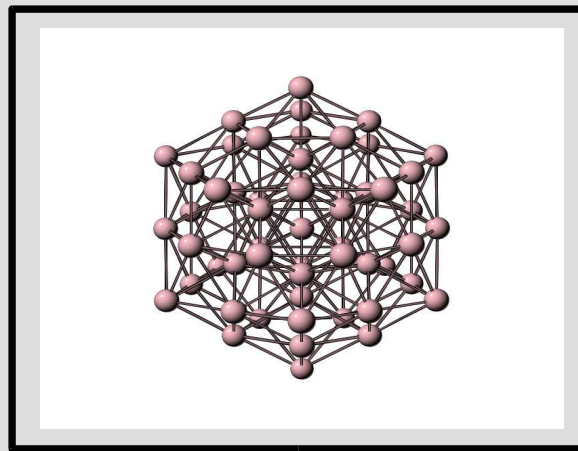


Redes libres

*Cada nodo un servidor;
Cada servidor un nodo ...*



David Gascón Cabrejas <483969@unizar.es>

Transparencias Liberadas bajo licencia GNU FDL

http://www.laotracara.com/redes_libres

Redes libres

- **Conceptos previos**
 - **Conexiones**
 - **Transmisión de la información**
 - **Estado de la información a nivel global**
 - **Anonimato**
 - **Privacidad de la información**
 - **Censura en la red**

Redes libres

- **Conexiones**

- **Directas**

- Se establecen entre 2 nodos, los cuales conocen la información necesaria para conectar con su 'par'

- IP + Puerto 155.210.100.100 : 80

- **Indirectas** (Topologías: anillo, chord, grid ...)

- La idea es poder establecer una conexión virtual entre A y C a través de B, de forma que A se conecta con B, y C se conecta con B (ambas conexiones de forma directa)

- Hay que pensar en entornos limitados (NAT, Firewall ...)

Redes libres

- **Transmisión de la información**

- Relegar en protocolos de transporte (TCP/IP , UDP/IP ...)
 - Modelo habitual de comunicación en Internet
- Crear rutas estáticas
 - El nodo inicial tiene que conocer a priori las posibles rutas, y en cada paquete mandar la información necesaria para llegar al destino
 - Popenet [<http://www.eskimo.com/~weidai/popenet.txt>]
- Crear rutas dinámicas partiendo de unas determinadas reglas
 - Gnutella , Mute ...

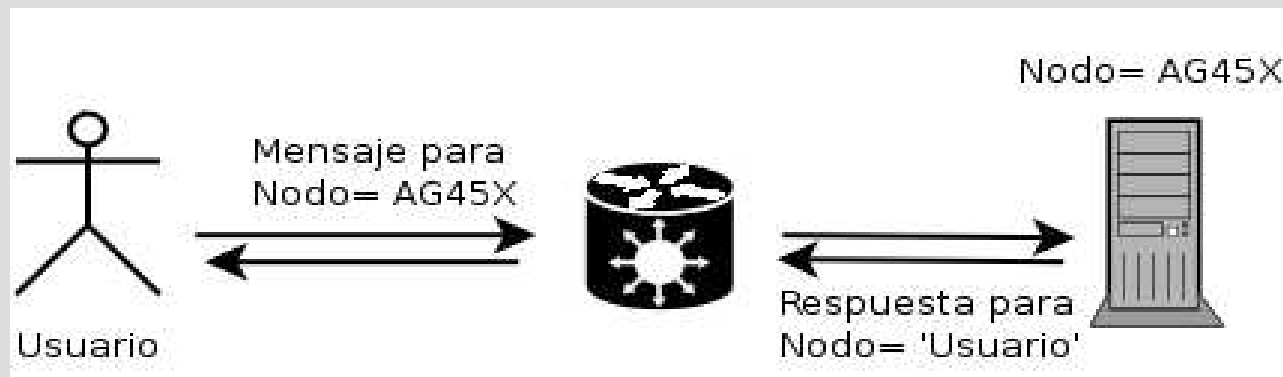
Redes libres

- **Estado de la información a nivel global**
 - Identificación (¿ cómo accedemos al contenido ?)
 - Duplicación (¿ de qué fuentes puedo conseguirla ?)
 - Cifrado
 - Distribución
 - modelos geográficos
 - balanceo de carga
 - Red como sistema de ficheros virtual (Freenet , Gnunet)

Redes libres

- **Anonimato**

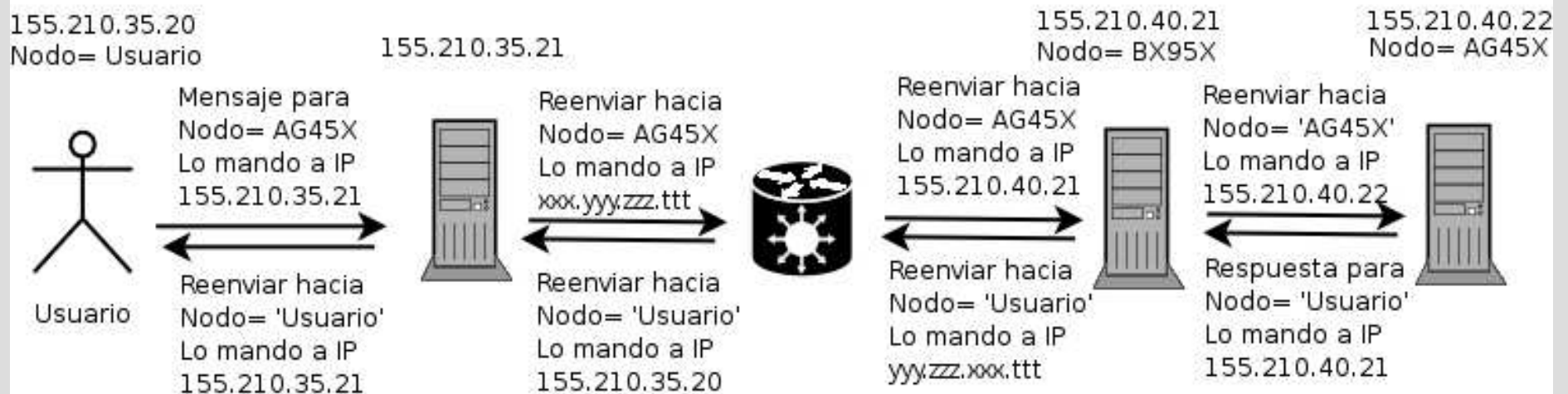
- Nosotros conocemos los datos de red (IP + Puerto) de los nodos 'vecinos' que son los que mantenemos una conexión directa, sin embargo sólo conocemos un Identificador del nodo destino; por lo que yo mando un mensaje al nodo vecino con destino el Identificador del nodo final



Redes libres

- **Anonimato**

- La idea es que cada nodo se comporte como un servidor, de forma que además de ocuparnos de nuestras conexiones lo hagamos de las de los demás, reenviando en el caso de que nosotros no seamos el nodo destino



Redes libres

- **Anonimato**

- De esta forma nunca conoceremos de quien estamos obteniendo la información; y lo que es mejor
 - nunca podrán saber que compartimos !!
- Pero ... y si tuviéramos 'pinchada' la línea de comunicaciones ?
 - Tampoco, porque la información se manda **CIFRADA**
 - Además hay algoritmos de transmisión que incluyen el enviar paquetes con información aleatoria para que no sea fácil si quiera monitorizar una tasa de envío

Redes libres

- **Cifrado**

- Cifrado directo entre nodo inicial y final

- Ejemplo

- Nodo A tiene Clave Pública de B: C_{PB}

- Nodo B tiene Clave Secreta de B: C_{SB}

- A consigue mensaje cifrado C_{SB} (Mensaje)

- Pero puede descifrarlo con la clave pública

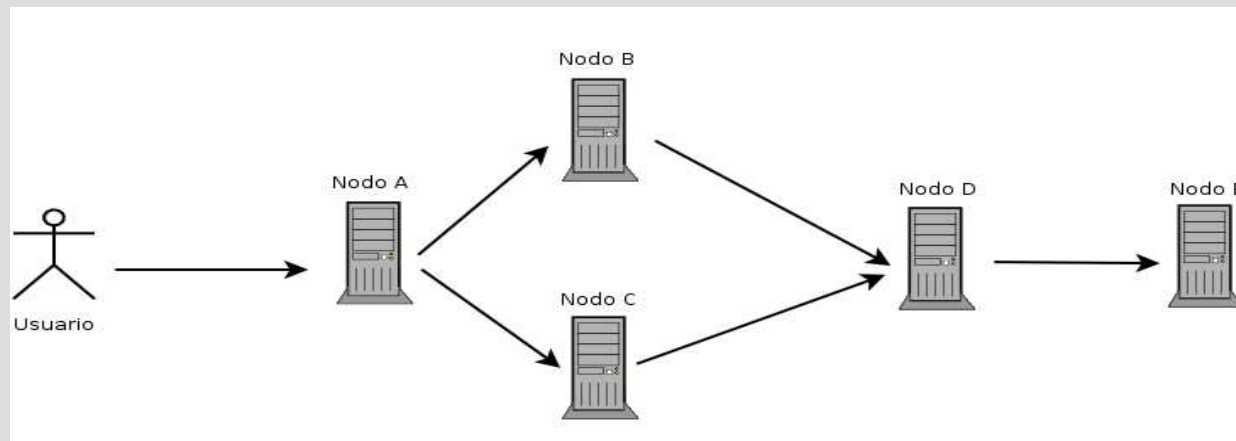
- $D_{PB}(C_{SB}(\text{Mensaje})) == \text{Mensaje}$

- Es utilizado por la mayoría de aplicaciones P2P

Redes libres

- **Cifrado**

- Cifrado múltiple entre nodo inicial y final
 - Es el método usado por redes de confianza
 - Posee anonimato asíncrono
 - Nodo Inicial conoce las posibles Rutas



Redes libres

- **Cifrado**

- Caminos

- A -> B -> D -> E

- Usuario manda : $C_A(C_B(C_D(C_E(\text{Mensaje}))))$

- A -> C -> D -> E

- Usuario manda : $C_A(C_C(C_D(C_E(\text{Mensaje}))))$

- Cada nodo aplica su clave para descifrado y reenvía

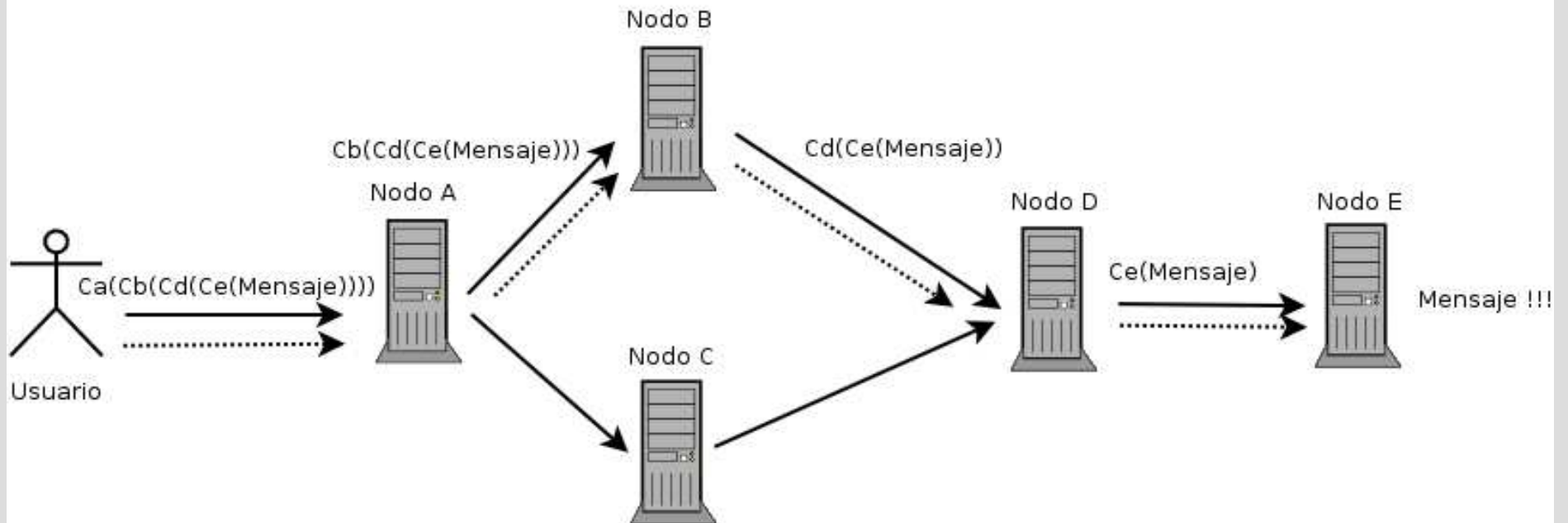
- $D_A(C_A(C_C(C_D(C_E(\text{Mensaje})))))) = C_C(C_D(C_E(\text{Mensaje}))) + @ \text{ Nodo C}$

- Como se puede observar lo que obtiene el nodo A al descifrar es el mensaje cifrado para el nodo C e información sobre el Nodo C

Redes libres

- **Cifrado**

- Como se puede ver el nodo inicial conoce la ruta y las claves de los nodos intermedios



Redes libres

- **Cifrado**

- Con este modelo de cifrado múltiple nos aseguramos de 2 cosas
 - sólo un nodo que contenga la clave secreta que 'toca' en ese momento puede conocer cual es el siguiente destino
 - sólo se podrá ver el mensaje si hemos realizado el camino completo

Redes libres

- **Censura en la red**

- ¿ La finalidad de esta charla es que podamos seguir publicando y consiguiendo todo tipo de información de la red ?

- **Por supuesto**

- ¿ Es cierto que aquí se exponen métodos para evitar ser contactados por entidades como la SGAE?

- **Sín duda**

- El intercambio libre de información es lo que se intenta promover , evitando cualquier tipo de censura previa

Redes libres

- **GNUTELLA**

- <http://www.gnutella.com/>
- Sistema distribuido de conexiones directas
- Permite las descargas simultáneas desde varios nodos
- Comienza la conexión con la red mediante:
 - Listas iniciales de nodos activos, web, IRC ...
 - Cuando contacta con un nodo le pide la lista de nodos que él conoce, y vuelve a empezar el proceso hasta que llega a una determinada cuota



Redes libres

- **GNUTELLA**

- Transmisión de la Información:

- Cada nodo reenvía a sus conexiones con otros nodos las búsquedas que le llegan (broadcast)
 - Esta expansión en forma de árbol entrelazado hace de la red Gnutella un sistema completamente descentralizado
 - Una vez que uno o varios nodos responden afirmativamente al usuario que inició la búsqueda , se establece una conexión directa entre ellos de forma que la descarga del fichero se hace de la forma más eficiente posible

Redes libres

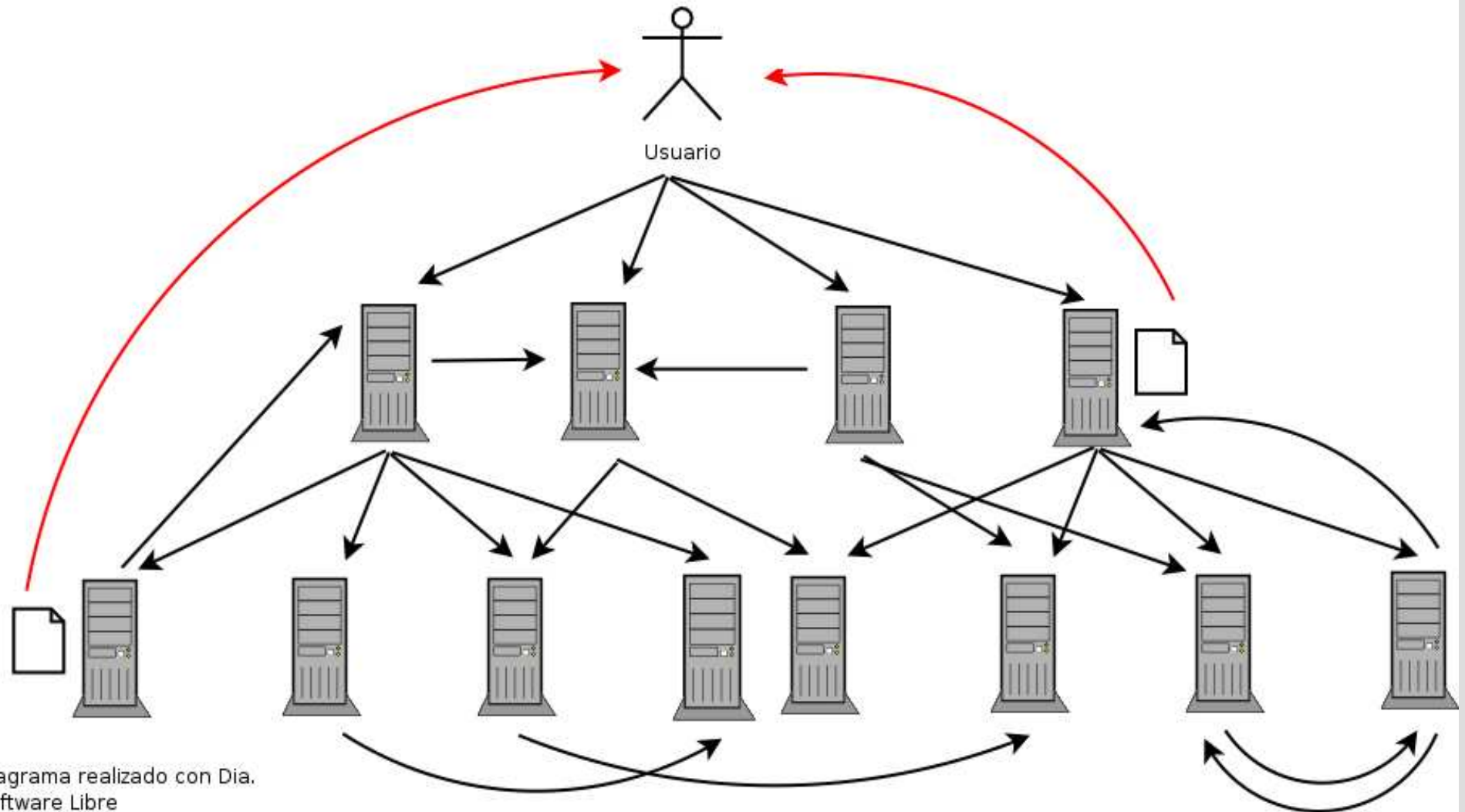


Diagrama realizado con Dia.
Software Libre
Autor: David Gascon

Redes libres

- **MUTE**

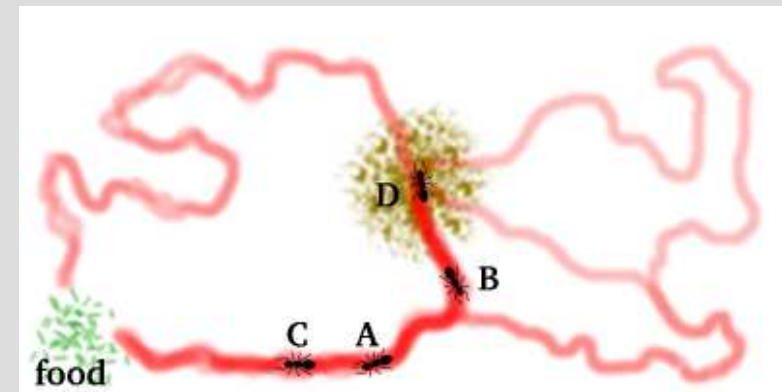
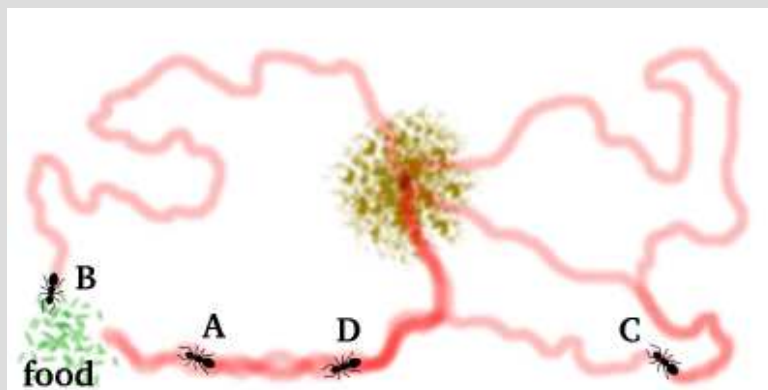
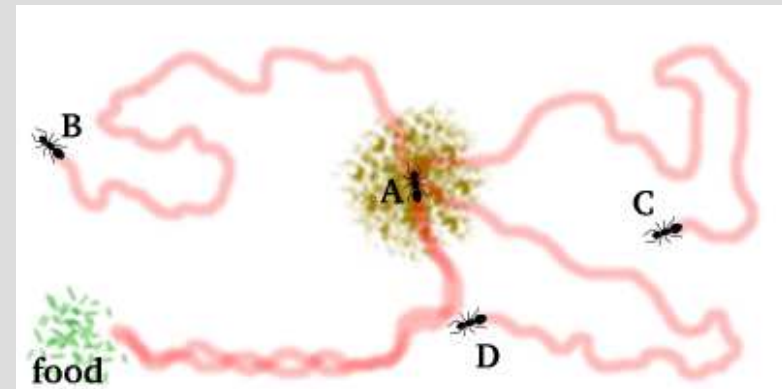
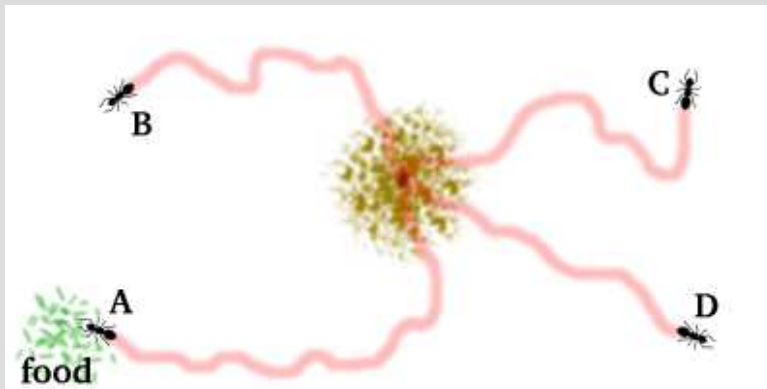
- <http://mute-net.sourceforge.net>
- Sistema distribuido, anónimo, cifrado
- Técnicas de enrutamiento basadas en el comportamiento de colonias de hormigas
- Uso de IP's virtuales; comunicación indirecta
- Creación de canales de transmisión inteligentes y con memoria
- La transmisión sigue siendo P2P, pero a través de la comunidad de usuarios



Redes libres

- **MUTE**

- Algoritmo de enrutamiento basado en hormigas



Redes libres

- **MUTE**

- Los nodos memorizan el número de paquetes que pasa con origen María y destine Luisma
- Poco a poco el camino A - B - F va acumulando un número mayor de transiciones por lo que se torna como el camino óptimo de enrutado
- A Luisma solo le llegan resultados del nodo A
- No sabe de donde viene la información (no conoce la existencia de María == Red Anónima !!)

Redes libres

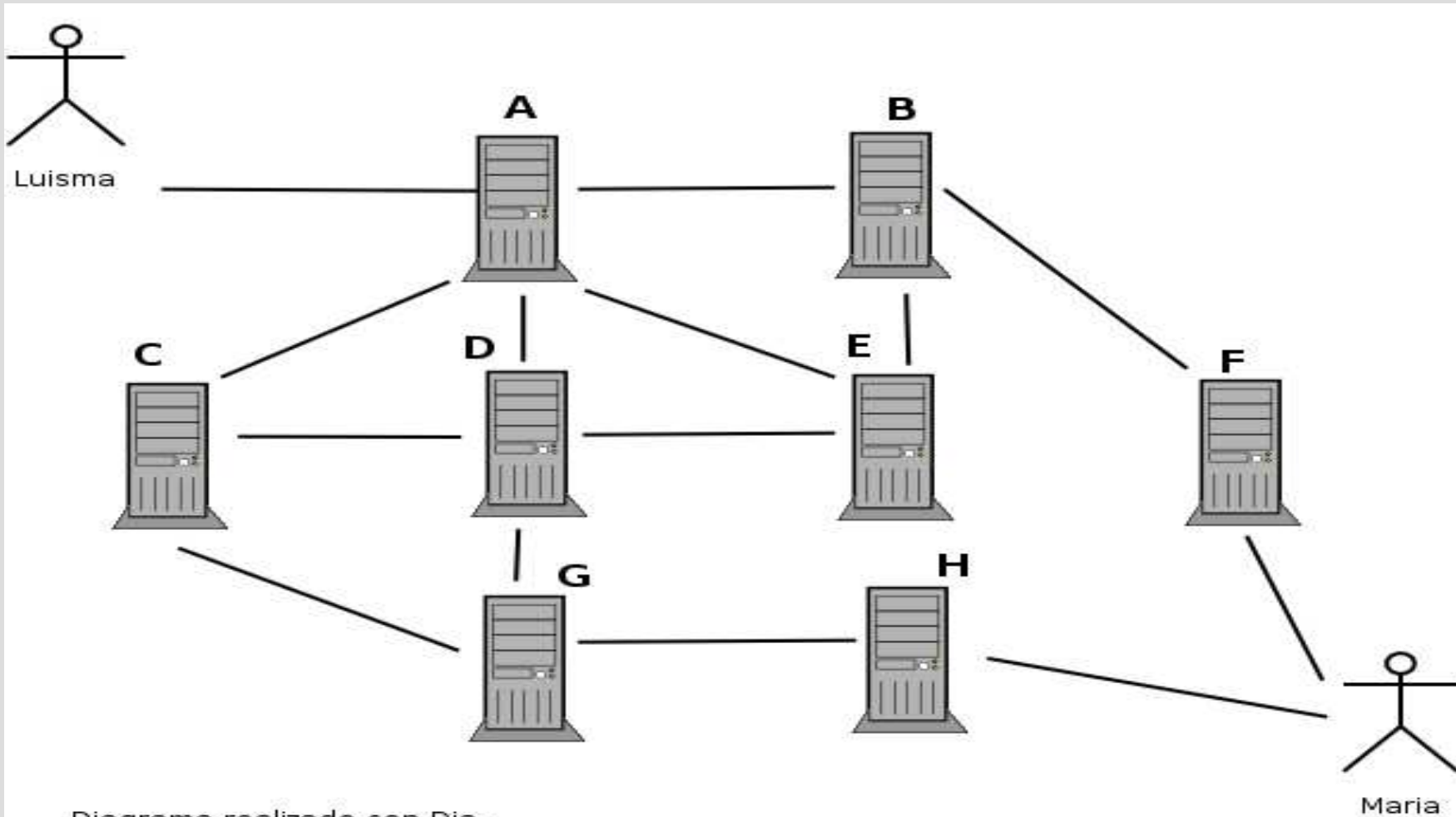
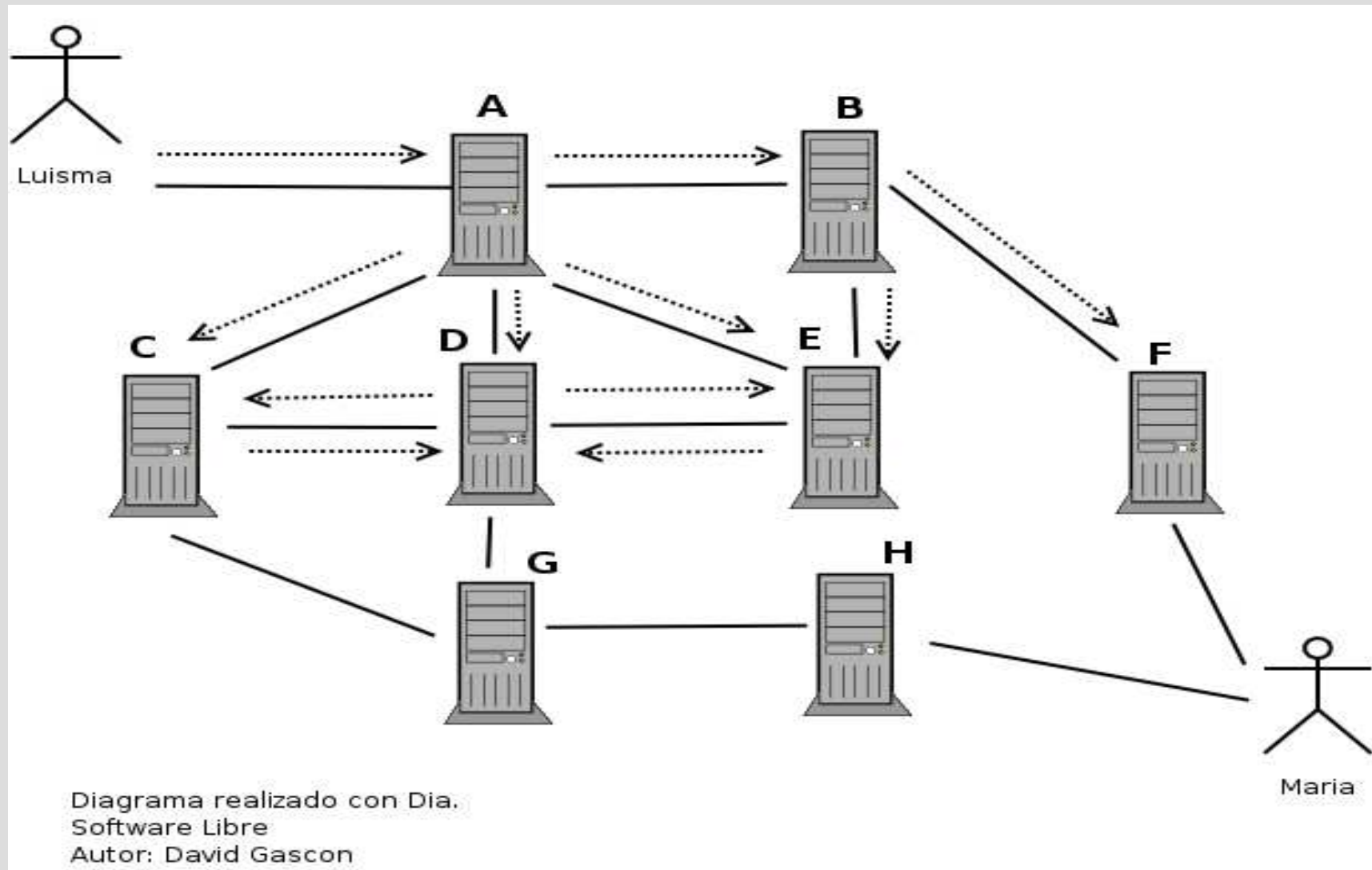


Diagrama realizado con Dia.
Software Libre
Autor: David Gascon

Redes libres



Redes libres

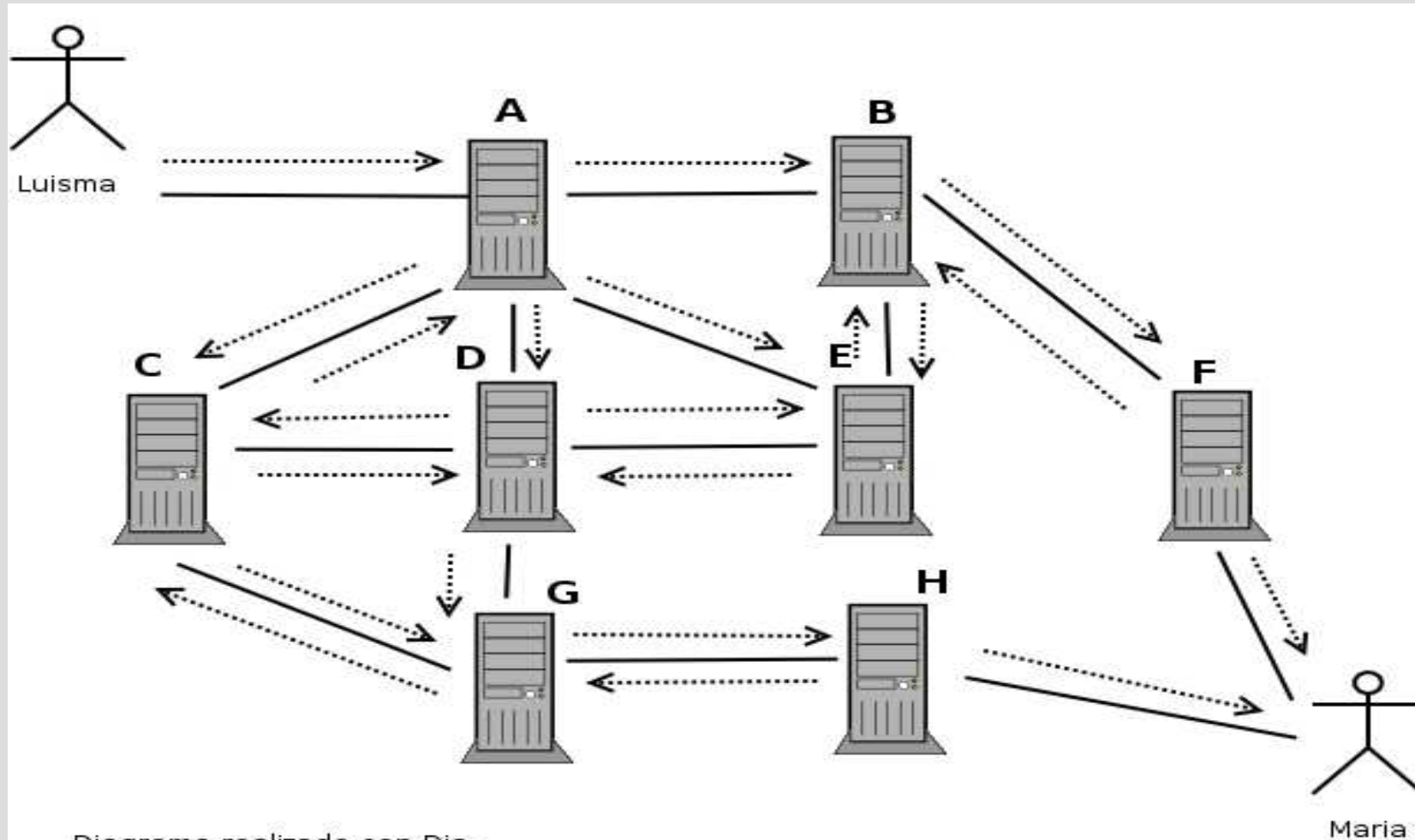


Diagrama realizado con Dia.
Software Libre
Autor: David Gascon

Redes libres

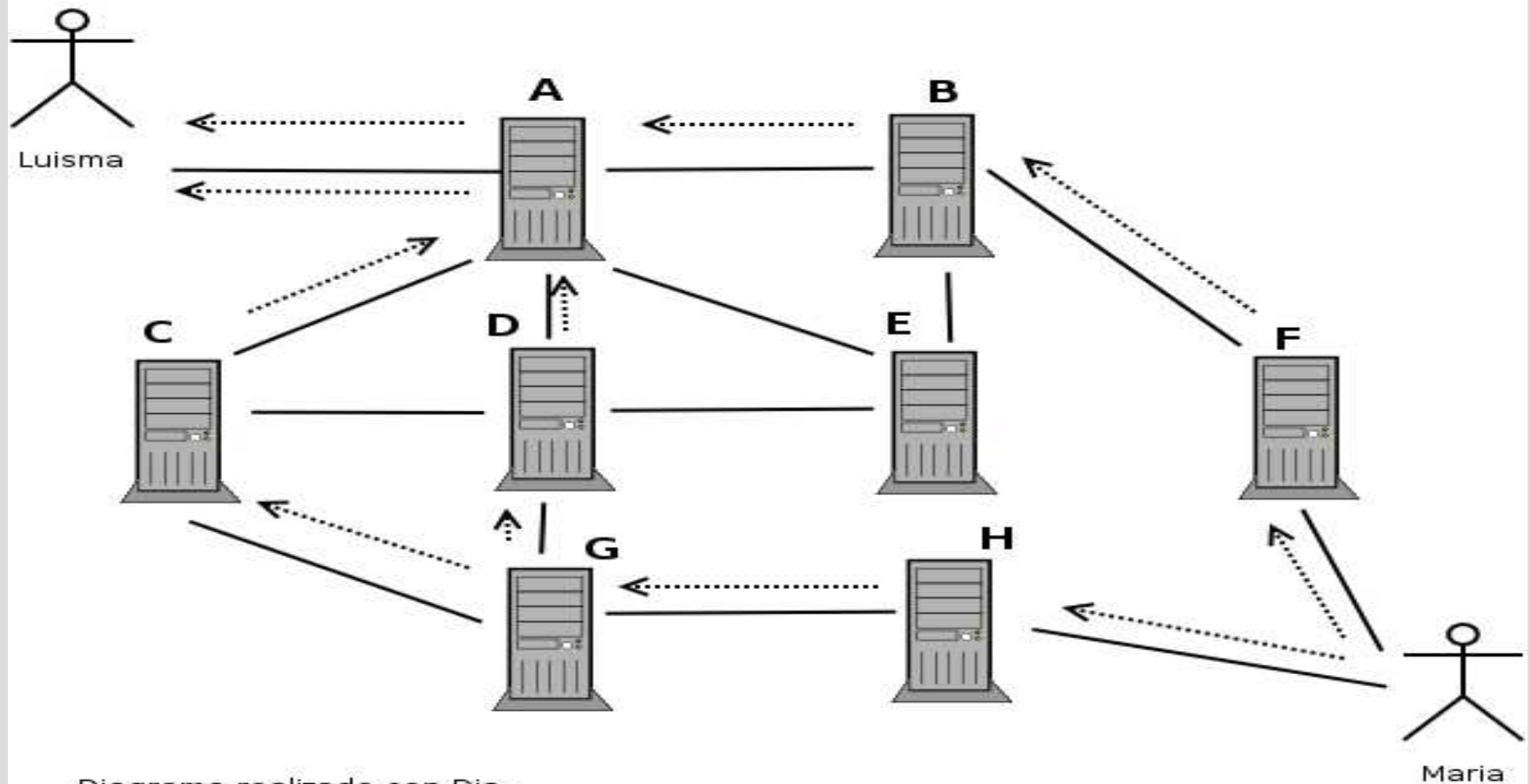


Diagrama realizado con Dia.
Software Libre
Autor: David Gascon

Redes libres



- **FreeNet**

- <http://www.freenetproject.org/>
- Nace como un modelo contra la censura a la que podemos ser sometidos hoy por hoy en internet
 - “ *she will come to me and say 'Daddy, where were you when they took freedom of the press away from the Internet?'* ”
- Se utiliza en países que se practica la censura como China
- La información vive en la Red
 - Los nodos se encargan de mantener un sistema de información que se mantiene si es requerida por los usuarios

Redes libres

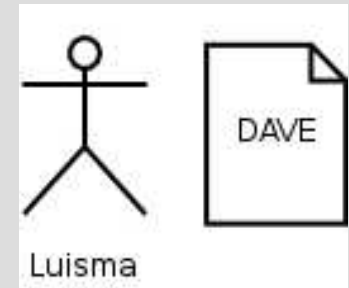
- **FreeNet**

- La idea principal del cifrado de la información no es su ocultación, sino el evitar que pueda ser censurada
- Nadie sabe que está compartiendo
- Nadie sabe a donde va la información que manda
- Pensemos en un gran sistema de ficheros virtual
- Algoritmos de enrutamiento inteligentes
 - varían según carga, latencia ... de los nodos que lo componen

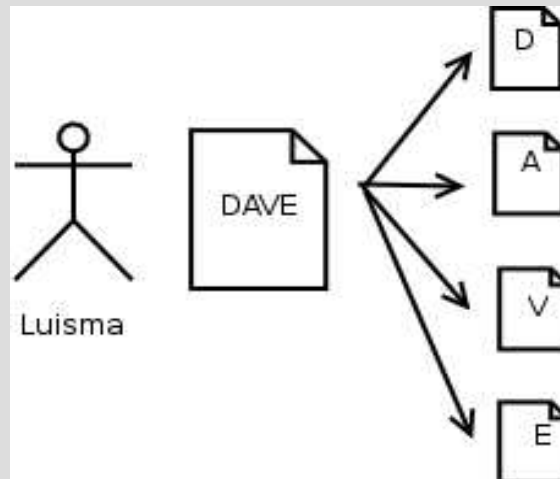
Redes libres

- **FreeNet**

- Inicialmente un usuario decide “publicar” un fichero



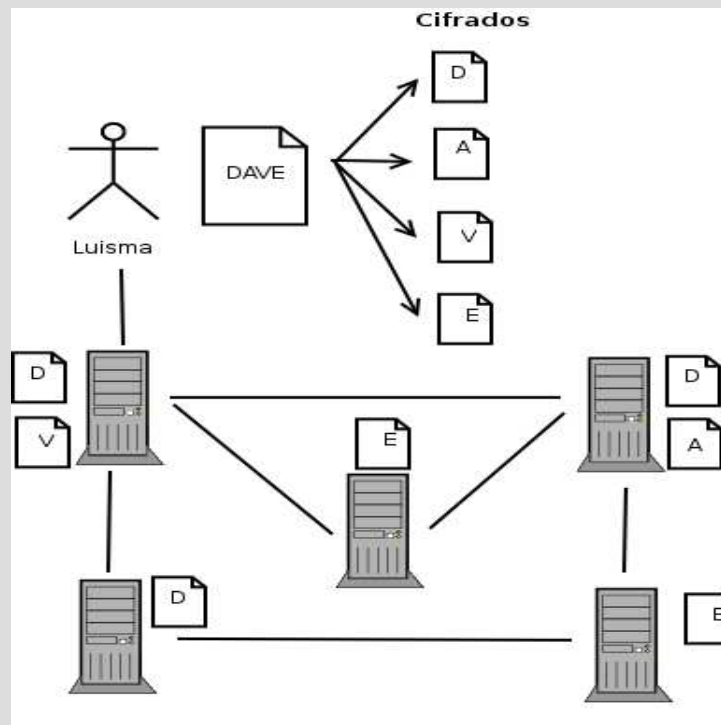
Antes de mandarlo lo parte en trozos y lo cifra



Redes libres

- **FreeNet**

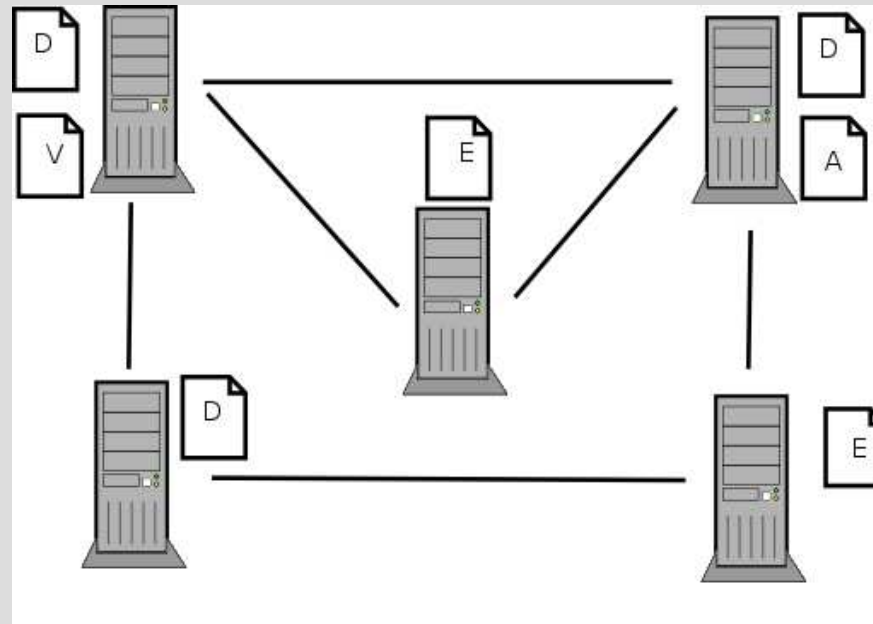
- Al publicarlo los otros nodos ya existentes en la red deciden compartirlo con otros nodos que “conocen”



Redes libres

- **FreeNet**

- Una vez publicado el fichero aunque el usuario inicial abandone la red, la información sigue existiendo en la red (cifrada ...)



Redes libres

- **GNUNET**

- <http://gnunet.org/>
- Se basa en la metodología usada para Freenet
- Introduce cambios en el sistema de almacenamiento global de la información
- Sistema de créditos: “los nodos generosos son recompensados”
- Más que un sistema de P2P
 - Posible modelo futuro de WWW
 - Información 100% distribuida ,anónima y cifrada



Redes libres

- **GNUNET**

- Codificación de la información:

- Cada fichero de datos es partido en bloques de 1 KB llamados DBlocks

- Estos DBlocks son identificados mediante una estructura formada por índices de todos ellos: IBlock

- Cada índice es resultado de aplicar una función de Hashing (H) sobre el valor del bloque:

- $I_i == H(B_i)$

Redes libres

- **GNUNET**

- Codificación de la información:

- Por lo que es fácil ver la composición total del bloque de Índices IBlock $(B) = H(B_0) + \dots + H(B_i) + \dots + H(B_{n-1})$

- Los bloques de datos se cifran usando el índice propio de cada bloque: $(H(B_i))$

- Cifrado $B = C_{H(B_i)}(B_i)$

- Y se identifican mediante su hashing: $H(C_{H(B_i)}(B_i))$

Redes libres

- **GNUNET**

- Codificación de la información:

- $I_{\text{Block_completo}} = (H(B_i), H(C_{H(B_i)}(B_i))) (i = 0 .. n-1) + \text{CRC}$

- Nos da la “@” de donde se encuentra cada bloque

- Y la clave que necesitaremos para descifrarlo

- Lo tratamos como un bloque más, por lo que lo ciframos e indexamos:

- Cifrado: $C(I_{H(I)})$

- Hashing: $H(H(I))$

Redes libres

- **GNUNET**

- Codificación de la información:

- RBlock

- Contiene la información necesaria para acceder al bloque de Índices == $H(H(I))$ y para descifrarlo: $H(I)$

- También tiene Metainformación

- palabras clave (k_i)

- comentarios

- Cifrado: $C_{k_i}(\text{Rblock})$

última indexación
↔

$H(H(H(k_i)))$

- Hashing: $H(H(k_i))$

Redes libres

- **GNUNET**

- Codificación de la información:

- ¿ Qué tiene que conocer el usuario para acceder a los datos?
 - únicamente las palabras que definen a ese fichero
 - ej: busquemos estas transparencias por la red bajo el nombre de *“Redes libres: Nueva generación de P2P”*
 - Como ya hemos dicho son las mismas palabras las claves usadas para cifrar la información del RBlock, que nos llevará al IBlock, y finalmente a los DBlock

Redes libres

11

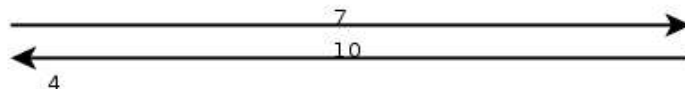
DBlock descifrado con $H(Bi)$

IBlock descifrado con $H(I)$

$I\text{Block} = \{H(Bi), H(C(H(Bi), Bi)) [i = 0 .. n-1]\}$

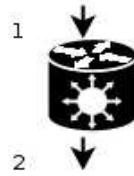


Usuario

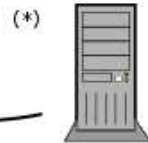


RBlock descifrado con $H(Ki)$
 $R\text{Block} = \{ H(H(I\text{Block})), H(I) \}$

$Ki == \text{"Red libre"}$
 $H(H(H(ki)))$



$H(H(H(ki))) = \{ (H(H(Ki))), C(H(ki)(R\text{Block})) \}$



(*)
 Se usa para comprobar que el nodo que nos envia la informacion no es un suplantador.

$H(H(I\text{Block})) = \{ C(H(I)I\text{Block}) \}$



8

$H(C(H(Bi), Bi))$



Bloques Cifrados



Bloques Cifrados



Bloques Cifrados

$C(H(Bi)(B(i)))$

9

Diagrama realizado con Dia.
 Software Libre
 Autor: David Gascon

Redes libres

- **Otras aplicaciones**

- **Mnet**

- Para comenzar: buscar el nodos iniciales ([http ...](http://...))
 - Usa el sistema de ficheros virtuales 'globales'
 - Preparado para lidiar con problemas como
 - NAT's
 - Firewalls
 - Gracias a la posibilidad de activar 'relay servers' que permiten conexiones indirectas



Redes libres

- **Otras aplicaciones**

- **Entropy** [<http://entropy.stop1984.com>]



- Facilita la publicación de contenido navegable haciendo de cada nodo un servidor web

- **I2P** [<http://www.i2p.net>]



- Posibilidad de concretar la creación de túneles
 - Garlic Routing : similar a la técnica de cifrado múltiple pero con mayores posibilidades de abstracción
 - Permite crear pasarelas para conseguir por ejemplo Bittorrent Anónimo
 - <http://www.gotroot.com/article/195>

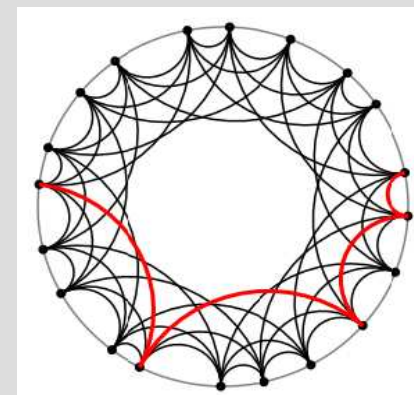
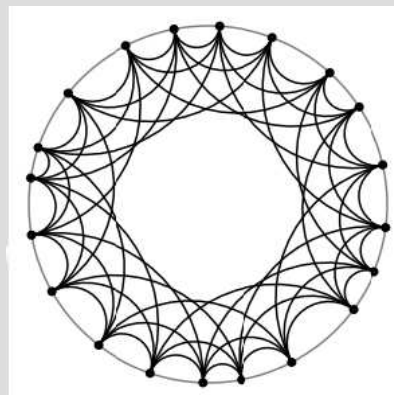
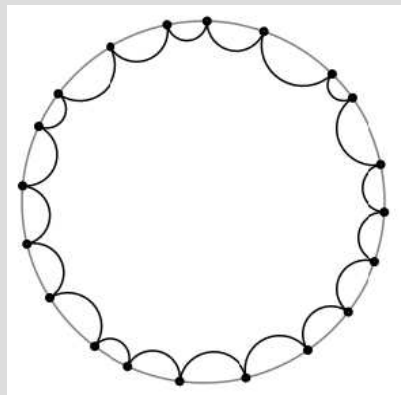
Redes libres

- **Otras aplicaciones**

- **The Circle** [<http://thecircle.org.au>]



- Crear redes en forma de anillo con vínculos a los nodos de forma que se puedan crear distintas rutas alternativas
 - Distribuir los ficheros mediante una tabla Hash global
 - Transmisión UDP !! (buen modelo para redes fiables ...)



Redes libres

- **Otras aplicaciones**



- **Ants**

- <http://www.myjavaserver.com/~gwren/home.jsp?page=custom&xmlName=ants>
 - Similar a MUTE
 - Con nuevas metodologías de enrutamiento
 - Se basa en UDP/IP mientras que MUTE es TCP/IP

- **JAP** (Java Anonymity & Privacy)



- <http://anon.inf.tu-dresden.de/>
 - No es totalmente distribuido
 - Ni convencen las razones por la que lo expone

Redes libres

- **Otras aplicaciones**

- **Pastry** [<http://freepastry.rice.edu/>]

- Introduce el principio de **Localidad** de los nodos
 - Todos con todos en $\text{Log}(n)$ pasos !

- **Eternity** [<http://www.cypherspace.org/adam/eternity/>]

- Importante debido a que es modelo perfilado tecnológica y políticamente
 - Se ocupa de plantear un modelo de almacenamiento mundial y sostenible con el sistema de mercado actual

Redes libres

- **Otras aplicaciones**

- **Publius** [<http://www.cs.nyu.edu/~waldman/publius/>]

- Modelo de publicación web distribuida
 - URL's cifradas

- **Taz Servers & The Rewebber Network**

- [http://www.firstmonday.dk/issues/issue3_4/goldberg/index.html]

- TAZ = Temporary Autonomous Zone
 - Cifrado doble
 - Basado en servidores 'Mixers'

Redes libres

- **Otras aplicaciones**

- **Anonymizer** [<http://www.anonymizer.com>]

- Proxy Cache

- Una trampa (consciente o inconscientemente)

- **Swarming** [<http://onionnetworks.com/technology/swarming/>]

- Formas de distribuir la carga en un Grid ...

- Intentan patentar ideas que se llevan usando desde hace bastante tiempo en los estudios de balanceo de carga ...

Redes libres

- **Otras aplicaciones**

- **Onion Routing** [<http://www.onion-router.net/>]
- **TOR** [<http://tor.eff.org/>]
- **Tarzan** [<http://www.pdos.lcs.mit.edu/tarzan/index.html>]
 - Hashing de IP's cifradas como ID del anillo
 - Usa el modelo de topología Chord

Redes libres

- **Otras aplicaciones**

- **Free Heaven** [<http://www.freehaven.net>]

- Tiene implementado un sistema de 'micropagos' de forma que los nodos que más aportan son los que más pueden aprovechar la red
 - Distribuye los ficheros de forma que se necesitan sólo 'k' de los 'n' trozos para poder reconstruir el fichero

- **Mojo Nation** [<http://advogato.org/proj/Mojo%20Nation/>]

- Los créditos que se generan son globales no importa en nodo que los use (se pueden 'vender entre nodos')

Redes libres

- **Otras aplicaciones**

- **Freedom**

- <http://osiris.978.org/~brianr/crypto-research/anon/www.freedom.net/products/whitepapers>

- Buen modelo de tratamiento de las conexiones entrantes y salientes en los nodos para conseguir anonimato y privacidad en la red

- **Morphmix** [<http://www.tik.ee.ethz.ch/~morphmix/>]

- Introduce conceptos interesantes como la distinción entre conexiones anónimas y túneles anónimos entre nodos

Redes libres

- **Otras aplicaciones**

- **Piazza** [<http://data.cs.washington.edu/p2p/piazza/>]

- **Mysternetworks** [<http://www.mysternetworks.com/>]

- **Nodezilla** [<http://nodezilla.cjb.net/>]

- **Sip** [<http://www.research.earthlink.net/p2p/>]

- **Dijjer** [<http://dijjer.org/>]

- Servicio de web – cache; distribución por nodos intermedios del contenido que viaja por la red

Redes libres

- **Otras aplicaciones**
 - **Servidores de Correo Distribuido**
 - **Miximinion**
 - <http://mixminion.net/>
 - **Mixmaster**
 - <http://mixmaster.sourceforge.net>

Ambos se basan en el comportamiento de los nodos como servidores que enrutamiento hasta el destino

Redes libres

- **Otras aplicaciones**

- **Konspire** [<http://konspire.sourceforge.net/>]

- Evolución del algoritmo de Bittorrent
 - Transferencia **1 a 1** a diferencia de Bittorrent que hace **n a n**
 - Crece exponencialmente
 - Para 19 transferencias ya ha superado a Bittorrent



Redes libres

- **Otras aplicaciones**

- **Konspire**

- Supongamos que un fichero cuesta de media mandarlo 1h

- 1h -> 1 1

- 2h -> 2502 2

- 10 h -> 112.510 1024

- 30 h -> 1.087.530 1.073.741.823 (1000 veces más)

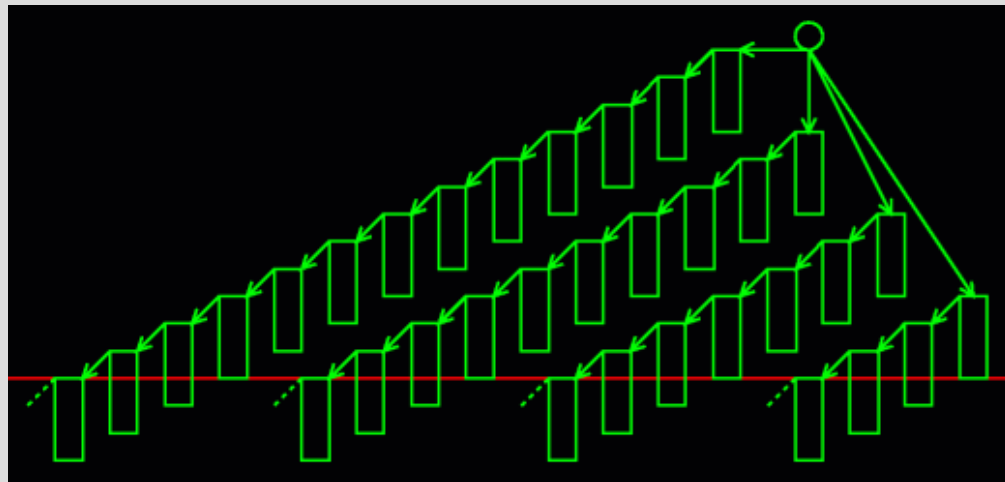
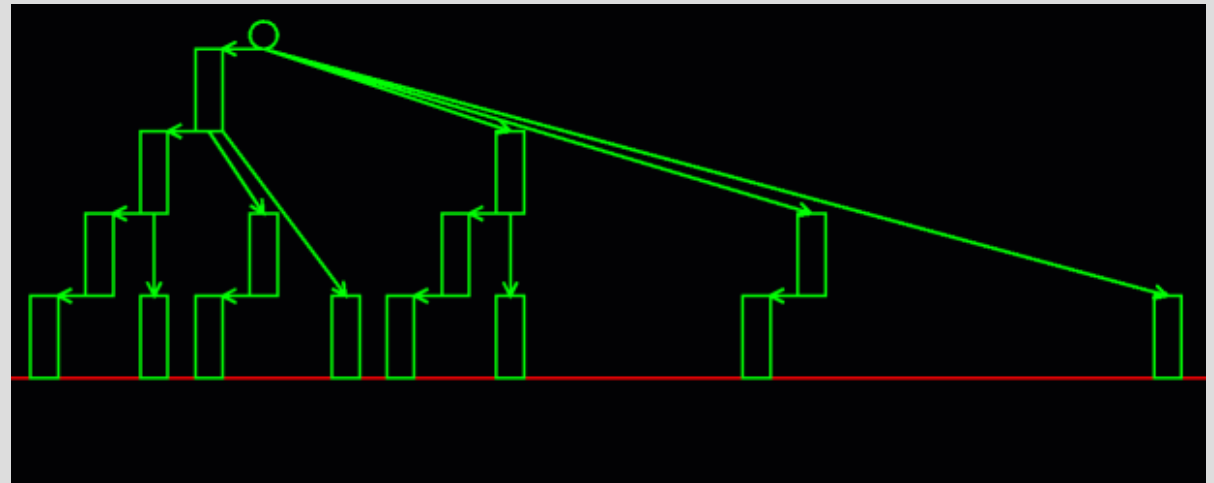
- Problema:

- Los usuarios cuando terminamos la descarga volamos

Redes libres

- **Otras aplicaciones**

- **Konspire**
 - VS
- **Bittorrent**



Redes libres

- **Otras aplicaciones**

- **Waste**



- **Nicotine (soulseek)**

- Permite conexiones indirectas



- **Bittorrent**

- Más centralizado debido a los Trackers: servidores que se encargan de crear la lista de usuarios activos



Redes libres

- **Asegurando las libertades de la Red**

- Aspectos legales de la tenencia de información
 - Monolith [<http://monolith.sourceforge.net>]
 - Random Pads [<http://www.eleves.ens.fr:8080/home/madore/misc/freespeech.html>]
- Cifrado, cifrado, cifrado ...
- Replantearse internet: es muy probable que Internet tal y como hoy lo conocemos deje de existir y se planteen nuevos modelos de compartición de información que sean menos vulnerables a la censura
- La libertad de expresión y el derecho a difundir nuestras ideas primará en este nuevo modelo de red

Redes libres

- **Asegurando las libertades de la Red**

- La evolución de la tecnología no es proporcional a la noción que se tiene de esta
- Las entidades militares no publican los avances que obtienen
 - Hay que pensar siempre que van un paso por delante sobre el desarrollo tecnológico actual
 - La computación cuántica puede desacer los modelos de cifrados usados hasta ahora basados en claves pública – privada
 - Los problemas NP-Completo pueden llegar a alcanzarse con este nuevo modelo ... (hablamos de computación exponencial)

Redes libres

- **MONOLITH** [<http://monolith.sourceforge.net>]
 - Canción con Copyright: 101001010100100 ...
 - Wav con datos random: 101010101010101 ...
 - Si aplicamos una función lógica como XOR obtenemos:
 - 101001010100100
 - 101010101010101
 - -----
 - 000011111110001 --> esta información es un fichero nuevo, totalmente distinto a cualquiera de los originales, NO es un trabajo derivado, tener este contenido NO puede ser ilegal

Redes libres

- **MONOLITH**

- Y como sistema de cifrado ???

- Si no conocieran el fichero WAV 'plantilla' con el que se cifró el número de posibles candidatos es de:

- $2^{\text{Tamaño_Canción}}$

- Tam = 3 MB = 3.000.000 Bytes = 24.000.000 Bits

- Posibles claves: $2^{24.000.000}$

- Estamos ante un problema **NP-Hard**

- Aún averiguando la clave no sabemos que hemos acertado (si no existen patrones ...)

Redes libres

- **MONOLITH**

- Problemas:

- Tamaño Clave = Tamaño Mensaje a cifrar

- Obtener información Randómica

- $x = \text{rand}()$ -> No es randómica sino pseudorandómica

- Los computadores son máquinas de estados finitos, no pueden producir números aleatorios puros

- Necesitamos de fuentes 100 % analógicas ...

- Tarjeta de Sonido (codificación del vacío ...)

Redes libres

APEIRON



Punto de encuentro para la investigación
modelos de comunicación que aseguren las
libertades de expresión en la red

<http://apeiron.laotracara.com>

David Gascón Cabrejas <483969@unizar.es>

Transparencias Liberadas bajo licencia GNU FDL

http://www.laotracara.com/redes_libres