$$\begin{aligned} \text{Plaintext Message Space} \quad & M = \{m_1, m_2, \dots, m_N\} \\ \text{Key Space} \quad & K = \{k_1, k_2, \dots, k_S\} \\ \text{Ciphertext Message Space} \quad & C = \{c_1, c_2, \dots, c_Q\} \end{aligned}$$

$$\boxed{c = E_k(m)}$$

The encrypting transformation using to the key k

$$\boxed{m = D_k(c)}$$

The decrypting transformation using to the key k

Two sets of probabilities

$$\boxed{\{p_1, p_2, \dots, p_N\} \text{ and } \{q_1, q_2, \dots, q_S\}}$$

Random Cryptographic Transaction

$$\text{Three random variables} \begin{cases} M = \text{the chosen plaintext} \\ K = \text{the chosen key} \\ C = \text{the resulting ciphertext} \end{cases}$$

- Sender produces a message M which is a random variable with

$$P(M = m_i) = p_i$$

- Sender selects a key K by an independent mechanism with

$$P(K = k_s) = q_s$$

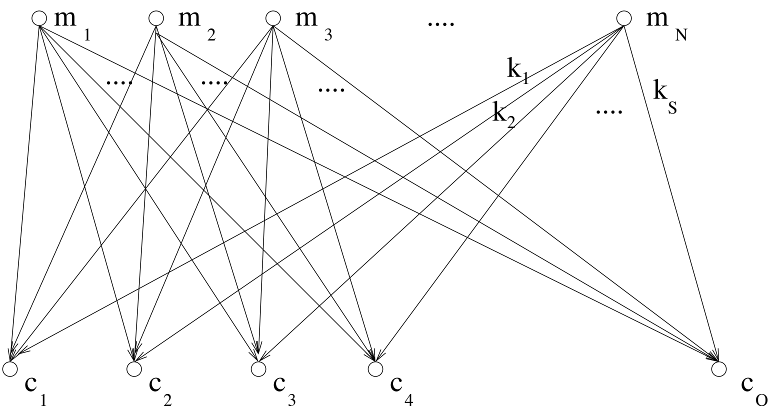
- The sender encrypts M into $C = E_K(M)$ and sends it to the intended recipient.
- Under our assumptions, the random variable C is dependent on M and K.

C yields no information about M means that M and C are independent random variables.

Definition: We say that a random cryptographic system achieves *perfect secrecy* if for all choices of $m_i \in M$ and $c_j \in C$, we have

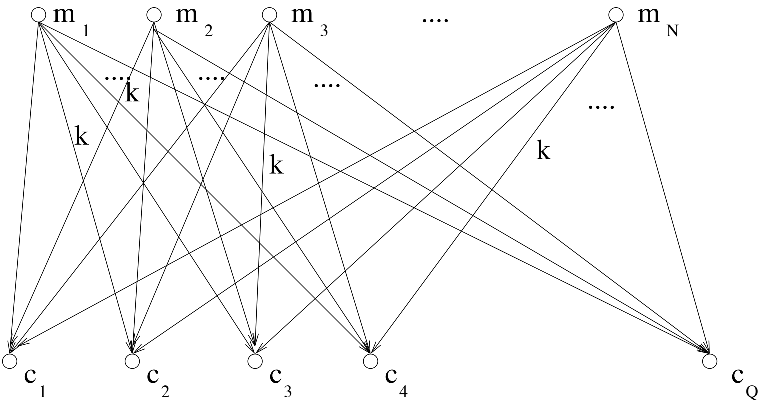
$$\boxed{P(M = m_i, C = c_j) = P(M = m_i)P(C = c_j)}$$

$$P[M = m_i, C = c_j] = P[M = m_i]P[C = c_j]$$

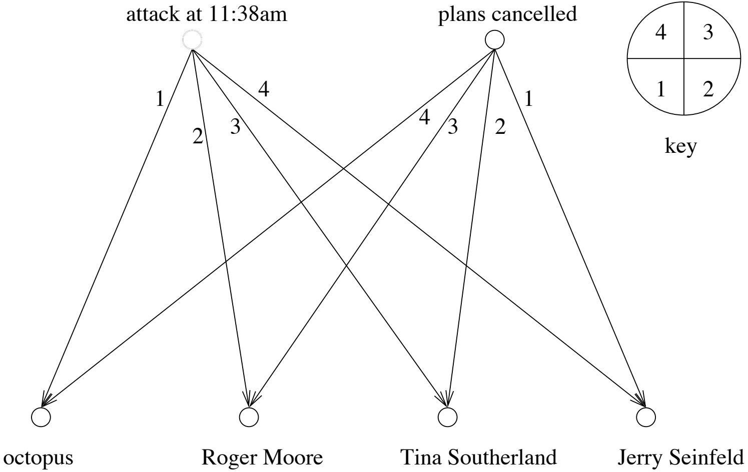


Since every message m_i must be able to be sent to every cyphertext c_j (since M and C are independent), it must be that the number of keys is larger than or equal to the number of cyphertexts.

$$P[M = m_i, C = c_j] = P[M = m_i]P[C = c_j]$$



Since if we fix a key k we see every message is sent to a different cyphertext we must have that the number of cyphertexts is larger or equal to the number of plaintexts.


attack at 11:38am
plans cancelled
4
3
1
2
key
1
2
3
4
4
3
2
1
octopus
Roger Moore
Tina Southerland
Jerry Seinfeld

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*

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

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*

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

Proof.

$$P(C = c_j) = \sum_{i=1}^{N} P(M = m_i) \sum_{E_{k_s}(m_i)=c_j} P(K = k_s)$$

But if there is only one key k_s yielding $E_{k_s}(mi) = c_j$ then the inner sum reduces to a single term, and if all keys are equally likely then $P(K = k_s) = 1/S$

$$P(C = c_j) = \sum_{i=1}^{N} P(M = m_i)\frac{1}{S} = \frac{1}{S}$$

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*

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

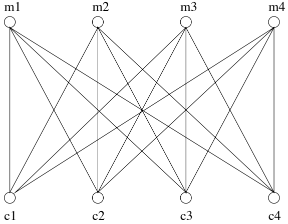
On the other hand

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

Latin Squares

$$\boxed{\#\text{ of Keys} = \#\text{ of Ciphers} = \#\text{ of Plaintexts}}$$

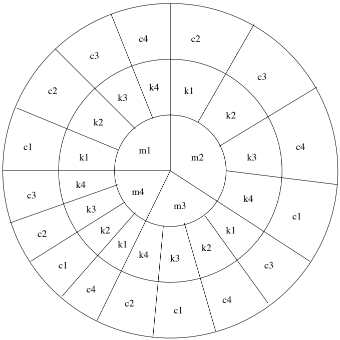
$$\begin{array}{c|cccc} & m_1 & m_2 & m_3 & m_4 \\ \hline k_1 & 1 & 2 & 3 & 4 \\ k_2 & 2 & 3 & 4 & 1 \\ k_3 & 3 & 4 & 1 & 2 \\ k_4 & 4 & 1 & 2 & 3 \end{array}$$



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

Latin Squares

$$\boxed{\text{\# of Keys} = \text{\# of Ciphers} = \text{\# of Plaintexts}}$$



$$\begin{array}{c|cccc} & m_1 & m_2 & m_3 & m_4 \\ \hline k_1 & 1 & 2 & 3 & 4 \\ k_2 & 2 & 3 & 4 & 1 \\ k_3 & 3 & 4 & 1 & 2 \\ k_4 & 4 & 1 & 2 & 3 \end{array}$$

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

One Time Pad

A "one time pad system" is one in which we encrypt a message with N letters by means of N random integer keys

$$k_1, k_2, \ldots, k_N$$

in the range $0 \ldots 25$ with each of these possibilities equally likely. The i^{th} letter of the message is encrypted by the Caesar substitution C_{k_i} (in other words the i^{th} letter is Caesar k_i-shifted). The vector

$$(k_1, k_2, \ldots, k_N)$$

is called the *key stream*.

Theorem

The one time pad system achieves perfect secrecy.

Proof. It is easy to see that given any cipher

$$c = Y_1 Y_2 \cdots Y_N$$

and message

$$m = X_1 X_2 \cdots X_N$$

there is one and only one key stream

$$(k_1, k_2, ..., k_N)$$

such that

$$Y_i = X_i + k_i \mod 26.$$

Since all keys are equally likely we have the conditions of the previous theorem are satisfied.