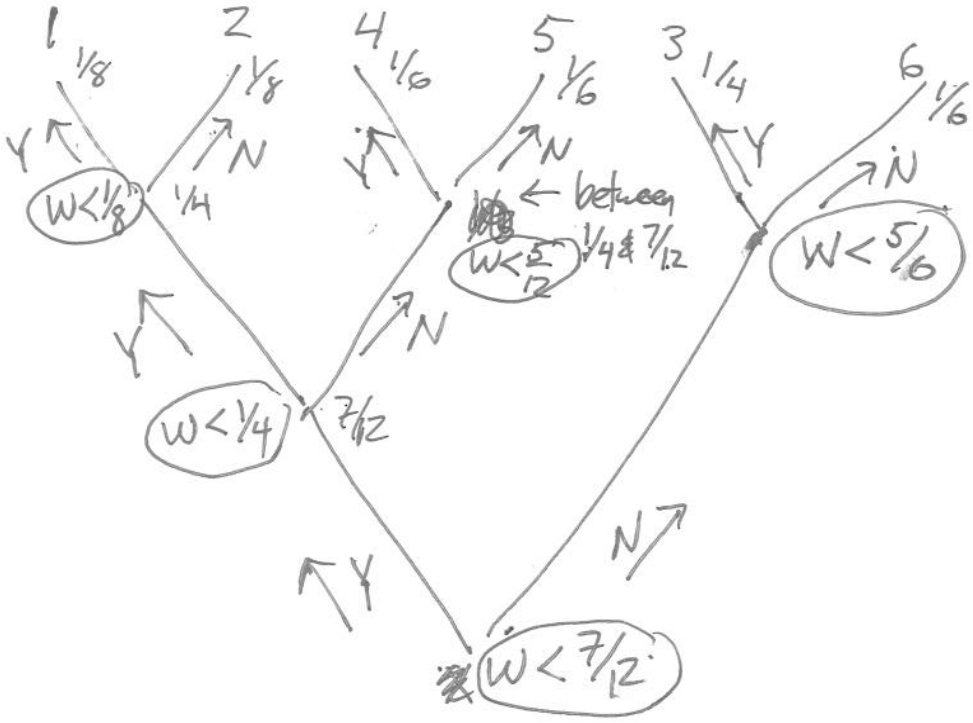
$$= N * 1.5$$

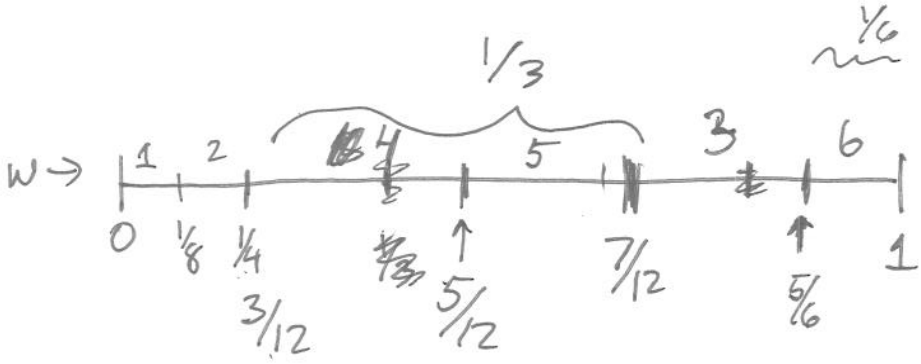
$$N \cong 25$$

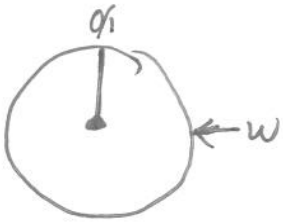
Playfair

	B		I	F
	C			
A		G	E	
	D			H

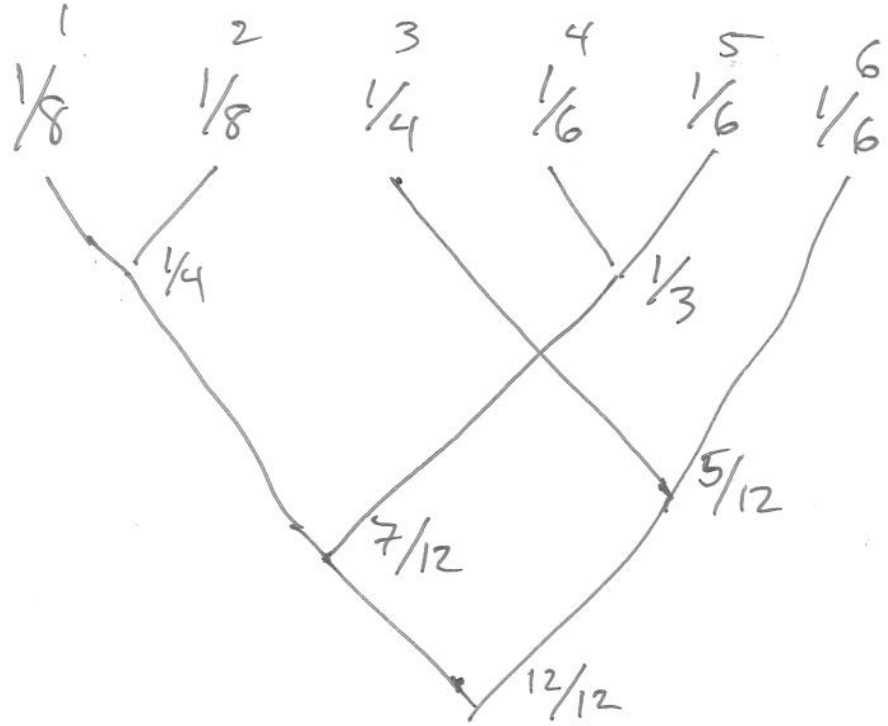
	D			H
	B		I	F
	C			
A		G	E	


1
1/8
2
1/8
4
1/6
5
1/6
3
1/4
6
1/6
Y
N
Y
N
Y
N
W<1/8
1/4
← between
1/4 & 7/12
W<5/12
W<5/6
Y
N
W<1/4
7/12
Y
N
W<7/12





W greater than/less than a value x



Expected Code Length

Theorem 2 *The best possible expected code length (bits per letter) is*

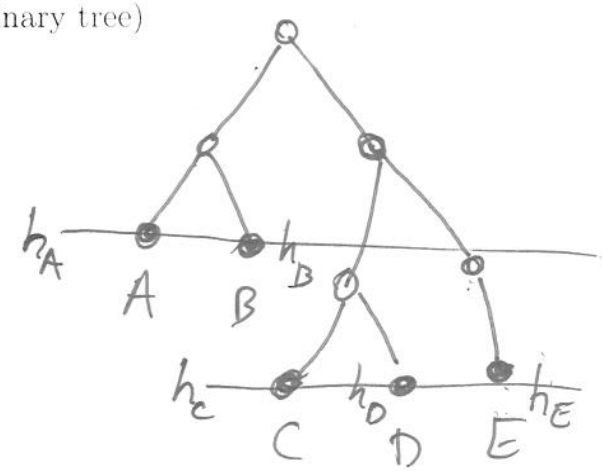
$$\boxed{H = \sum_{i=1}^{n} p_i \log_2 1/p_i}$$

Proof.

Letter frequenices $N_1, N_2, \ldots, N_k$ ($N = \sum_{i=1}^{k} N_i$)

Code lengths $h_1, h_2, \ldots, h_k$ (from a binary tree)

$p_i = N_i/N$ and $q_i = 1/2^{h_i}$



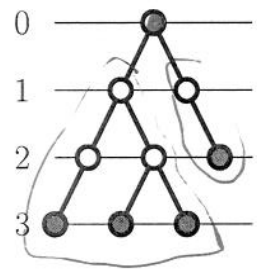
$$\begin{aligned}
N = \text{File length} &= \sum_{i=1}^{k} N_i h_i \\
&= N \sum_{i=1}^{k} \frac{N_i}{N} \log_2 2^{h_i} \\
&= N \sum_{i=1}^{k} p_i \log_2 1/q_i \\
&\geq N \sum_{i=1}^{k} p_i \log_2 1/p_i = NH
\end{aligned}$$

$(\geq)$ $\geq$

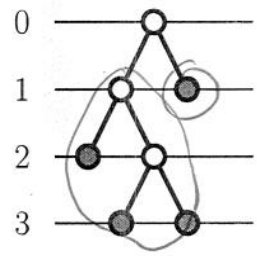
N_A = # of A's

N_B = # of B's

Leaf Heights



$$\frac{1}{2^3} + \frac{1}{2^3} + \frac{1}{2^3} + \frac{1}{2^2} = 5/8$$



$$\frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^3} + \frac{1}{2^1} = 1$$

Theorem 1 *The sequence of integers $h_1, h_2, \ldots, h_n$ are leaf heights of a binary tree if and only if*

$$\sum_{i=1}^{n} \frac{1}{2^{h_i}} \leq 1$$

with equality only if the tree is complete.

proof is by induction

Theorem

Perfect secrecy is achieved when

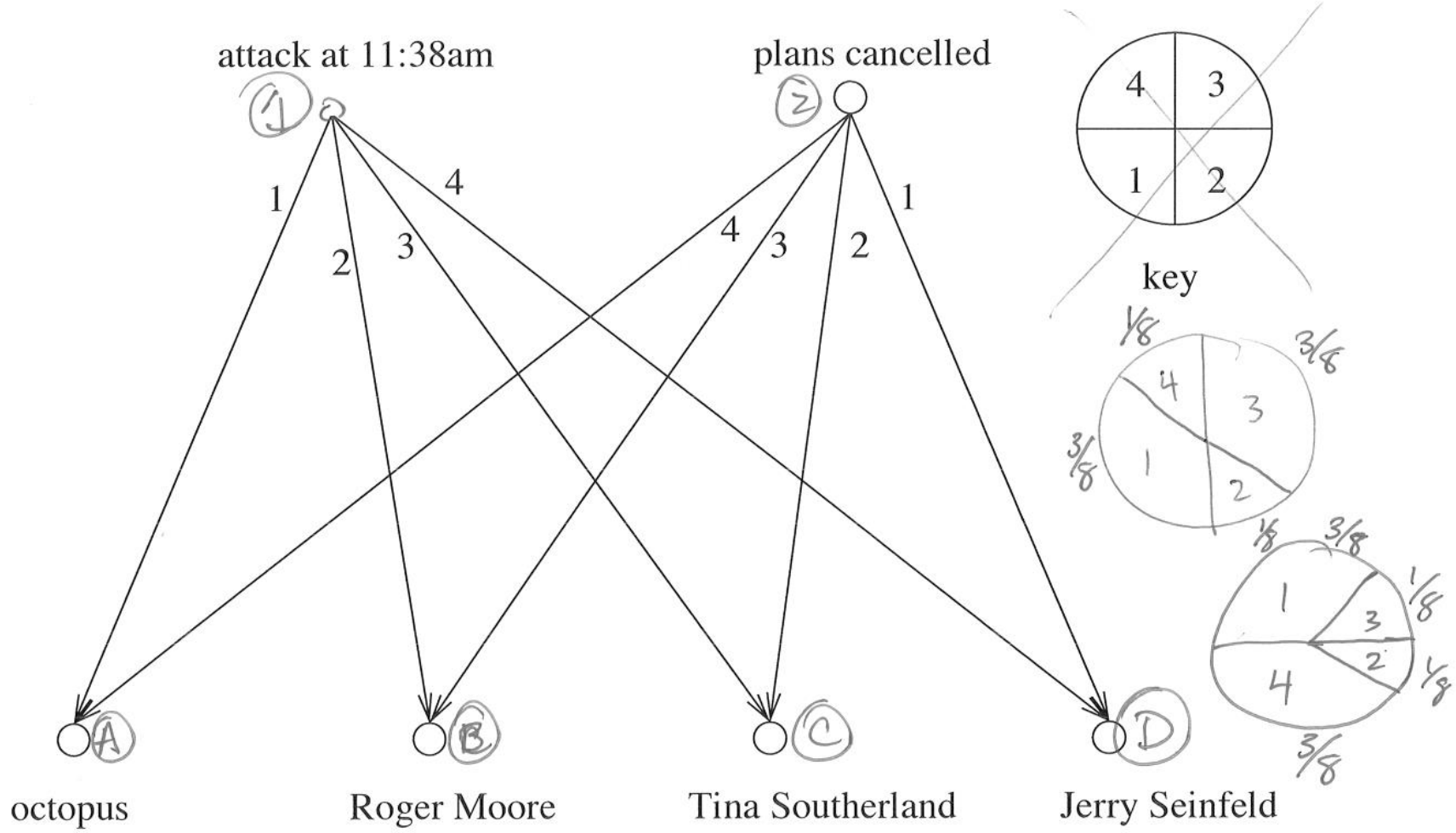
1. *All keys are equally likely*
2. *For each pair (m_i, c_j) there is a unique key, k_s, such that*

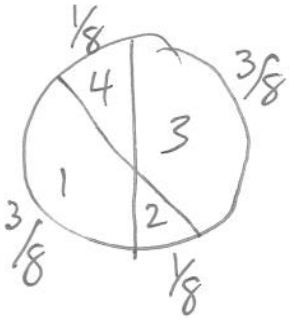
$$E_{k_s}(m_i) = c_j$$

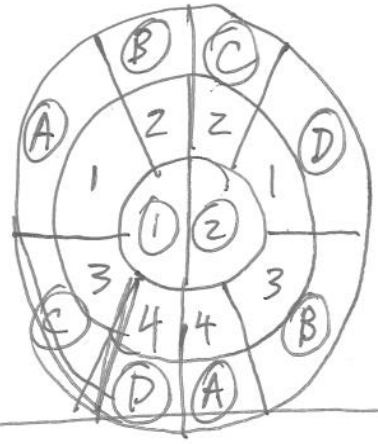
On the other hand

$$\begin{aligned} P(M = m_i, C = c_j) &= \sum_{E_{k_s}(m_i)=c_j} P(M = m_i)P(K = k_s) \\ &= P(M = m_i)\frac{1}{S} \\ &= P(M = m_i)P(C = c_j) \end{aligned}$$

$\Rightarrow$ M & C are independent.


attack at 11:38am
plans cancelled
1
2
1
2
3
4
4
3
2
1
A
B
C
D
octopus
Roger Moore
Tina Southerland
Jerry Seinfeld
key
4
3
1
2
1/8
3/8
3/8
1/8
1
3
2
4
1/8
3/8
1/8
1/8
3/8



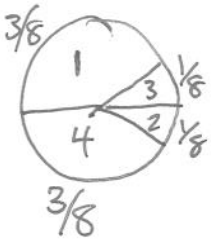


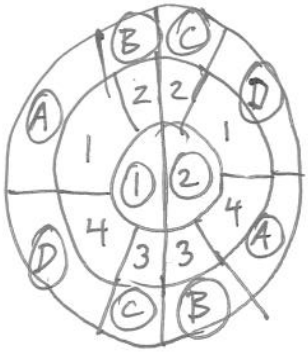
M & C

are not indep

$P(M=1 \,\&\, C=B) = 1/8 \cdot 1/2$

$P(M=2 \,\&\, C=B) = 3/8 \cdot 1/2$

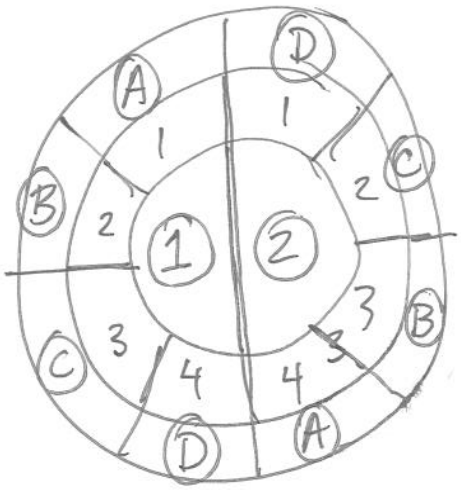


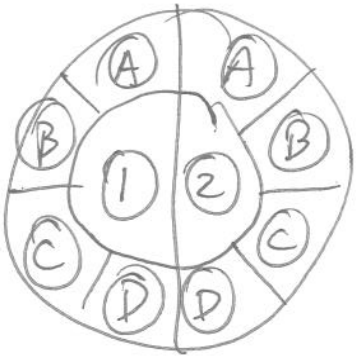


M & C are independent

$P(M=1 \,\&\, C=A) = \frac{1}{2} \cdot \frac{3}{8} = P(M=1) \cdot P(C=A)$

$P(M=1 \,\&\, C=B) = 1/2 \cdot 1/8$





Inner wheel M

middle K

outer C