



GOLDBUG

Secure Instant Messenger

User Manual

v.1.3

("NTRU Release")

<http://goldbug.sf.net>

What is GoldBug?

GoldBug is a secure Instant Messenger.

You can be sure with using GoldBug (GB), that no third party can look into your chat communication.

Private user-to-user communication remains private.

GoldBug therefore uses strong multi-encryption with different layers of modern encryption technologies of well known and revised crypto libraries (like libgcrypt (GnuPG) and OpenSSL). For example it generates more than 8 public / private encryption keys based on RSA or NTRU or ElGamal.

The app offers as well decentral and encrypted Email and decentral public E*IRC-Chat.

As in every Messenger, you can share and transfer files. With tools like Rosetta Cryptopad and/or the File-Encryption tool you can convert text and files into ciphertext.

Why encryption matters:

Today mostly every WIFI is protected with a password.

In a few years as well every plaintext message or email to friends over the internet will be encrypted too.

It is not a question to have something to hide or not,

- it is a question to control by yourself the security of your communications - or having it controlled by others.
- It's a question of free thinking and
- taking away the presumption of innocence.*)
- Democracy requires the thinking and debate of alternatives in private and public.

Strong-Multi-Encryption ensures the declaration of human rights in broad constitutional consensi and is a digital self-defense, everyone needs to learn and utilize.

GoldBug is one easy to use tool for that.

*) <http://www.faz.net/aktuell/feuilleton/buecher/themen/autoren-gegen-ueberwachung/demokratie-im-digitalen-zeitalter-der-aufruf-der-schriftsteller-12702040.html>



*"The question is not 'do you have something to hide?'
The question is whether we control
or they controls us." - Oliver Stone*

<http://www.youtube.com/watch?v=0U37hl0n9mY>

Why the name GoldBug?

" 'The GoldBug' is a short story by Edgar Allan Poe. The plot follows William LeGrand, who recently discovered a gold-colored bug.

His companion, Jupiter, fears LeGrand is becoming now obsessed with searching for treasure, knowledge and wisdom after being in contact with the GoldBug - and goes to LeGrand's friend, an unnamed narrator, who agrees to visit his old friend. After LeGrand has deciphered a secret message the three start an adventure as a team.

'The Gold-Bug' - as one of the few pieces of literature - incorporates ciphers as part of the story. Poe took advantage of the popularity of cryptography as he was writing 'The Gold-Bug' in 1843, and the success of the story centers e.g. on one such cryptogram and the search for the Philosopher's Stone. 'The Gold-Bug' was an instant reviewed story and was the most popular and most widely evaluation of Poe's works during his lifetime. His ideas also helped to popularize secured writing and cryptograms." - Wikipedia.

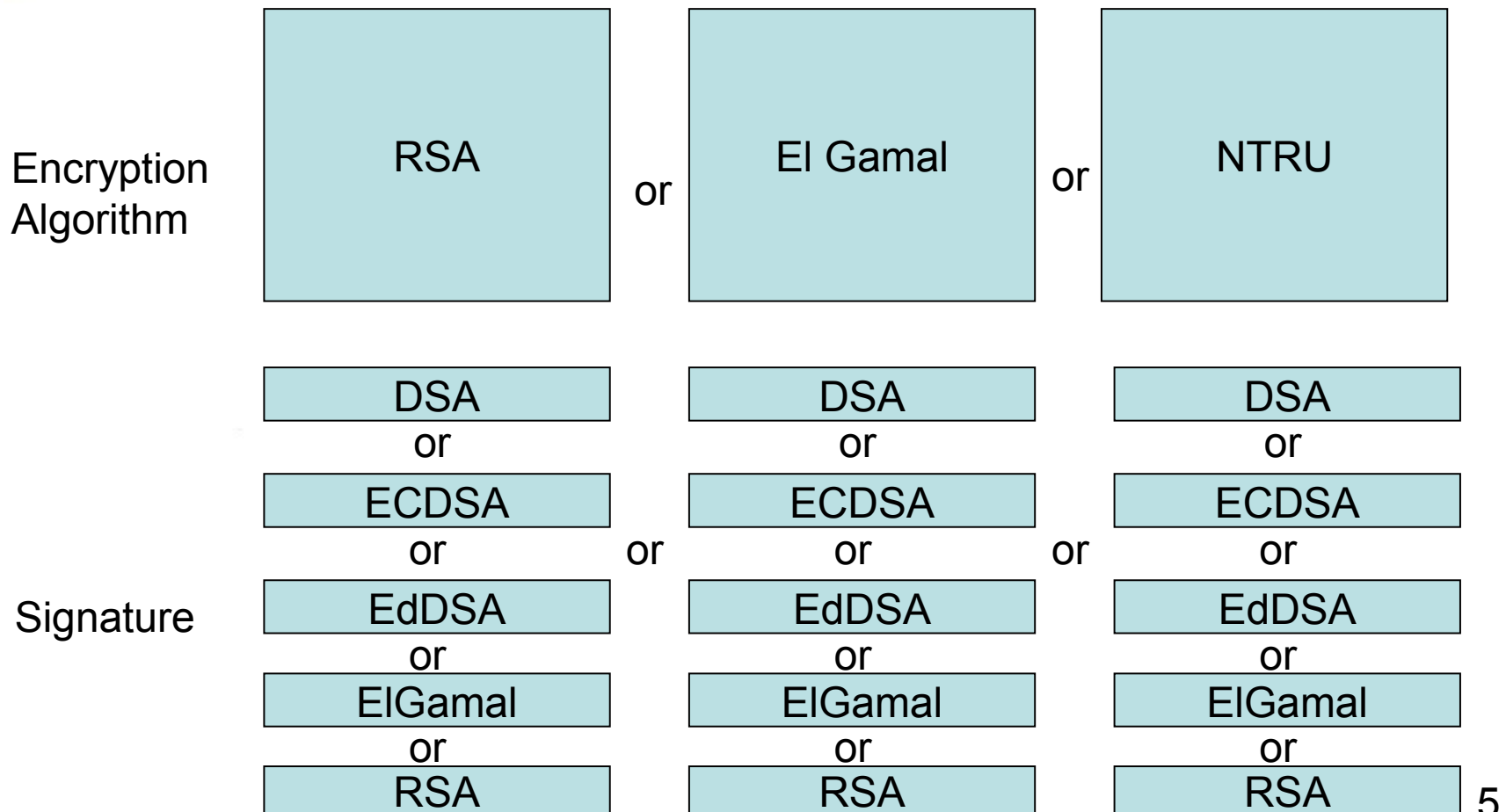
170 years later

encryption has more weight than ever.

It has to be a standard when sending out communication over the Internet.

GoldBug has alternatives to RSA

Find your own setting of encryption components: RSA, NTRU, ElGamal, DSA.
of course: Keysize! .. and for: Cipher, Hashtype, Iteration Count, Salt Length.



RSA vs. ElGamal vs. NTRU

NTRU is an open source public-key cryptosystem that uses lattice-based cryptography to encrypt and decrypt data. It consists of two algorithms: NTRUEncrypt, which is used for encryption, and NTRUSign, which is used for digital signatures. Unlike other popular public-key cryptosystems, it is resistant to attacks using Shor's algorithm and its performance has been shown to be significantly better. Unlike RSA and Elliptic Curve Cryptography, NTRU is not known to be vulnerable to quantum computer based attacks.

<http://en.wikipedia.org/wiki/NTRU>

RSA is one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977.

A user of RSA creates and then publishes a public key based on the two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

[2] Breaking RSA encryption is known as the RSA problem. It is an open question whether it is as hard as the factoring problem.
[http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

In cryptography, the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. It was described by Taher Elgamal in 1985. ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm is a variant of the ElGamal signature scheme, which should not be confused with ElGamal encryption. ElGamal encryption is probabilistic, meaning that a single plaintext can be encrypted to many possible ciphertexts, with the consequence that a general ElGamal encryption produces a 2:1 expansion in size from plaintext to ciphertext.

http://en.wikipedia.org/wiki/ElGamal_encryption

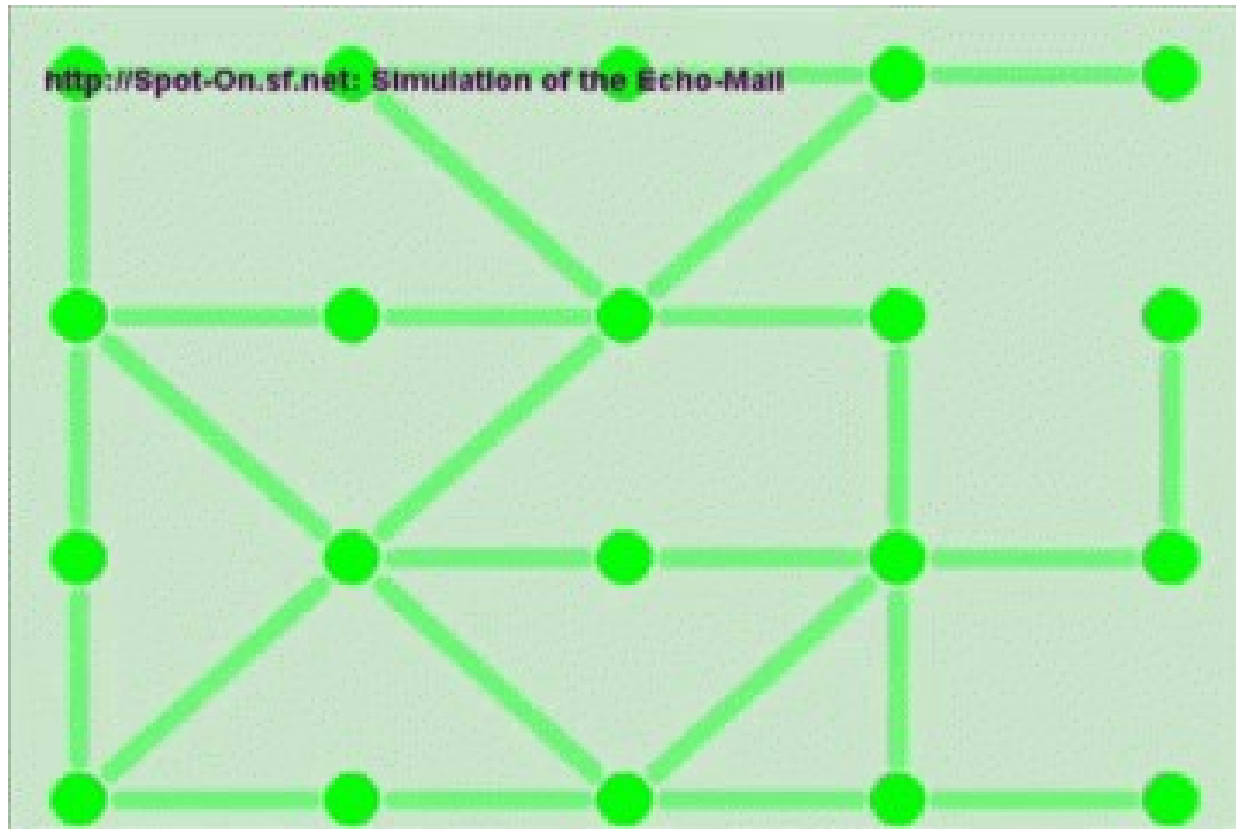
Echo Protocol ?!

- Echo Protocol simply means, each Message is encrypted...
- $\text{SSL} (\text{AES} (\text{RSA}^* (\text{Message})))$
 - *) instead of RSA you also can use ElGamal or NTRU.
- ... and every Neighbor sends every Message to every Neighbor.
- Small World Phenomen: Everyone can reach everyone over 7 hops in a f2f/p2p network or over a common chat server.
- Half Echo modus sends the message only one hop.
- Adaptive Echo sends the message only to tokenized nodes.
- Echo Accounts allow only friends to connect.

Echo Protocol !

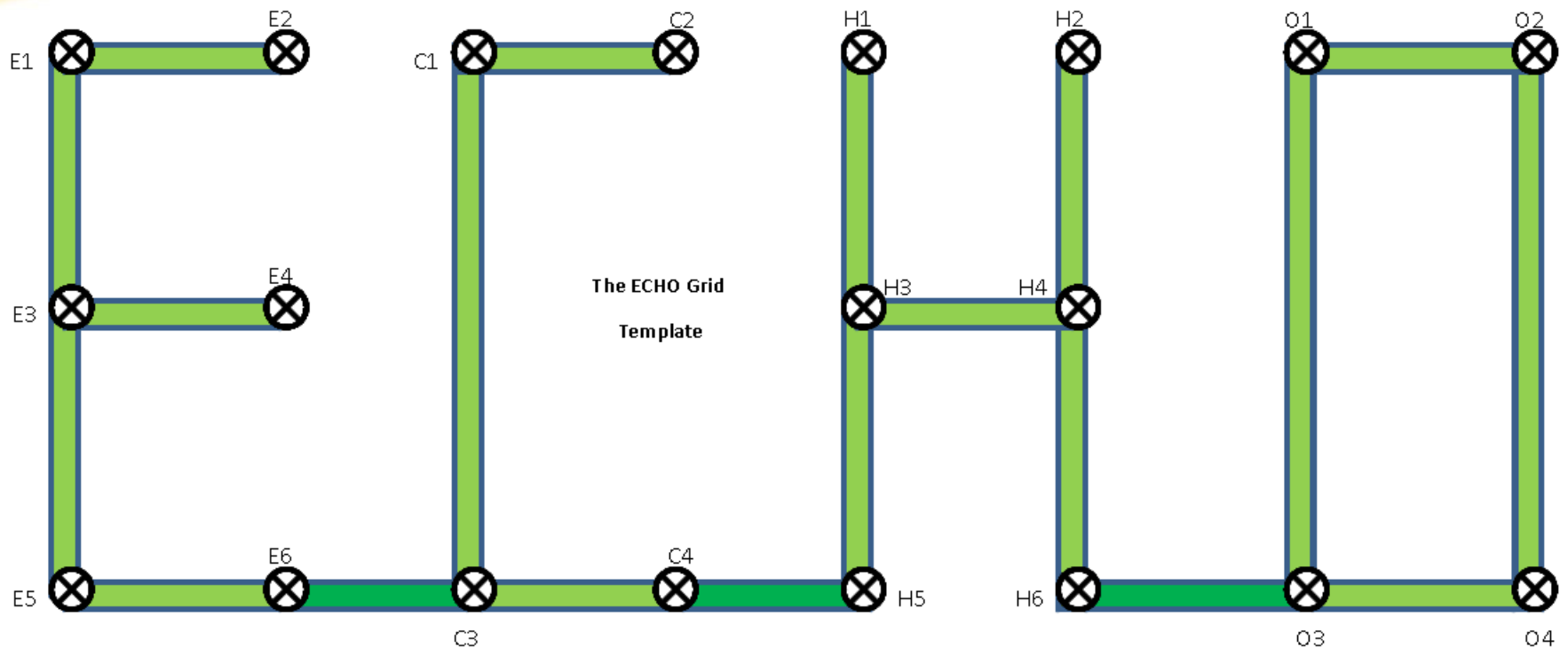
Every neighbor sends every message to every neighbor.

(Click on the image to see the simulation)



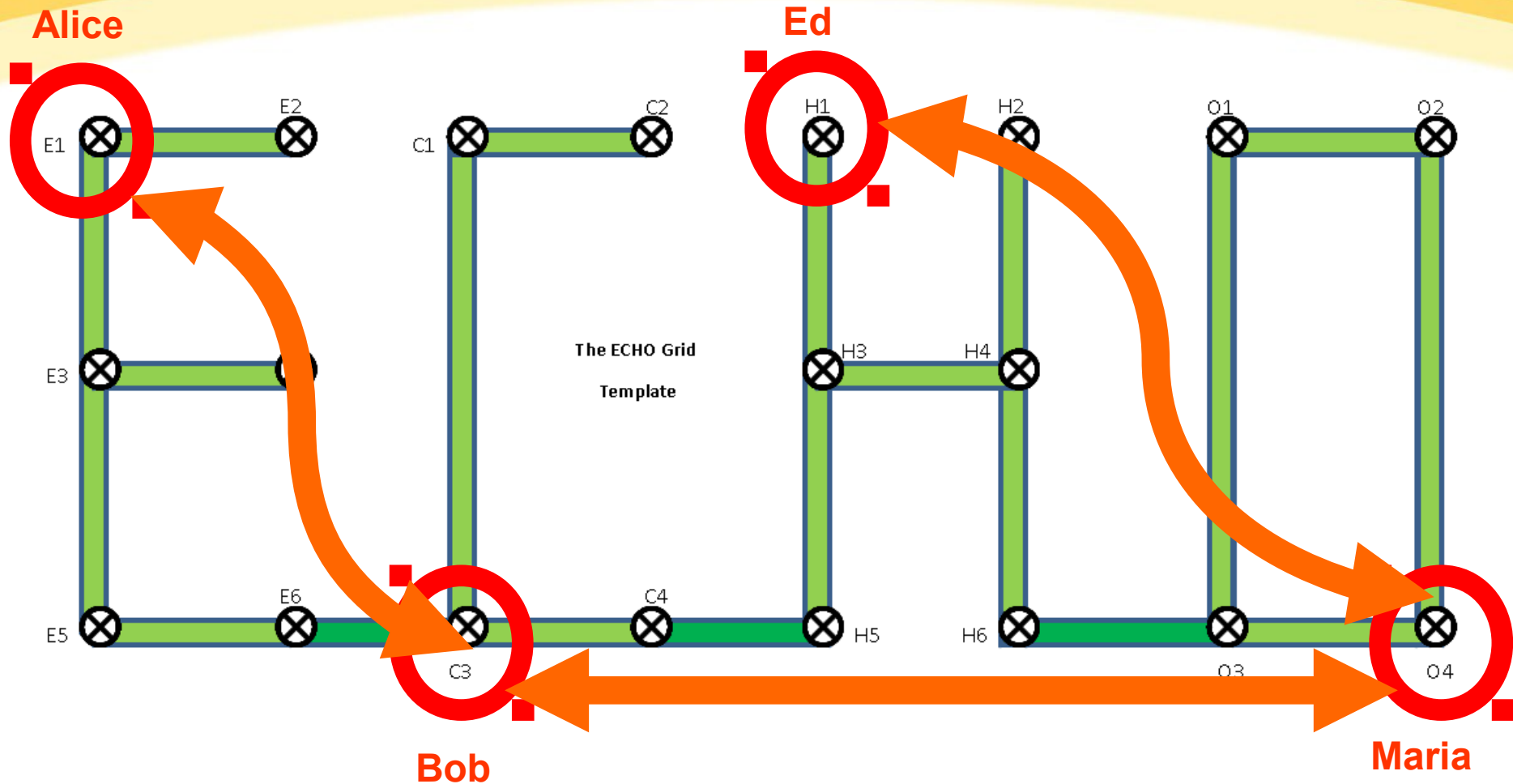
If you receive a duplicate message, it is controlled in your cache for congestion.
You can also send out fake or impersonated messages, to disturb tracking.

The Echo Grid: E1 – O4



When we talk and teach about ECHO, we just draw an Echo Grid from E1 - O4 and connect the letters on the bottom line. E.g.: E1-E2 describes a neighbor IP connection.

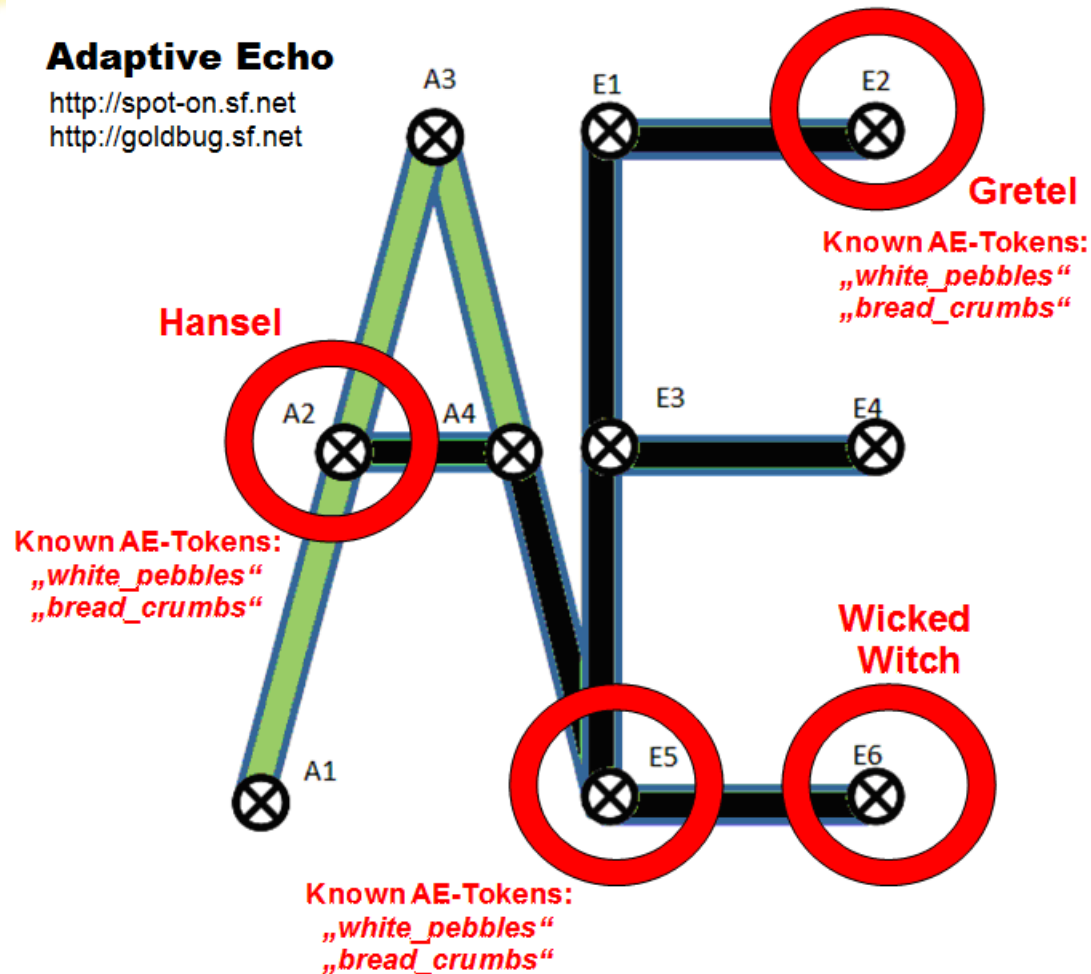
Paths based on Keys



Examples of the Key-Exchange of Alice, Bog, Ed and Maria.

- Alice (IP=E1) and Bob (IP=C3) swapped their keys and are connected over the IP-Neighbours: E1-E3-E5-E6-C3.
- Bob (C3) and Maria (O4) are friends too, they swapped encryption-keys as well: and use the IP-connection of the neighbors: C3-C4-H5-H3-H4-H6-O3-O4.
- Finally, Maria (O4) is a friend of Ed (H1). They communicate over either: O4-O3-H6-H4-H3-H1 or they use the path of: O4-O2-O1-O3-H6-H4-H3-H1. As every IP-neighbor sends every message to every connected neighbor, the path within shortest time delivers the message.
- Direct IP Connections of Neighbors like e.g. E1-E3 can be secured by using an account information: No other IP address than E1 can connect to the listener of the neighbor E3. That way a web of trust can be established, without being dependent on encryption keys, nor need the neighbor a friend, you share your chat or email key with.
- „Turtle hopping“ is more efficient: When Ed and Alice share a Starbeam-Filesharing-Magnet, the Echo protocol transports the packet over H1-H3-H5-C4-C3-E6-E5-E3-E1. Maria is not in the route, but will get as well the packets over echo, if she knows the Starbeam-Magnet.
- A Buzz IRC Channel Room can be created/hosted by O2. As only Ed knows the Buzz Room name, all other Neighbors and Friends are kept out. Advantage: you can chat with unknown friends in a buzz room without swapping your public chat key, instead you use a one-time-magnet for a buzz room.
- Maria is a common friend of Ed and Bob, she enabled for Emails the C/O-Funktion, that allows Ed to write emails to Bob, though he is offline, Maria keeps the emails until Bob comes online.
- Further: Alice enabled an institution for email: Ed sent his email-key to Alice and Ed added Alice Email institution-magnet. Now as well Bobs emails to Ed are stored in Alice, even if Maria is offline.

Adaptive Echo (AE) Tokens



When you, your chat-friend and the chat-server add the same Adaptive-Echo (AE) Token, then the chat server will send your message only to your friend (and not to all connected users, as provided by the "Full Echo"). With an AE-Token no one else will get or see your message and hence no one can try to break encryption, because potential recording nodes are excluded.

Hansel and Gretel - another Adaptive Echo Example: When node A2, E5 and E2 share the same AE-Token, then E6 will not get any message, which A2 (Hansel) and E2 (Gretel) will exchange. Node E5 learns via the known token "white_pebbles", not to send to E6 (Wicked Witch).

An "Adaptive Echo" Network does not reveal any destination information (comp. Ants Routing). Remember: "Half Echo" sends only one hop to the connected neighbor and "Full Echo" sends the message to all connected nodes over infinite hops. While "accounts" prevent clients from connecting, "AE-Tokens" provide graph- or path-"exclusivness" for sent messages via nodes, knowing an AE-Token. Server admins can share their tokens with other server admins as well, if they trust each other (ultrapeering for trust).

Test the Adaptive Echo (AE) Tokens

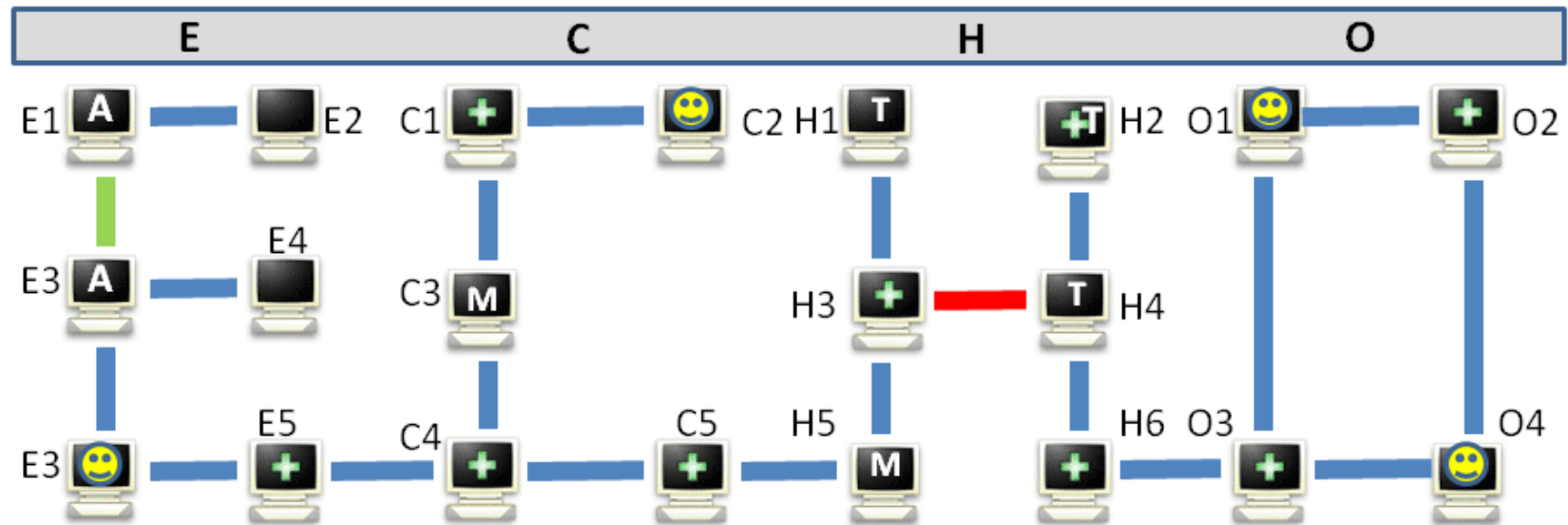
Use SPOTON_HOME, to create several nodes on one machine (or use three machines)

1. Create a server node.
2. Create two client nodes.
3. Connect them to the server node.
4. Share keys between the two clients.
5. Testing normal communications.
6. Enable a token on the server.
7. Test normal communications.
8. Enable a token on one client.
9. See results: The server-node is not sending out the message to nodes, which have not the token.

Simple.

How the ECHO PROTOCOL works

Full Echo | Half Echo | Adaptive Echo (AE) | Echo Accounts



Node with Echo-Kernel as Client.



Node with Echo-Kernel as Listener/Server.



Node (Listener/Server) with Echo-Account:
F2F Connection only with Login Credentials.



Echo User with asymmetric Key.



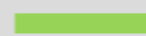
Echo User with symmetric Magnet URI:
• C3 and H5 can chat in the same room.



Echo-Node knowing an AE-Token:
H4 learns, not to forward to H6 and „O“-Quadrant.



Physical Connection to a Neighbor.



Physical Connection to a Neighbor
with Echo-Account:

- E1 connects to E2 only with Login Credentials
- E2 cannot connect to E1
- E4 cannot connect to E3.



Half-Echo Connection to a Neighbor:
Messages are sent only one hop

- User O4 and C2 cannot talk.



Virtual Connection: User E3 and User C2
talk over keys, not attached to their IP-Address.

Explore and evaluate lots of GoldBug Features

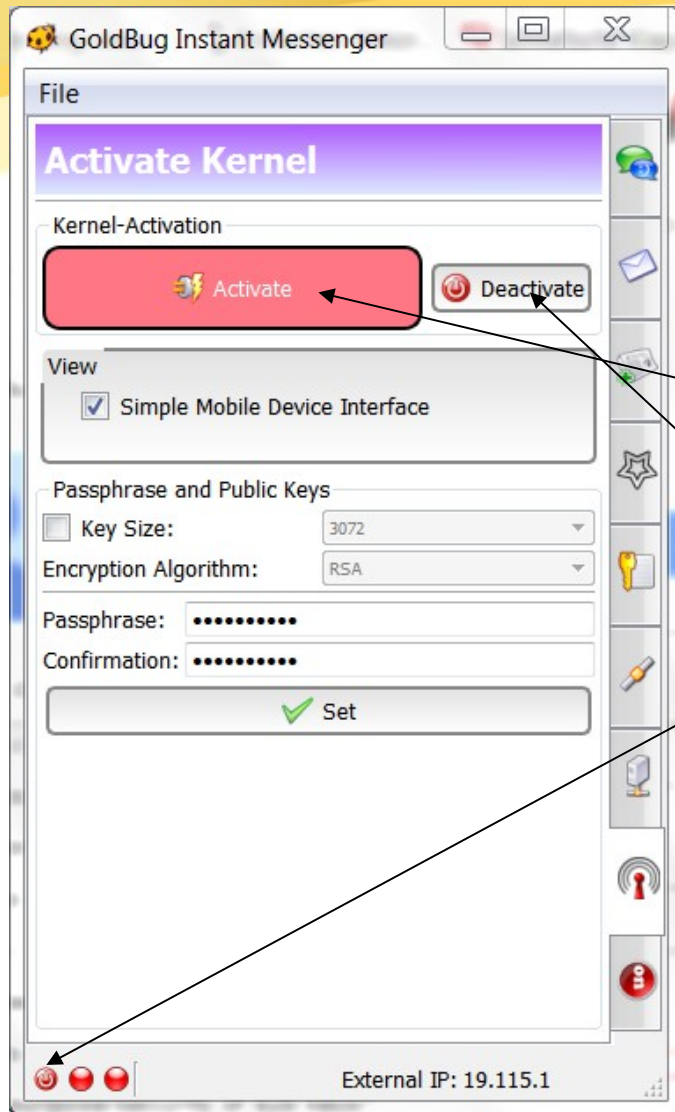
- Encrypted 1:1 Chat: GoldBug encrypts your private chat with RSA-Keys, SSL and end-to-end encryption.
- Encrypted Groupchat: With all your friends you can create a group chat
- Starbeam: FileSharing: Anonymous Seeding.
- Public/Priv. RSA Keys: GoldBug uses public/private keys. The public key must be exchanged between friends.
- Repleo: Either you send your key in plaintext or you use the Repleo, which encrypts your key itself.
- Gemini: The Gemini is an AES-end-to-end encryption for chat and an additional layer of encryption.
- GoldBug-Passphrase: Secure your GB-Emails with a passphrase per each email. This is called a GoldBug-Phrase.
- p2p Email: Next to Chat: GoldBug offers you serverless p2p Email without data retention. Integrated BitMail.sf.net
- e*IRC: Public Chat is provided with e*IRC, which is echo-ed IRC: Groupchat on AES Channels.
- MELODICA: The MELODICA Button provides instant forward secrecy. Renew your Gemini in a second!
- Instant Fwd Secrecy: Session AES-keys are inde-pendent from longterm RSA-keys. Use MELODICA often! Multi-Encrypted-Long-Distance-Calling.
- Opt. Authentication: GB provides optional use of signatures, for authenticated Chat & Emails. Trust, when needed.
- Chat over Tor-Proxy: Yes, GoldBug can be used over the Tor-Proxy. It is a new TorChat Application with end to end encryption, which keeps the tor-exit-node out of your communication.
- Echo Protocol: Next to encryption & f2f Email: Echo is a new algorithm, that makes GB resistant to tracking.
- Half Echo Modus: Half Echo sends messages only directly to one friends IP. Exclude others to ever get your message.
- Simulacra-Scrambler: The simulacra sends out random fake messages from time to time. And No, it's not the Mona Lisa.
- WoT-Deniability: The Half Echo Modus creates a deniability for a web-of-trust (f2f) in a p2p-environment.



Screenshots:

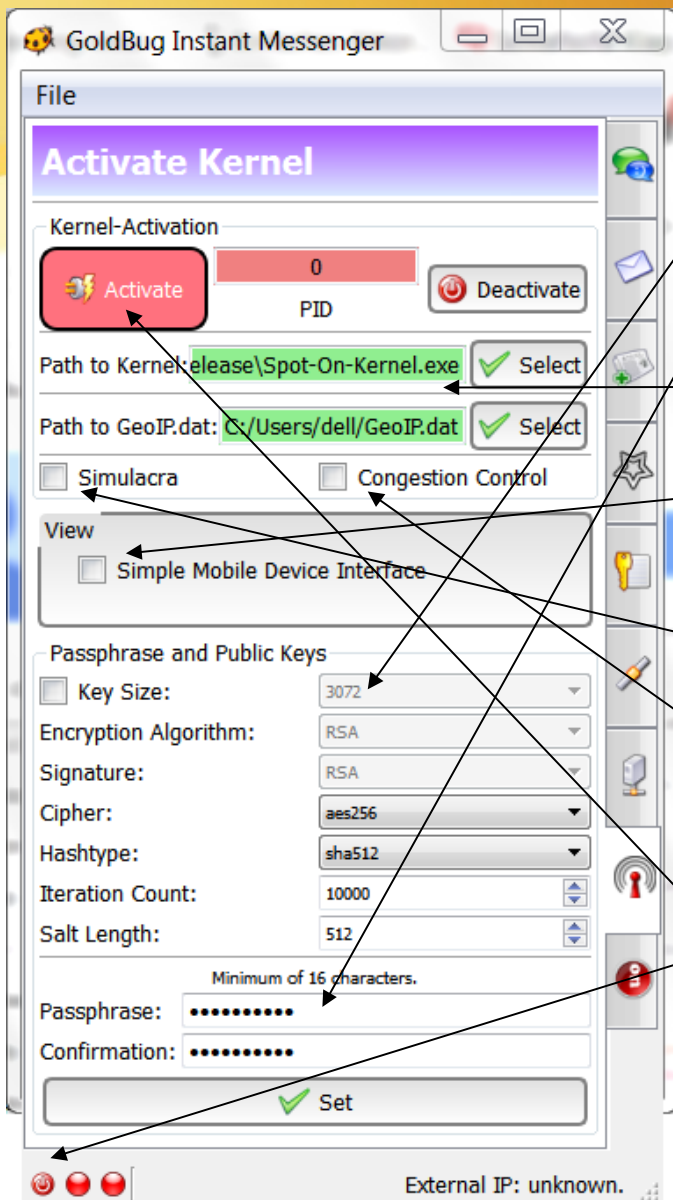
- Kernel Activation

Activate Kernel (Simple View)



- When you have set your password and checked (after restart) the simple view, the tab looks like this.
- Just press the activate button to start the kernel.
- When you close the gui, you close the gui, and the kernel will still be running. When you want to quit both, first deactivate the kernel and then close the gui.
- You can de/activate the kernel by pressing the left LED or the button „Activate“.
- Your generated keys are stored in the subpath `/.spoton`. In case you want to set up a new account and want to erase all your data, just delete the path and start fresh.

Activate Kernel (Full View)



- Choose (any) settings for the public keys, e.g. choose a key size greater than 2048 bit.
- Enter a passphrase with a minimum of 16 characters and press the „set“-button.
- Make sure, the path to GeoIP.dat and Spot-On-Kernel is set correctly (highlighted in green).
- If the pathes are set correctly, you can check the simple mobile device interface view, this structures the interface even more simple.
- Check „Simulacra“, in case you want to send out fake messages from time to time.
- Check „Congestion Control“ in case you have a slow cpu or less bandwidth: it remembers the hash of an incomming (encrypted) message & reduces redundancy by not sending the same message out a second time. Default now.
- Most important: Activate the kernel by pressing the red button. GUI (Graphical User Interface) and Kernel create a secure local socket connection and provide a Process ID (PID). The left LED at the status bar will get green.



Communication

- Emoticons ☺
Groupchat
- Personal 1:1 Chat
 - p2p Email
- echoed IRC (e*IRC)

Pop-Up Chat-Window: Send-Button Tooltip

Someone from

US people

lb-ip.com

n Spec

ame:

Chrome 3

address]

ey, Colora

turning Vi

pplicable

09.181

lite




















09.181 ha

09.181 cou

age loads

re port

Send

List of Emoticons					
O:-)	angel		:~)(-:	kiss	
:~	angry		:	neutral	
:~/	confused		(t)	phone	
8-)	cool		@ > -- > --	rose	
:'(crying		:-(sad	
o-)	cyclops		:~O	shocked	
}:)	devil		C:-)	skywalker	
:~D	laugh		:~)	smile	
:~))	happy		:~P	tongue	
			;)	wink	

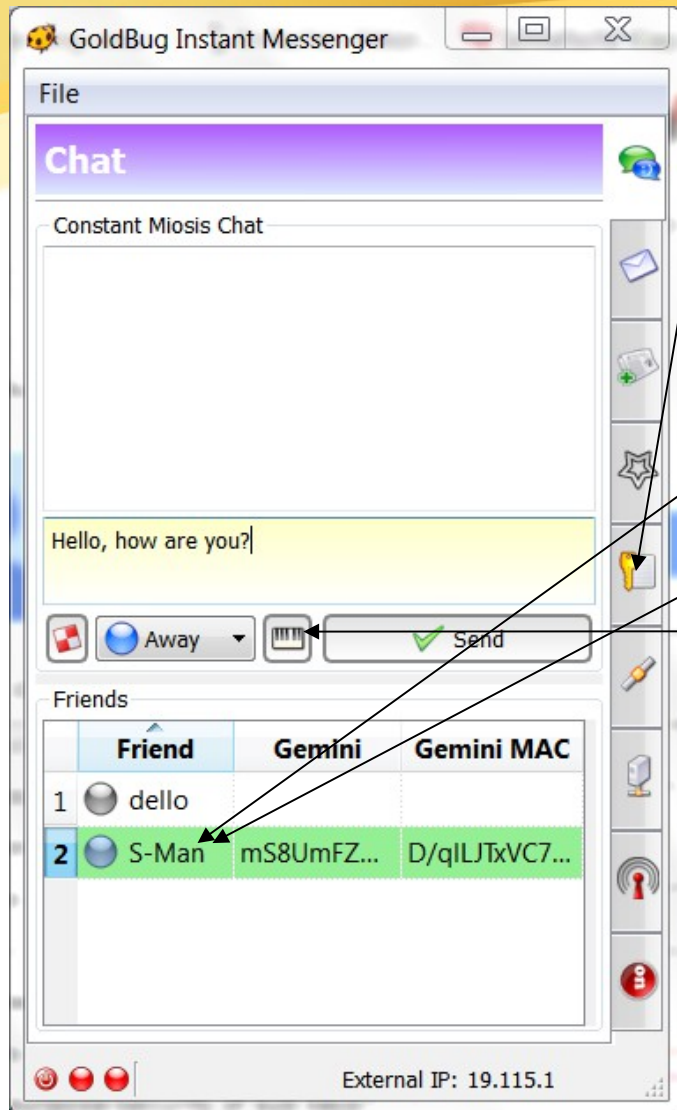
My Name:

mike

Save

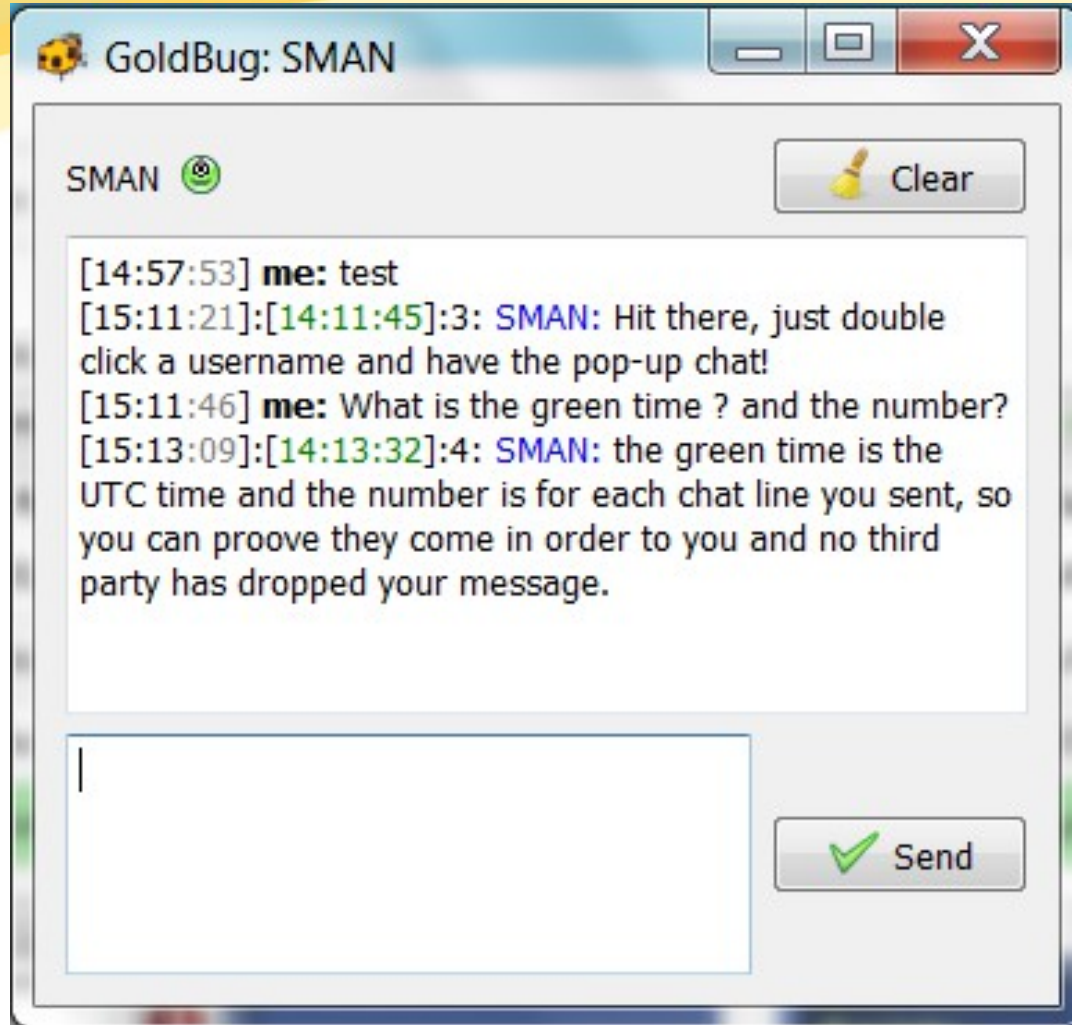
☒ Enable emoticons.

GoldBug Chat is secure!



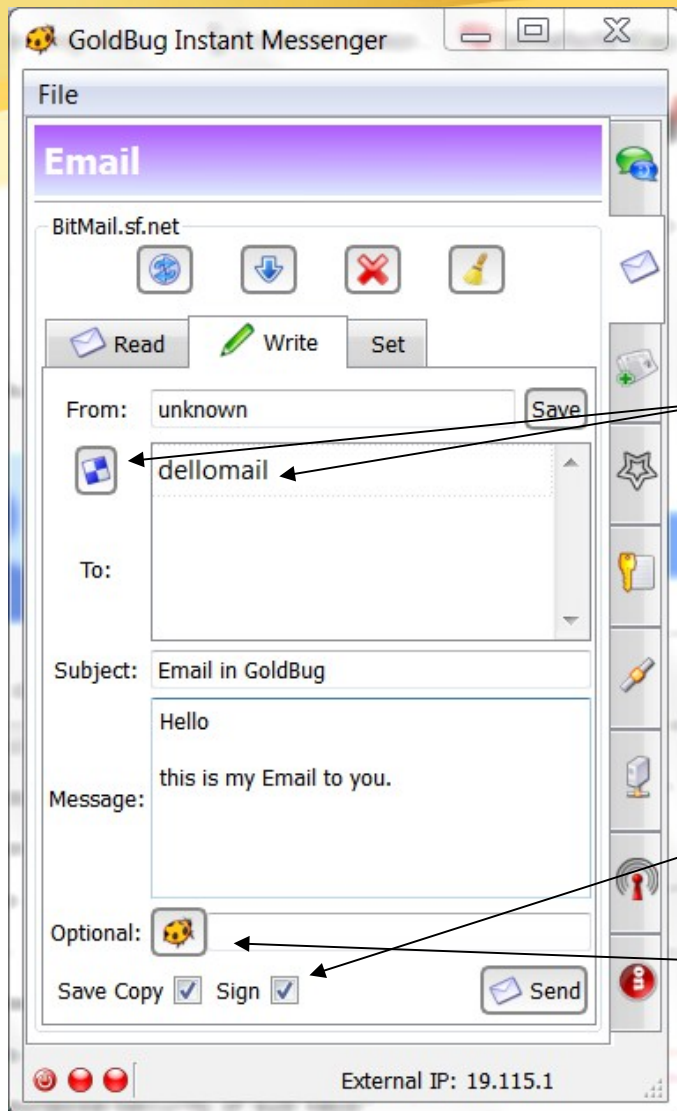
- After „kernel activation“ and „key exchange“ you will find your friend in the chat tab.
- Both friends need to exchange keys and paste the friends key into the add friend tab.
- You can just copy your key from the add friend tab or: you send a so called „repleo“ to your friend, then your key will be sent not as is, but encrypted with the (already gotten) key of your friend. This allows to prevent to send your key as is. So it is not - as a string – searchable in email accounts.
- Select a friend and enter some text, then press the send button.
- You can select even more than one friend to send out a groupchat.
- **Doubleclick on the friend to open a chat-pop up window.**
- MELODICA stands for **M**ulti **E**ncrypted **L**ong **D**istance **C**alling and is the button to „call“ a friend. This generates 2 End to End Encryption keys, first an AES-256-Key, the gemini, and the so called MAC-Key, which additionally secures the Gemini transfer. The transfer of the Gemini is done within the RSA-/SSL-Encryption.
- You can „call“ instantly new. That is: „Instant Forward Secrecy“.
- Right mouseclick opens the context menu to find the commands as well there.

1:1 personal chat in a pop-up



- Have each friend in a pop-up chat.
- Double click on the friends name.

p2p Email: without data retention

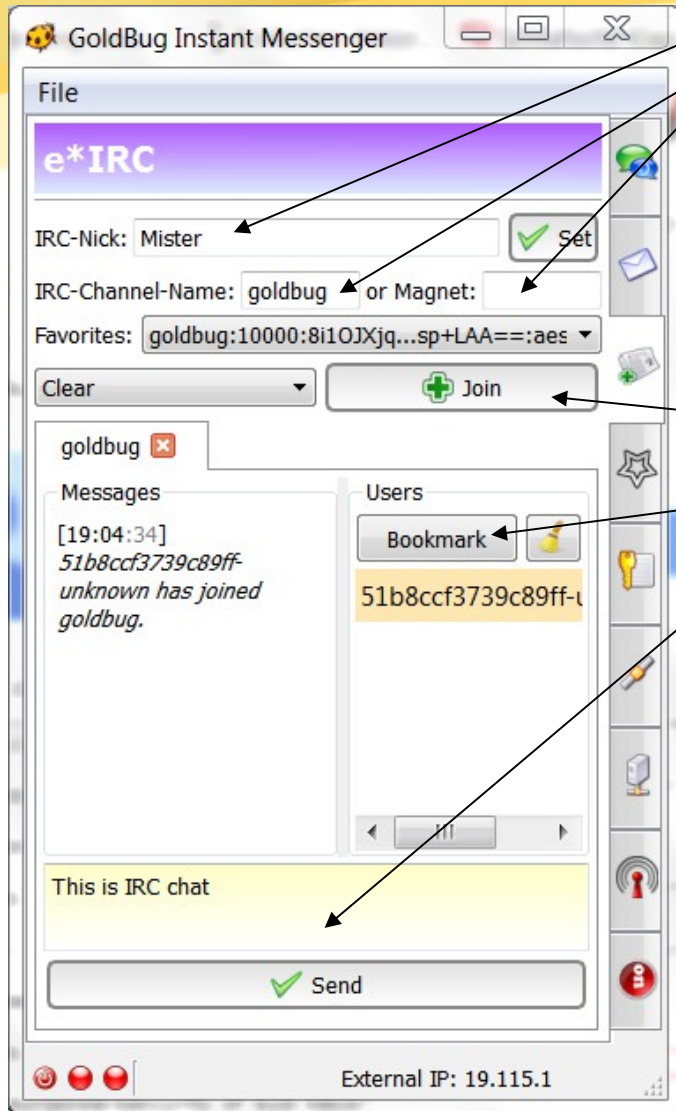


- GoldBug has integrated a p2p Email client based on the architecture of libspoton and the Bitmail.sf.net client.
- You can use it as full Email client to email your friends.
- Chat and Email have different RSA keys due to security reasons. You might want to add a friend to email, but not to chat. In case you shared the All-in-one-key, you share both keys: for chat and email (next to URLs and Rosetta Key).
In case you share only the email key, you need to approve the friend over the right mouse context menu „Accept key“ and you need to send your friend as well your own email-key. You can use as well a Repleo-Button for that, which encrypts your key (so you dont send it in plaintext).
- You can send emails as well to offline friends!
- Emails have no central server and are stored in your other friends, so try to get more than one friend into your email list. As the emails are encrypted, these „caching“ friends cannot read it.
- You can use signed (= authenticated) messages, but need not.
- When you want to set additionally a password on your email, you can use the GoldBug button, which sets an AES-key on the email, but you then need to transfer this key to your friend.
- Or you agree with your friend, that all emails are secured with the password e.g. with the town, you met first.

Anonymous p2p Email with Institutions

- Enable the C/O-Funktion in the tab for Email Settings.
- Create an Institution and chose a Name and Address for the Institution.
- E.g. Name = „Google“ and Addres = „Dotcom“
- Add the email key of a friend to your node and let friends add your magnet of the institution to their node. The Magnet will look like this: **magnet:?
in=Google&ct=aes256&pa=Dotcom&ht=sha512&xt=urn:institution**
- Then your node is saving emails of your friend while they are offline.
- You (as institution creator) need not to share your email key with your friends/subscribers. The friends/subscribers just add their email key to your institution and they add the magnet of your instituton.
- With Intitutions Offline-email is possible in the p2p network, without the Institutions or friends beeing connected as IP-Neighbor. That means within the echo grid you have anonymous email boxes over the institutional feature.
- You can share your email key in a buzz channel room, then even the institution creator remains anonymous for the key/magnet swap process.
- (Or you choose for offline email the c/o method of a third common friend enabling the c/o feature).

echoed IRC



Set your Nic-Name for the echoed IRC Chat (e*IRC)

To join a channel, simply enter the name of the channel-room or add a provided magnet link. The magnet link might have additional values next to the roomname such as key, hash or encryption cipher type etc.

- When you enter just the roomname, the default values of 0000 are chosen for the encryption details and the channel will be encrypted based on the hashed roomname you provide.
- Once done, press the button „Join“ (for magnets as well the pull down menu „de-magnetize“ will bring you into the room).
- The Room-Tab opens, and you can set or delete the bookmark function for this room.
- Enter some message and press the button „send“.
- The Chat room is fully end-to-end encrypted and can be private or public, that depends on how you spread the roomname or the magnet link.
- As a public chat room you can link the magnet on your website and everyone knows how to come into the room. It is like IRC just with the difference, that the ISP and routing servers of the internet cannot look into the communication, as it is encrypted.
- Private room: you can easily open up a secure room beside the RSA 1:1 chat of your exchanged keys. A one-time-room shared with your friend over your secured RSA Chat.



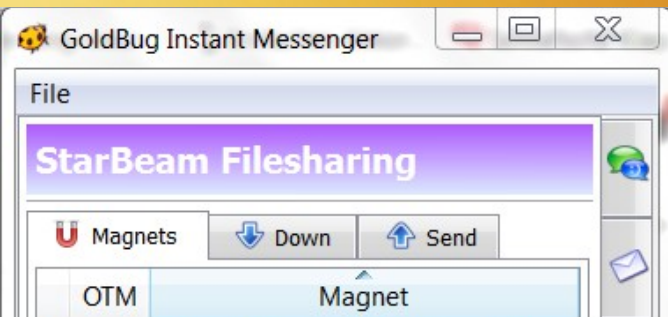
FileSharing:



StarBeam

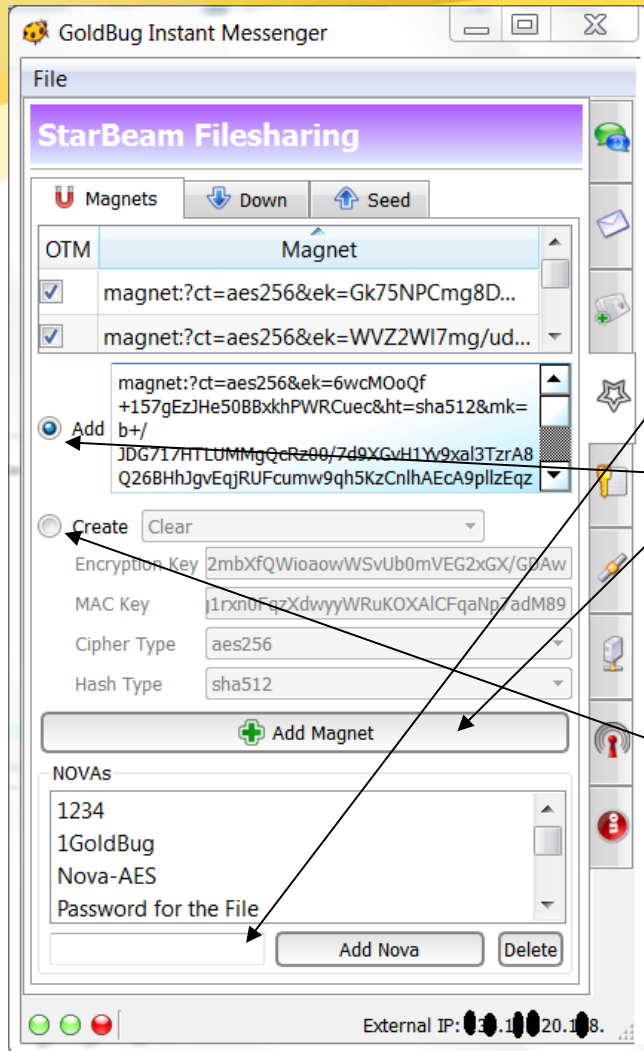
- Add/Create a Magnet
 - Optional: Nova
- Optional: RAR/ZIP-Password
- Select File+Magnet: Seed anonymously

StarBeam FileSharing



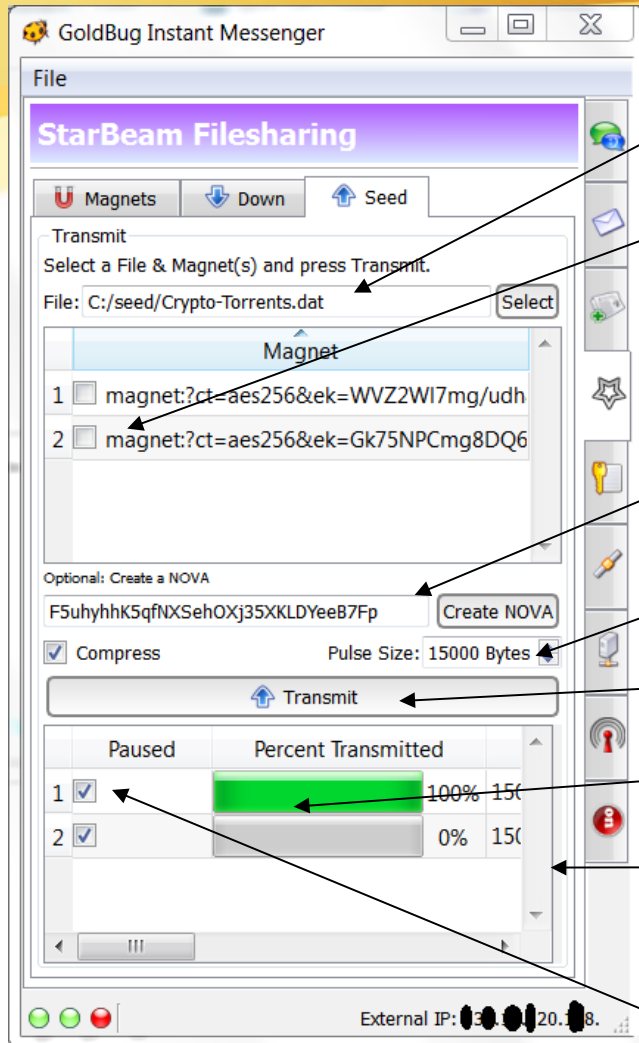
- The advantage of GoldBug is, that keys and IP addresses do not belong together. You just need a connection to any chat node. (Option: you can use accounts for building a Web of Trust (WoT)).
- Of course, you can use the echo protocol and GoldBug to transfer files – like any other messenger. Encrypted Transfer of Files has been introduced with V 07 of GB and is called StarBeam.
- Sharing files is the same as sending a text message in chat. You need an encrypted channel or the right key, to decrypt chunk by chunk.
- That's why you don't share a specific file in StarBeam, you share a wormhole, a crypto-channel. The channel is defined by a magnet.
- Ideally you have for each file one magnet, for that you need to generate or add a (given) magnet. This can be a One-Time-Magnet (OTM). So once you have transferred ONE file over this magnetized crypto channel, the magnet expires and is deleted. But of course you can establish one crypto-channel with your sister and send out first the holiday pictures and then the text diary for the travel route.
- A NOVA is an additional layer of encryption (AES) to protect the file. Like a magnet it must be given prior to be able to record the transmit.
- Of course you can share a password protected rar/zip-file and share the secrets after the transmit has been done.
- You can share a StarBeam Crypto-Slot with the public or just one person.
- Once you have transferred a chunk of a file, the receiver can share it back and upload it again to the same or any other magnet-slot – and you even can do this with a time delay.

StarBeam: Magnets & NOVA's



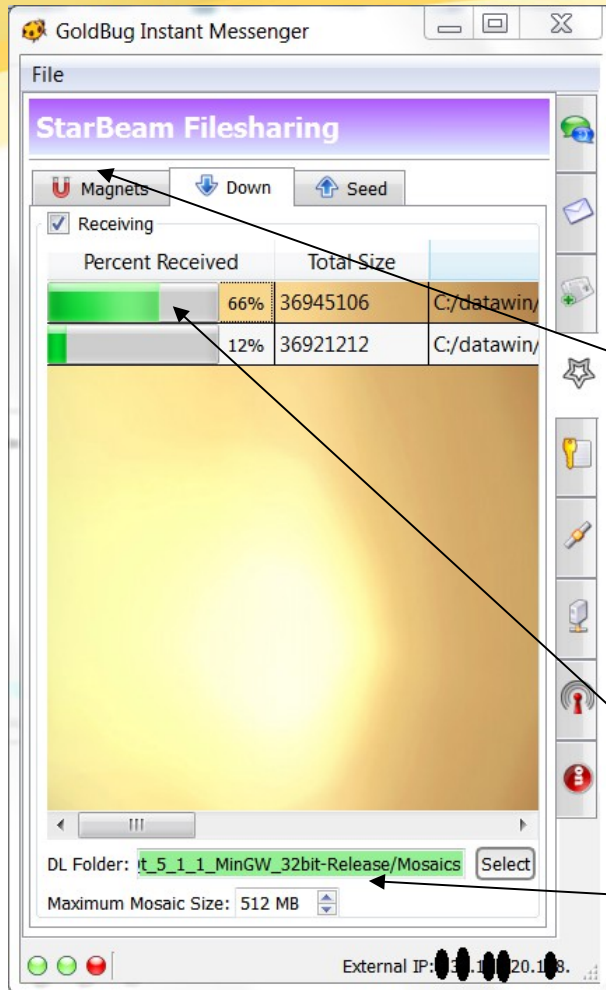
- When you want to download a file, just „add“ the given magnet (and maybe optional the NOVA-key).
- NOVA is an additional encryption passphrase on the file.
- Once the Magnet is added and your friend starts the seed, you see in the downloads tab the progress bar for the incoming file.
- When you want to upload/seed a file, just „create“ one or more magnets and you will be able to select them in the Seed-Tab.

StarBeam: Transmit & Seed



- Select a file
- Select one or more magnets (that's what you generated in the magnet tab)
- Optional: Set Nova-key.
- Define Pulse/Chunk Size
- Press Transmit Button
- See the upload in the table
- Side splitter to copy the magnet & transfer the magnet to a friend
- Un-check „paused“ to start.

StarBeam: Downloads



- Copy a Magnet from a website or get it from a friend.
- Add/Paste the magnet in the magnet tab.
- Tell your friend you are ready to receive.
- See the download starting.
- (Set path and mosaic cache size).
- StarBeamAnalyzer (over Tools Menu) allows to check, if all chunks/links have been transmitted, if not, copy out the Missing-Links-Magnet and your friend can paste it in his client, to send you only the missing links/chunks. Otherwise he can rewind the full file and seed/upload it a second time.

Magnet URIs

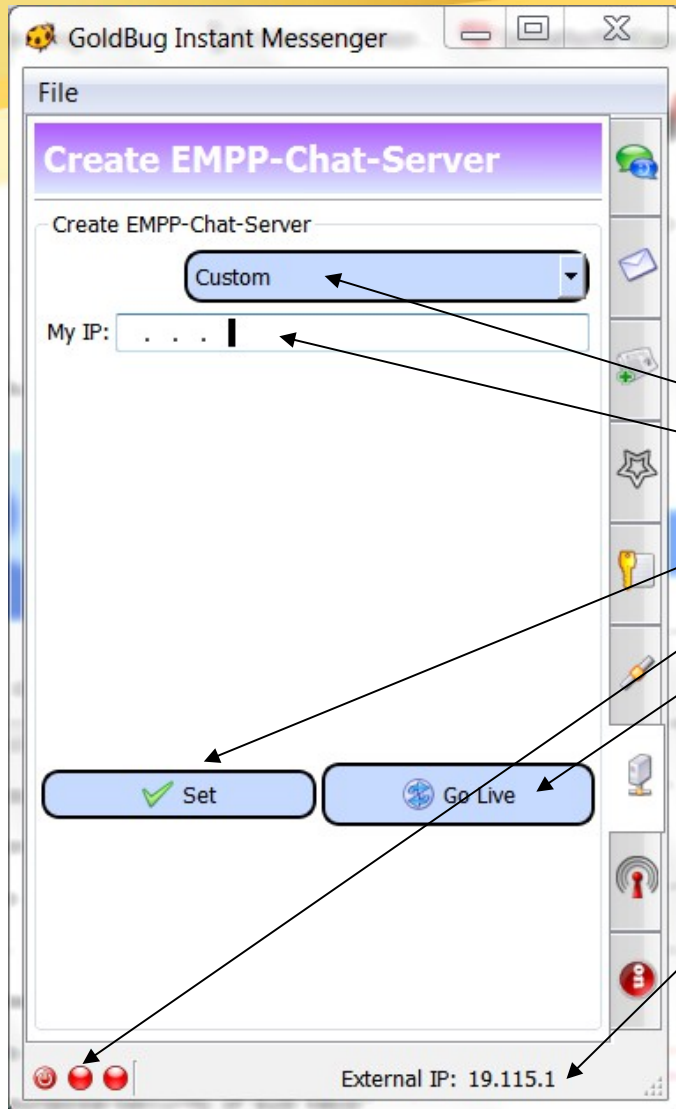
- Magnets are used for a crypto-information bundle.
- New extensions for the Magnet URI standard
- Magnets replace e.g. RSA public & private Key exchange (Magnets are the new PGP).
- OTP => ORM: One Time Magnets (OTM) are the new One Time Pad (OTP)
- Starbeam Filesharing: Magnets describe not a file, but a crypto channel. You can link it without sorrows on any website.
- Rar/zip-Files might have a further passphrase, which is given when the transmit has been done.
- Do StarBeam Magnets offer a new way of thinking in terms of „Crypto-Torrents“ with anonymous Seeds on the echo protocol?



Set up

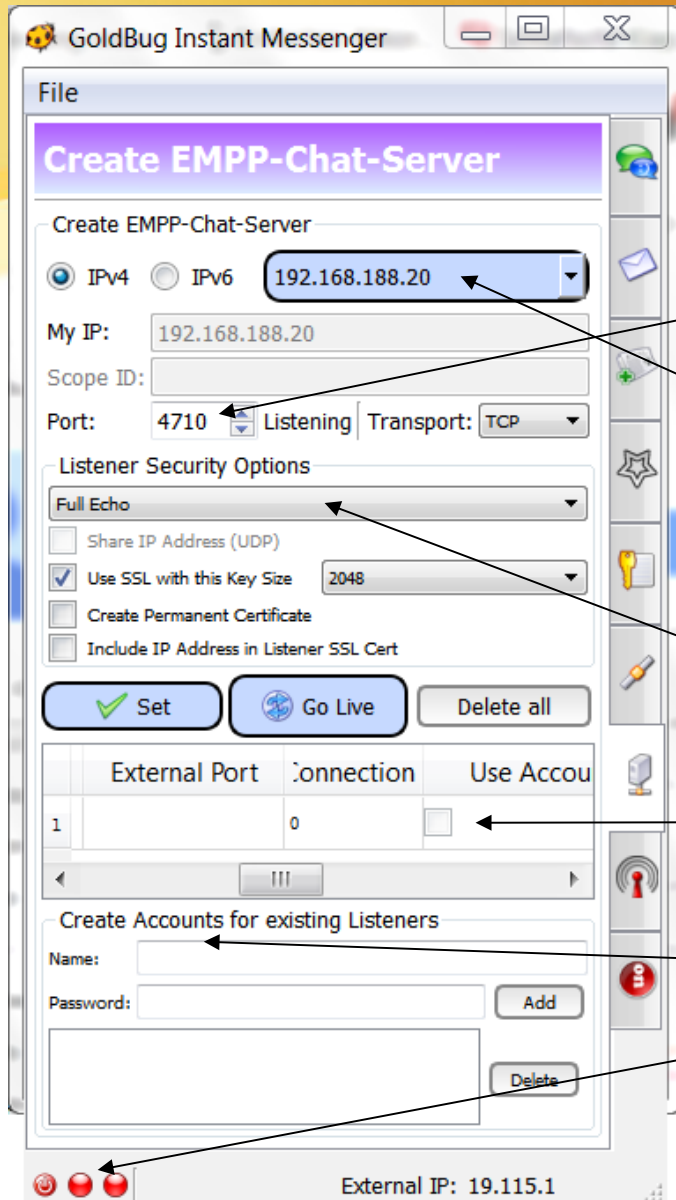
- Chat server/ Listener
 - Accounts
 - connect Neighbor
 - exchange Keys
- further details

EMPP-Chat Server (simple view)?



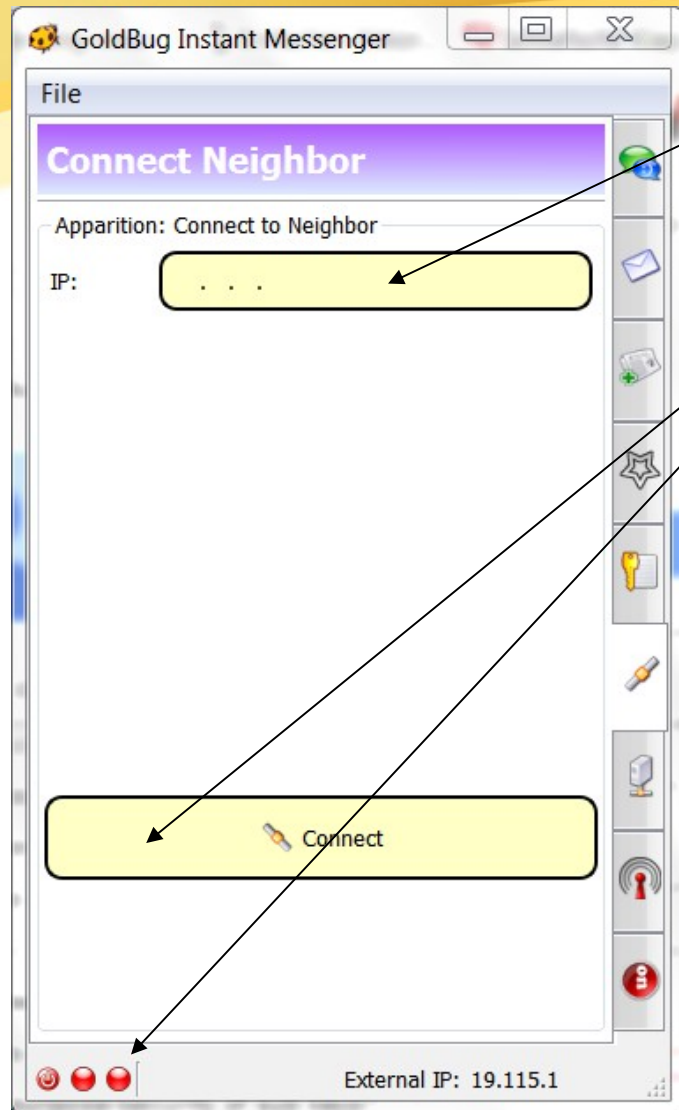
- Let's look at the simple view to create a chat server. It is really simple and you should forward the IP and Port in your router, so you have all 3 LEDs green. Then your friends can reach you even without a third webserver for the chat.
- Use the Pull-Down menu to choose your local device IP.
- Click it into the „My IP“ Textfield.
- GoldBug automatically uses the TCP port 4710.
- Press the button „Set“....
- And you should see the LED in the middle as well green.
- Press now the button „Go Live“, this announces to your online friends, that this Listener/Chat Server has been created by you and the clients from your friends will connect.
- Setting up a chat server has never been so simple.
- Your external IP from the ISP is shown in the status bar. Be sure this is not your local device IP you have in the pulldown menu and you want to enter into the IP field. It must be your internal local device IP

EMPP Chat Server (full view)



- You can connect either as a client to a chat server, or, open up at home your client as a „servent“ (server and client) and create a so called „listener“ for that.
- A Listener is defined by a port. Default GoldBug uses Port 4710.
- To define that, you need to choose from the pull down menu your local device IP-Address and press the button „set“. TCP is best for the transport.
- Maybe you are at home, then you need to forward that Port and IP within your router or Nat. Otherwise your friends cannot reach you.
- When you choose „half echo“ as an option, messages are sent only from client to server, one hop. Messages are not forwarded, that means, your friends can only chat with your directly connected server.
- The Listener table shows you your created listener. With the check box „use accounts“ you also have the option, that your friends connect only with login credentials to your chat server.
- You can create a chat account for your listener in the referring box.
- The LED in the Middle will highlight in green, that you created successfully a listner for your chat server.
- EMPP stands for **E**choed Messaging and Presence Protocol

Connect a Neighbor (simple view)



Set the Graphical User Interface in Settings to „simple view“ and you see, how easy it is to connect to a neighbor, friend or chat server:

- Just enter the IP, (we assume the chat server has default port 4710)
- And press the „Connect“ button
- The right LED gets green.
- That's it. Exchange keys and see your friend online.
- In case a connection will not work, just delete in the path `./spoton` the file „neighbors.db“ . In this encrypted database all the neighbor IP addresses are saved and if you delete it, GoldBug will make it new and you can enter a fresh IP address to connect, which hopefully makes the LED green.

Connect a Neighbor (full view)

To connect to a chat network, to your friend or a chat server you need the IP-Address. Just enter it into the IP field.

Set the port of the chat server, by default it should be 4710.

Your friend could have set up a listener/Chat Server which requires you to define the protocol: TCP or UDP, but normally it should be a TCP Listener, otherwise ask your friend.

The chatserver might drop TCP-SSL connections, which have not a defined SSL key size standard, so you can set the SSL key size which is needed for this server-connection.

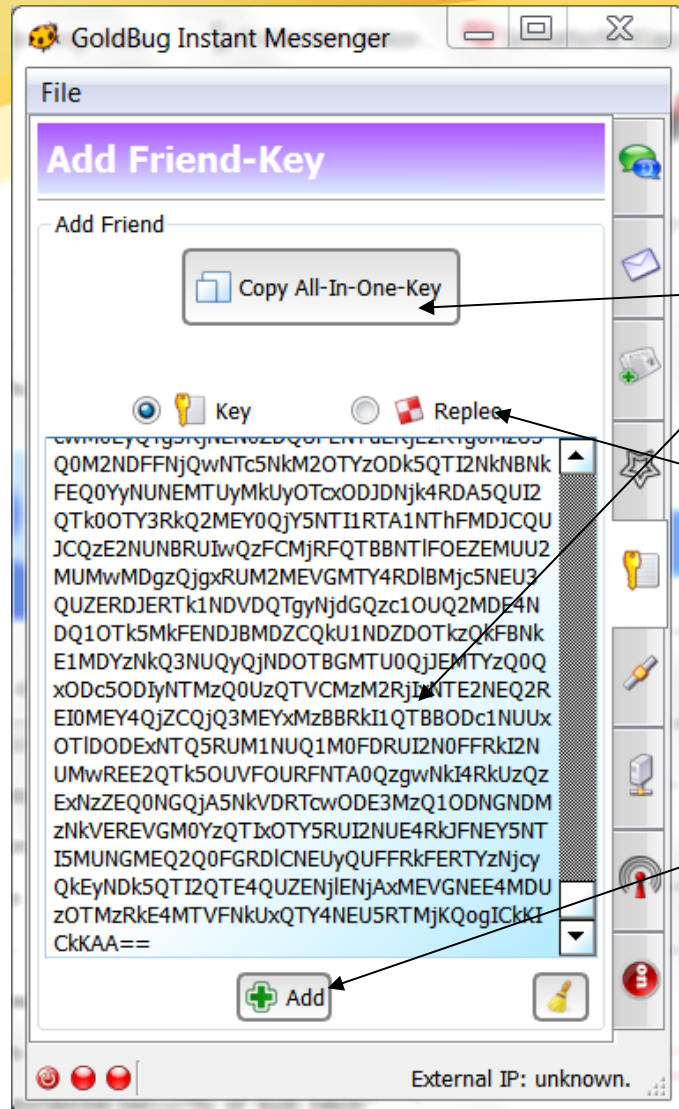
You as well can set, to not connect to chat servers, that have not the SSL key size, you await (as client).

When you choose the half echo, your messages are only sent to the chat server and not to any further node. This means the chat server will be your only direct connected friend, other friends or nodes will not be in the „forwarding-loop“ (echo) and your message is shared only between these two nodes.

If your network requires a proxy, you can add the details and credentials for your connection. This can be used to chat as well over Tor, so the IP address is anonymized and the exitnode of Tor cannot read the message, as it is encrypted by GoldBug. An established TorChat application with end to end encryption that hides your chat at Tor-Exit nodes.

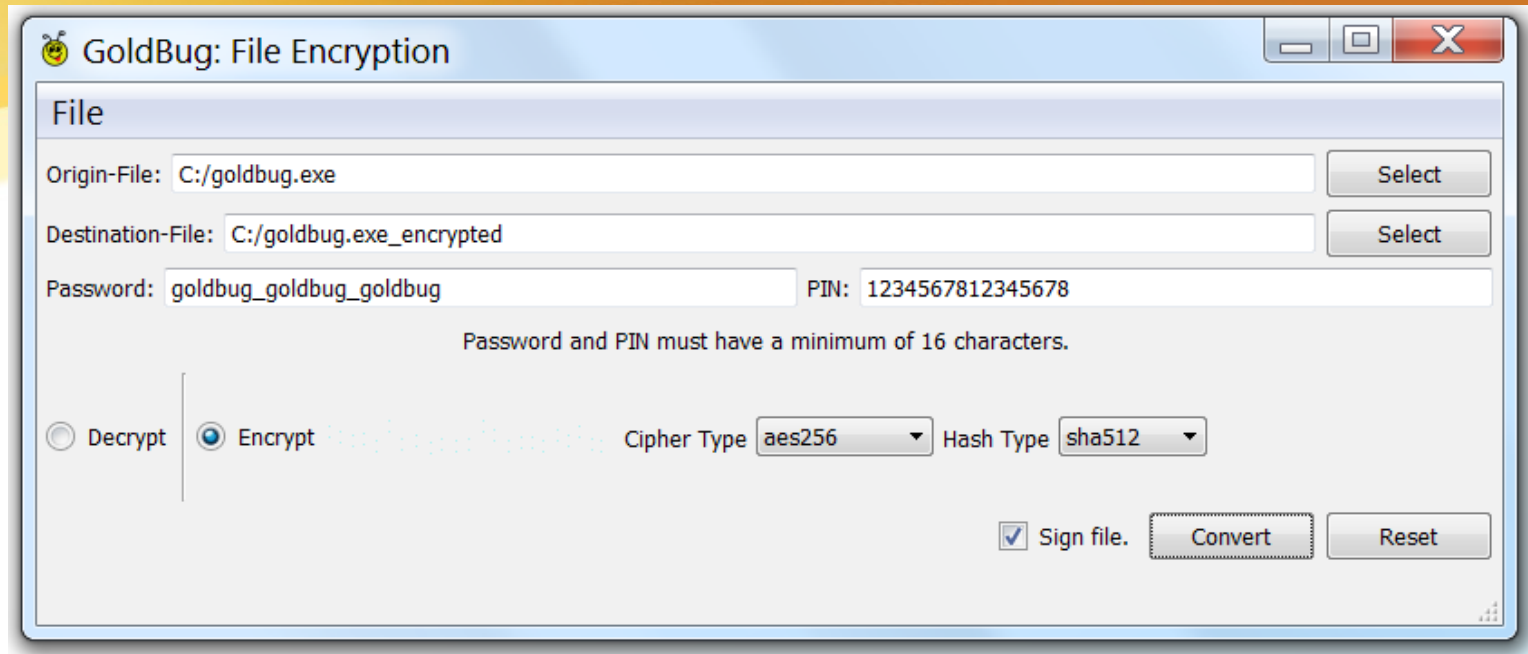
Enter the IP and press the button „connect“ and the right LED gets green.

Exchange Keys



- GoldBug uses a public/private Key infrastructure you know from GnuPG. The public key can be shared and the private one remains encrypted on your machine. For that, it generates several keys (one for email, one for chat etc) at the initial setup.
- There is a button, which has all these keys in one text. Copy the full text of the key and share it with your friend.
- You as well need to get the key of your friend and enter it into the key-box.
- In case you do not want to send your key in plaintext, you can send it encrypted with the key from your friend, you already just got. This is called to make a REPLEO. A repleo is the text of your key, but encrypted with the provided public key of your friend. That means you will not transfer your own key in plaintext. Your public key keeps private.
- A „key“-text starts always with the letter „k“ or „K“ and the Repleo with „r“ or „R“, so you know, which radiobutton to choose, depending on what your friend sends you.
- Press the „Add“ button and see, if the friend is appearing in the chat friends list and in the email „to“-field as a recipient.
- Set your usernames (in the chat and email tab) before you transfer keys, so your friend knows your name. Otherwise by default „unknown“ is written, which will update on connection.

Tools: File Encryption



- Since version 1.0 GoldBug offers under Menu/Tools a File-Encryptor.
- Choose Origin-File, set a Destination-File-Path and convert the file.
- Pin and Password needs at least 16 characters.
- Set (single or multiple) Vectors, Cipher and Hash.
- The tool is an offer for replacing / additionally encrypting unsecure Truecrypt-Containers or to encrypt files before you transfer them – over GoldBug-StarBeam Crypto-Torrents or regular methods like E-Mail or any Uploads to Dropbox, Megaupload etc.

Tools: Rosetta CryptoPad



- Find it under Tools.
- Exchange/Add a Rosetta-Key with/of a Friend.
- Enter Text.
- Convert.
- Post the Output to the Web anywhere. The Paranooids can post a Rosetta-Ciphertext even in Goldbug-Chat.
- Decrypt Vice Versa.
- A slow-chat-Tool.
- Why the name? See Wikipedia. Stone of Rosetta.

Further Implementations & GB Features

- **Accounts:** Enter your password to the account, it is not transferred to the server, just a hash comparison is done on both sides.
- All data on your hard disk (.db files) is strong encrypted.
- **Gemini** (end-to-end encryption key) is secured by a **MAC Gemini Hash**.
- Secure Key Transfer: **Repleo** encrypts your public key.
- Chat over Tor with GoldBug.
- **Instant Forward Secrecy** with MELODICA Button: Change the encryption key end to end whenever you want.
- Set an **additional password for emails** (based on AES).
- Send p2p Emails to offline friends.
- **Email-Signatures:** Decide, if you want to send and receive authenticated emails or just non-authenticated.
- **StarBeam (SB):** Transmit your file into a network of encrypted packets anonymously.
- TCP & UDP transport for the echo protocol: UDP is ideal for echoed VoIP.



MELODICA

Instant Forward Secrecy

- MELODICA stands for **Multi Encrypted Long Distance Calling** and is the button to „call“ a friend.
- This function generates 2 end-to-end Encryption keys, first an AES-256-Key, the Gemini, and the so called MAC-Key, which additionally secures the Gemini transfer.
- The transfer of the Gemini is done within the RSA-/SSL-Encryption.
- Alternatively send a new AES over the actual AES.
- Only end-to-end encrypting apps are secure today.
- The echo protocol provides an environment, in which you can share and renew the passphrase, only two people should know, instantly.
- UDP Transport allows end-to-end encrypted VOIP applications based on the echo protocol & MELODICA calls.

Libspoton-Implementation



- Spot-On is the underlying library for the GoldBug Instant Messenger.
- Spot-On has as well a gui and is full of adjustable options, GoldBug aims to be a desktop/mobile messenger with a smaller set of options to fit mobile or tablet devices.
- Spot-On is a c++ library as an exploratory research project investigating an encrypted communication and data transfer protocol, called the "echo protocol" or short "EMPP" protocol: Echoed Message and Presence Protocol. The package which includes the 'libspot-on' library, is found here: spot-on.sf.net
It enables personal and group messaging, decentral p2p email, echoed IRC/Buzz Chat Channels and secure Filetransfer with multi-encryption (SSL, RSA (PGP / GnuPGP) / ElGamal, AES, libgcrypt, OpenSSL etc). IP Addresses are detached from Encryption Keys. It is programmed in c++ and is the underlying library for chat, email and messaging applications like the GoldBug Instant Messenger App.

Spot-On can be deployed by every c-developer into chat and filesharing apps.

List of criteria for evaluations

1. Tiered application: kernel and user interface processes.
2. Use proxy capabilities?
3. Send email messages to offline friends?
4. Send email with encrypted attachments?
5. Having different Keys for Chat, Email, Cryptopad, Filetransfer etc.?
6. Is the key stuck to your IP Address?
7. Mutual access authentication?
8. No hashing of a file and sending it with hash and senders/receivers ID to neighbors, so it is identifiable?
9. Are there alternatives to RSA, like ElGamal or NTRU? Can a NTRU-user chat to a RSA-user?
10. You can use SSL or not? Selectable SSL ciphers?
11. Selectable hash algorithms?
12. Just need connectivity, no key exchange, keys are optional?
13. You are more autonomous?
14. Trust is not needed, or can be added as you define it?
15. Technical simplicity?
16. Anonymous seeds?
17. You cannot determine, who is reading which message (as you have no destination ID or info added)?
18. Free of Web of Trust-Graphs and no mapping of connections ?
19. Its different, its fun?
20. Local database stores all info in encrypted .db' s?
21. Re-encode support of locally-encrypted data.
22. Optional authentication of messages ?
23. You can communicate without public keys, using Magnets ?
24. Support for TCP and UDP and SCTP communications?
25. Support the multi-layer of encryption
26. Having multi encryption? e.g. SSL + RSA + AES ? Or even Ciphertext over SSL + RSA + AES (Rosetta-Cryptopad ciphertext sent over encrypted channels)?

List of criteria for evaluations

27. Multiple listeners are possible?
28. A kernel is given? Multi-threaded?.
29. IRC-like channels?
30. Simple IP-based firewalls?
31. You can define many points of connections?
32. Do scramblers send out fake messages?.
33. You can store messages in friends ?
34. You have the option to use an end-to-end key for communication?
35. You have the option to renew the end-to-end key each time you want (not only session based)?
36. Encrypted file transfer protocol (StarBeam)?
37. Using a one time magnet (OTM) for a crypto channel?
38. Having ipv6 support?
39. Having Qt 5 and up deployed ?
40. Hops are not forwarding, no routing, is it always a wrap the message new and send to just to your friend?
router-less and forwarding-less protocol?
41. Sending a message to a friend to his dedicated connection and not to all connections?
42. Hiding the key exchange online?
43. Use several encryption keys on one filetransfer?
44. Adding a passphrase on a file transfer ?
45. Use it as client without a listener?

... over 40 criteria, someone could analyse and write about in her/his master thesis - with these different implementations in different tools compared.



The digital encryption
of your private communication
in the context of ...

Principles of the protection of private speech, communication and life (I)

Principles of the protection of private speech, communication and life:

Universal Declaration of Human Rights, 1948 (Art. 12)

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

<http://www.un.org/en/documents/udhr/index.shtml#a12>

http://en.wikipedia.org/wiki/Universal_Declaration_of_Human_Rights

International Covenant on Civil and Political Rights, 1966 (Art. 17)

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

<http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>

http://en.wikipedia.org/wiki/International_Covenant_on_Civil_and_Political_Rights

European Convention on Human Rights, 1950 (Art. 8)

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

<http://conventions.coe.int/treaty/en/Treaties/Html/005.htm>

http://en.wikipedia.org/wiki/European_Convention_on_Human_Rights

Principles of the protection of private speech, communication and life (II)

Charter of Fundamental Rights of the European Union, 2000 (Art. 7, 8)

Article 7. Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8. Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

http://en.wikisource.org/wiki/Charter_of_Fundamental_Rights_of_the_European_Union

http://en.wikipedia.org/wiki/Charter_of_Fundamental_Rights_of_the_European_Union

Basic Law e.g. for the Federal Republic of Germany, 1949 (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1)

Article 2 [Personal freedoms]

(1) Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law.

Article 1 [Human dignity – Human rights – Legally binding force of basic rights]

(1) Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority.

<https://www.btg-bestellservice.de/pdf/80201000.pdf>

http://en.wikipedia.org/wiki/Basic_Law_for_the_Federal_Republic_of_Germany

Secrecy of correspondence - Fernmeldegeheimnis (Art. 10 Abs. 1 Grundgesetz)

§ 88 Abs. 1 Fernmeldegeheimnis - Telekommunikationsgesetz:

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

(4) Befindet sich die Telekommunikationsanlage an Bord eines Wasser- oder Luftfahrzeugs, so besteht die Pflicht zur Wahrung des Geheimnisses nicht gegenüber der Person, die das Fahrzeug führt oder gegenüber ihrer Stellvertretung.

Principles of the protection of private speech, communication and life (III)

§ 206 Verletzung des Post- oder Fernmeldegeheimnisses

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt 1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft, 2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder 3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die 1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen, 2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder 3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigen Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekanntgeworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

http://www.gesetze-im-internet.de/gg/art_10.html
http://en.wikipedia.org/wiki/Secrecy_of_correspondence
<http://de.wikipedia.org/wiki/Briefgeheimnis>
<http://de.wikipedia.org/wiki/Fernmeldegeheimnis>
<http://de.wikipedia.org/wiki/Postgeheimnis>
http://www.gesetze-im-internet.de/tkg_2004/_88.html
http://www.gesetze-im-internet.de/stgb/_206.html

United States Constitution: Search and Seizure (Expectation of Privacy, US Supreme Court)

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

<http://www.usconstitution.net/const.html>



More Information at the
Website
<http://goldbug.sf.net>