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

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

by (*) there is only one term

$\Rightarrow$ we have perfect secrecy

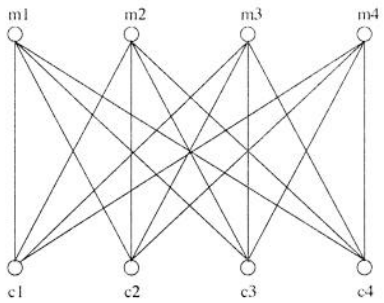
BUT there are other ways of acheiving perfect secrecy

Latin Squares

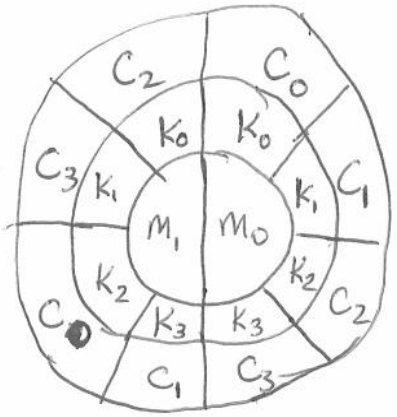
of Keys = # of Ciphers = # of Plaintexts

each ciphertext appears once in each row & each column once.

	m_1	m_2	m_3	m_4
k_1	1	2	3	4
k_2	2	3	4	1
k_3	3	4	1	2
k_4	4	1	2	3



A latin square is an $n \times n$ array where the integers 1 through n appear exactly once in each row and column.



M_i and K_j are sent to $C_{2i+j \pmod 4}$

We acheive perfect secrecy BECAUSE of the theorem.

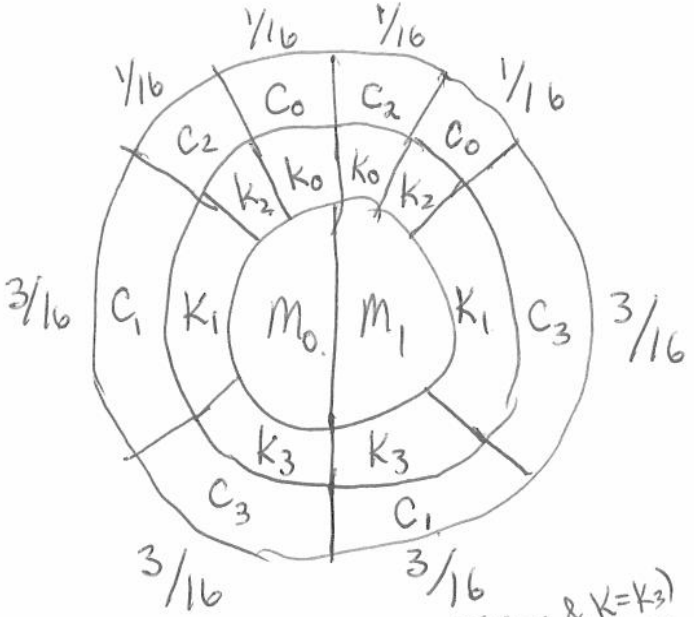
But also

$$P(M=m_i, C=c_j) = 1/8$$

$$P(M=m_i) \cdot P(C=c_j) = \frac{1}{2} \cdot \frac{1}{4} = 1/8$$

M & C are independent

$\Rightarrow$ the definition of perfect secrecy that M & C are independent.



$$P(M=m_1 \& C=c_0) = \frac{1}{16}$$
$$= P(M=m_1) \cdot P(C=c_0)$$
$$= 1/2 \cdot (1/16 + 1/16) = 1/16$$

$$P(M=m_1 \& C=c_1) = 3/16$$
$$P(M=m_1)P(C=c_1) = \frac{1}{2} \cdot 2 \cdot \frac{3}{16} = \frac{3}{16}$$

$$P(M=m_1 \& C=c_2) = 1/16$$
$$P(M=m_1)\&(C=c_2) = \frac{1}{2} \cdot \left(\frac{1}{16} + \frac{1}{16}\right) = 1/16$$

$$= P(M=m_1 \& K=k_3)$$
$$= P(M=m_1)P(K=k_3)$$
$$= 1/2 \cdot 3/8$$

$\Rightarrow$ M & C are independent

$\Rightarrow$ this system acheives perfect secrecy

2. Say that there are two equally probable messages in a certain encipherment scheme. Say also that there are 6 equally probable keys k_1-k_6 and three ciphertexts c_1, c_2, c_3. The encipherment scheme uses the following table to encrypt and decrypt.

	k_1	k_2	k_3	k_4	k_5	k_6
m_1	c_1	c_2	c_3	c_1	c_1	c_2
m_2	c_2	c_1	c_1	c_2	c_3	c_1

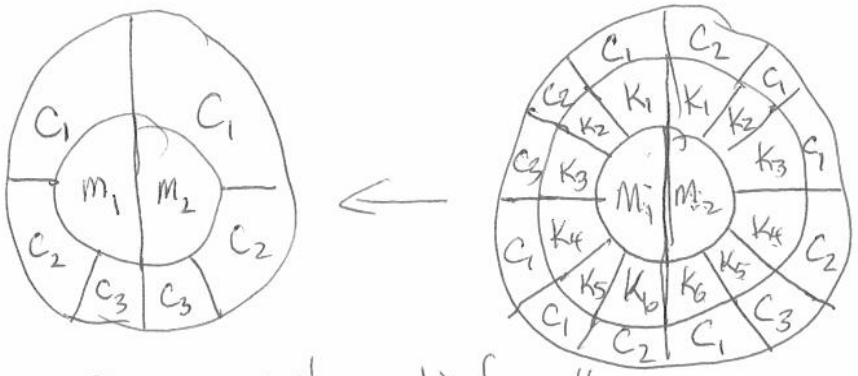
$P(C=c_1) = 1/2$
$P(C=c_2) = 1/3$
$P(C=c_3) = 1/6$

a) Calculate H(K) and H(K | C)

$H(K) = \log_2 6$

$H(C) = \frac{1}{2}\log_2 2 + \frac{1}{3}\log_2 3 + \frac{1}{6}\log_2 6$

b) Does this system achieve perfect secrecy? Why or why not?



$H(K,C) = H(C) + H(K|C)$

$=$

$\log_2 12$

$H(K|C) = \log_2 12 - \left(\frac{1}{2} + \frac{1}{3}\log_2 3 + \frac{1}{6}\log_2 6\right)$

Does not satisfy the conditions of the theorem.

We do have perfect secrecy. Because M & C are independent (see wheel to le

$a < b$

$$\gcd(a, b) = \gcd(b \bmod a, a)$$

$gcd(a, b)$ = greatest common divisor of a and b

= largest divisor of both a and b

= if d divides a and b, then d also divides $gcd(a, b)$

Example: compute $gcd(963, 657)$ $= \gcd(657, 963) = \gcd(963 \bmod 657, 657)$

$= \gcd(306, 657)$

$\frac{657}{963} = \frac{73}{107}$

$963 = 1 \cdot 657 + 306$ $\quad 306 = 963 - 657$ $= \gcd(657 \bmod 306, 306)$

$657 = 2 \cdot 306 + 45$ $\quad 45 = 657 - 2 \cdot 306$ $= \gcd(45, 306)$

$306 = 6 \cdot 45 + 36$ $\quad 36 = 306 - 6 \cdot 45$ $= \gcd(306 \bmod 45, 45)$

$45 = 1 \cdot 36 + 9$ $= \gcd(36, 45)$

$36 = 4 \cdot 9$ $= \gcd(45 \bmod 36, 36)$

$= \gcd(9, 36)$

$= 9$

Conclusion: $gcd(963, 657) = 9$

To solve:
$aX \equiv b \pmod{m}$

$$\begin{aligned} gcd(963, 657) = 9 &= -36 + 45 \\ &= -(306 - 6 \cdot 45) + 45 \\ &= -306 + 7 \cdot 45 \\ &= -306 + 7(657 - 2 \cdot 306) \\ &= -15 \cdot 306 + 7 \cdot 657 \\ &= -15(963 - 657) + 7 \cdot 657 \\ &= -15 \cdot 963 + 22 \cdot 657 \end{aligned}$$

In general we can always use these equations to write

$$gcd(a, b) = k \cdot a + \ell \cdot b$$

for some integers k and ℓ.

Example solve $127x \equiv 4 \ (mod\ 963)$ $\gcd(127, 963) = 1$

$$963 = 7 \cdot 127 + 74 \quad 74 = 963 - 7 \cdot 127$$
$$127 = 1 \cdot 74 + 53 \quad 53 = 127 - 74$$
$$74 = 1 \cdot 53 + 21 \quad 21 = 74 - 53$$
$$53 = 2 \cdot 21 + 11 \quad 11 = 53 - 2 \cdot 21$$
$$21 = 1 \cdot 11 + 10$$
$$11 = 1 \cdot 10 + 1$$

$$1 = 11 - 10 = 11 - (21 - 11) = 2 \cdot 11 - 21$$
$$= 2(53 - 2 \cdot 21) - 21 = 2 \cdot 53 - 5 \cdot 21 = 2 \cdot 53 - 5(74 - 53)$$
$$= 7 \cdot 53 - 5 \cdot 74 = 7(127 - 74) - 5 \cdot 74 = 7 \cdot 127 - 12 \cdot 74$$
$$= 7 \cdot 127 - 12(963 - 7 \cdot 127) = 91 \cdot 127 - 12 \cdot 963$$

$1 = 91 \cdot 127 - 12 \cdot 963$

$1 - 91 \cdot 127$ is a multiple of 963

$1 \equiv 91 \cdot 127 \ (mod\ 963)$

$x \equiv 1 \cdot x \equiv (91 \cdot 127) \cdot x \equiv 4 \cdot 91 \ (mod\ 963)$

Conclusion, because $91 \cdot 127 - 12 \cdot 963 = 1$,

$$91 \cdot 127 \equiv 1 \ (mod\ 963)$$

Therefore if we have

$$127x \equiv 4 \ (mod\ 963)$$

$$x \equiv 1 \cdot x \equiv 91 \cdot 127x \equiv 91 \cdot 4 \equiv 364 \ (mod\ 963)$$

Definition $a \equiv b \ (mod\ m)$ means that m divides $a - b$ or there exists a k such that $km = a - b$.

$\equiv \ (mod\ m)$ is an equivalence relation since

- $a \equiv a \ (modm)$ or m divides $a - a$. (reflexive)
- if $a \equiv b \ (mod\ m)$, then $b \equiv a \ (mod\ m)$ since if m divides $a - b$ then it divides $b - a$. (symmetric)
- if $a \equiv b \ (modm)$ and $b \equiv c \ (mod\ m)$, then $a \equiv c \ (mod\ m)$. (transitive)

Alternate definition $a \equiv b \pmod m$ if a & b have the same remainder when you divide by m.

Why? if $a = km + r$ and $b = \ell m + r$ then $a - b = km + r - \ell m - r = (k - \ell)m$

It is defined on the integers and so it can easily be shown that for any integer k,

- $a \equiv b \ (mod\ m)$ if and only if $a + k \equiv b + k \ (mod\ m)$.
- if $a \equiv b \ (mod\ m)$, then $ka \equiv kb \ (mod\ m)$.

if $ka \equiv bk \ (mod\ m)$, then sometimes $a \not\equiv b \ (mod\ m)$.
e.g. $2 \cdot 3 \equiv 2 \cdot 0 \ (mod\ 6)$, but $3 \not\equiv 0 \ (mod\ 6)$.
e.g. $4 \cdot 5 \equiv 4 \cdot 2 \ (mod\ 12)$, but $5 \not\equiv 2 \ (mod\ 12)$.

When $gcd(k, m) = 1$, if $ka \equiv kb \ (mod\ m)$, then $a \equiv b \ (mod\ m)$

Computational elements that we will use in some new cryptosystems

- Compute $a^k \ (mod\ m)$ using only squaring operations and multiplication by a.
- $gcd(a, b)$ using the Euclidean algorithm
- Find k and ℓ such that

$$ka + \ell b = gcd(a, b)$$

- If $gcd(a, m) = 1$, then there is a k such that

$$ak \equiv 1 \ (mod\ m)$$

find k & ℓ s.t.
$k \cdot a + \ell \cdot m = 1$
then $k \cdot a \equiv 1 \pmod{m}$

There is a function called the Euler 'phi' function

$\phi(n) = \#$ of integers relatively prime (i.e. $gcd(k, n) = 1$) and are between 1 and n

n	integers between 1 and n which are relatively prime	$\phi(n)$
1	1	1
2	1	1
3	1,2	2
4	1,3	2
5	1,2,3,4	4
6	1,5	2
7	1,2,3,4,5,6	6
8	1,3,5,7	4
9	1,2,4,5,7,8	6
10	1,3,7,9	4
11	1,2,3,4,5,6,7,8,9,10	10
12	1,5,7,11	4
14	1,3,5,9,11,13	6

$12 = a \qquad m = 23$

$a^{576} \pmod{23}$

$(12^{576/2})^2 \equiv (12^{288})^2 \equiv 36 \equiv 13 \pmod{23}$

$(12^{288/2})^2 \equiv (12^{144})^2 \equiv 26 \pmod{23}$

$(12^{144/2})^2 \equiv (12^{72})^2 \equiv 81 \equiv 12 \pmod{23}$

$(12^{72/2})^2 \equiv (12^{36})^2 \equiv 9 \pmod{23}$

$(12^{36/2})^2 = (12^{18})^2 \equiv 3 \pmod{23}$

$(12^{18/2})^2 = (12^{9})^2 \equiv 16 \pmod{23}$

$12^9 = 12^8 \cdot 12 \equiv 4 \pmod{23}$

$(12^{8/2})^2 = (12^4)^2 \equiv 8 \pmod{23}$

$(12^{4/2})^2 = (12^2)^2 \equiv 13 \pmod{23}$

$12^2 \equiv 6 \pmod{23}$

$23\overline{)144}$ 6 r 6, 138

169, 161

$23\overline{)96}$ 4 r 4, 92

$23\overline{)256}$ 11 r 3, 23, 3

$23\overline{)81}$ 8 r 12