30C3 How to CryptoParty

General Topics:

[Entrance is here]
Group 1: Reasons sensability (I have nothing to hide!)

- short story to show "daily situation)
- make handouts (paper is more present than one more URL)
- reasons from work, hobbies,
- bad feeling about what is going on
- Q&A collection (?)
    - Q: if I encrypt everything, wouldn't this make a broken disk a mess for me?
    - A: use a backup system which can handle this

Group 2:

- Discussion about picking the right time slot
    - 3-4 hours per topic not much more
- Importance for Mixed or "Women only" or "eldery cryptoparties"
    - When its 50/50 it works great as well
    - The code of conduct helps
    - Another alternative is to advertise the party as "For women and allies" to put the emphasis but still include everyone
    - Tandems (one young and one old person)
        - For kids (mother/father and kid tandems)
- Having a handout that people can bring home
- People should bring their own machine + power cable
- Make it such that people feel safe to ask any question => e.g. have a cryptcat chatroom for questions
    - also IRC: http://www.cryptoparty.in/communication/irc
        - Need help setting up secure emails, secure instant messaging, browsing the web anonymously, disk encryption or securing your mobile phone? Come and chat with us: http://www.cryptoparty.in/communication/irc
- (Irc might be to difficult for beginners)
    - solution: hint: people that are not familiar with IRC can just click here to chat: https://oftc.net/?channels=cryptoparty in your browser. This works with Torbrowser, too, for added anonymity so if you want to be more secure then you can download and run https://www.torproject.org/projects/torbrowser.html.en before you connect to chat
    - https://**crypto.cat**/
- Make it fun (Alice and Bob dialogue)
- You should not scare people (or tell true stories)
- Be sure to encurage people to use crypto, don't come off as a smartass
- Self hosting
- Teaching how weak is SMTP by default
    - Ask two people (Alice and Bob) in the room and send a message to Bob as AliceuGeneral issues about organizing an event
    - Finding a room
        - University
        - Libraries
        - Community colleges
        - Art centers

[Windows are here (left corner)]
Group 3:

- experience from Freiburg
    - intro on NSA leaks to explain relevance
    - standardise on tools:
        - everybody learns to use pgp in combi with Thunderbird. Even though ppl learn pgp by becoming clickmonkeys, it's a start
- Where to store the private keys, is it safe to store it on your cell
- Point of discussion: is it better to teach normal people some basic data hygiene (anti-tracking browser extensions, strong passwords...) versus teaching them how to use pgp if they won't use it bcs they don't have anyone to email with who also uses it?
- t

Group 4: Real world examples for explaining crypto

- Public/Private-Key Method:
    - Box is being constructed with an open lock, I keep the key to open it. I send the box to other people which put contents into the box and close the padlock. Only I will be able to open the box, since I keep the key.
- Use known exaples to bring unexperienced attendees closer to the topics (enigma etc).

[Windows are here (right corner)]
Group 5:
Discussion & Debate
---
collection of talkinpoints in german translation needed:
http://wiki.piratenpartei.de/Ich_habe_nichts_zu_verbergen!

Predictable arguments, talking points or phrases are often used to justify the further weakening our privacy -- or the spectre of terrorism & sex offenders are used to evoke a fear which will a) stop a conversation on our right to privacy, and b) attempt to garnish our consent for a further loss of privacy. These phrases are usually the following;

If you've nothing to fear, you've nothing to hide.

Paedophiles and terrorists seek privacy, therefore to catch paedophiles there must be a reduction in everyone's privacy.

Paedophiles and terrorists seek privacy, therefore anyone who seeks privacy is suspicious.

Collecting small amounts of personal information isn't a breach of privacy.

Etc.

Privacy concerns effect everyone, and thus far the privacy debate has been framed as a law & order necessity, rather than a debate on a person's rights & liberties -- allowing a person to think these questions do not effect o concern them personally.

| Group6 |
Experience report from previous organizers::

- mode of operation was long debated before (party mode versus lecture style) with its pros and cons

- we came to the conclusion that a short introduction (e.g. "what is a public key?" how does email roughly work, etc) is a good idea and should be followed by a more interactive demo/workshop phase.
- Prefer two speakers sharing their duties over one. This makes the talk typically more lively, even entertaning (sometimes by accident but that's ok) ;)
- we limited ourselves to a single topic per party (at least in the Email/OpenPGP case) because there is just so much to talk about even without explaining the web of trust
- We had some trouble promoting the party. Every time only about 10 people showed up. (It was promoted via local newspaper, Facebook, local radio station, no posters/flyers, though).
- "theater" (we actually brought a physical box and some locks) helped people understand what public/private keys are. works for explaining MITM attacks, too ;)
- Number of people needed (organizers, angels): 2+3, at least one for Windows
- sitting in circle or U-form helps people help each other
- supporter angles are a good idea to avoid disruption. It's bad when the speaker has to go fix other peoples' computer problems.
- Cryptoparties might be at pubs, with beer, or like workshops (maybe also with beer)
- Include warnings about possible compromization of the device, that subject lines are not encrypted, unexpected advances in cryptology might happen, and most importantly: enable encrpytion _before_ writing the Email (or disable draft storage on the server) unless you want unencrypted drafts to be transmitted to your email server!
- Inform the audience where to look for the next party covering possibly other topics.

Different aspects:

- It might be interesting/useful to go into topics of general computer safety. But this needs several sessions, and is slightly off title.
- Idea to explain encryption: lock (public key) and key (private),
- signature: signet in old style letters, or wachs inprint of key
- when inviting for party: ask for inofficial notice of participation, Computer knowledge, System
- possibilities: fixed topic (pro: better prepared, con: people might not be interested) vs. several possible topics and let people choose (con: lot of work to prepare), vs. chaos party (needs people in audience that can help the others)

Commets from Nivatius (wasn't at the c3, organized some Parties)

- having two speakers is a really good idea, one can take questions and remind the other person of things they forget. the change between two people makes it more fun to listen

Tools
=====
1. Private Conversations Over Instant Messaging (OTR/Pidgin/Adium) // DONE
   1.1 Plugin: http://www.cypherpunks.ca/otr/
   1.2 Application: http://www.pidgin.im/
   1.3 More info here: Pidgin (software) :
https://github.com/cryptoparty/handbook/blob/master/src/chapter_12_instant_messaging_encryption/00_setting_up_encrypted_messaging.md
2. Encrypting Emails (PGP/Enigmail/Thunderbird/GPG4USB/GPGTools) // NOW
http://www.mozilla.org/thunderbird/
http://www.enigmail.net/
3. Disk Encryption (Truecrypt)

   Slides: http://www.truecrypt.org/

   Screencast Video : https://www.youtube.com/watch?v=puzx_RSTRHY

4. Privacy Protected Browsing (Tor Browser Bundle)

[Slides]

5. Anonymity Techniques

Group 6.2:

- Focus on what the users want
- Actual encryption maths is not necessarily important - it might be enough to just say what the encryption does (hides content), and does not (hide identities)
- Do standardised/crossplatform tools (Firefox + plugins, not every browser, thunderbird, not outlook/Mail.app/foo)
- It might be a good idea to serialise/make it continuous to build up a community/recurrent group of people, and to grow from time to time

group 7.1: **motivation**/ chaos experts for social challenges and for technology education

- Are "we" responsible?
- Does the society expect solutions from the hacker community? (Esp. considering press/ media coverage at the moment- which could generate expectations)
- Should we train the trainers?

group 7.2: PR/ management of **media/ press/ journalists**

- Decide on inviting press or not inviting press at the beginning of the planning
- Communicate explicitly on press/ media being invited for the event or not (so everyone knows they'll be coming).
- Provide journalists with sufficient information before the event so they can get the (or at least *a*) bigger picture.
- Press/ media need people to communicate with. Try to find someone in your community who is willing to do this.
- Find people who are willing to appear in media (quoted in interviews) (possibly in disguise/ with their pseudonyms), should press/ media be invited for an event.
- None of "us" in the media means that both our ideas will not be spread as good as possible and also that society might think of "us" as a strange crowd. And thus ignoring us or the insight/ information we are willing to share.
- Press/ media do not understand our (not existing) organisational hierarchy. For them the term "chaos" has a negative connotation!

Link collection:

https://bettercrypto.org/
http://cryptoparty.in/
collection of material (german) http://wiki.piratenpartei.de/HowTo_Kryptoparty
Mindmap, cryptoparty howto: http://mind42.com/public/c1203c00-b809-4f0f-b94d-70def8b4e9c1

- improve, translate and edit the handbook: https://github.com/cryptoparty/handbook
- remix cc slides: https://github.com/cryptoparty/slides
- remix cc artwork: https://github.com/cryptoparty/artwork
- remix cc flyers: https://github.com/cryptoparty/flyers

- global map: https://github.com/cryptoparty/cryptoparty.in

https://cryptoparty-hamburg.de/slides/ (German) -> Dev: https://github.com/ccchh/Cryptoparty-Slides
https://www.accessnow.org/pages/protecting-your-security-online

- Collection of *all* Cryptoparty links, applications and tutorials
  https://opleviathan.piratenpad.de/brainstorming-tutorials

irc.oftc.net:6697 #cryptoparty howto here: http://www.cryptoparty.in/communication/irc
https://www.ccczh.ch/Cryptoparty (German, Review of held Cryptoparty)

Nice Demo of RSA Cryptography (German/English):
http://www.cryptool.org/

https://de.wikibooks.org/wiki/Privacy-Handbuch (German, developing phase)

Workshop handouts
https://www.4zm.org/files/2013/cp13-ws-street-smart.pdf (swedish)
https://www.4zm.org/files/2013/cp13-ws-mobile.pdf (swedish)
https://www.cryptoparty.se/ (swedish)

https://kinko.me/ when it only goes live

https://www.coursera.org/course/crypto <- Math courses: how the ciphers work
http://arstechnica.com/security/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/
Some Slides from the "Anti Prism Party" in Karlsruhe: (German)
http://www.anti-prism-party.de/cms/downloads/downloads.html
http://retroshare.sourceforge.net/ < What to do with gpg besides e-mail
https://prism-break.org/
http://sourceforge.net/projects/enigmagpg (gpg encryption on the web. gmail, etc.)
http://www.mailvelope.com/ for people who want to use PGP in GMail
http://retroshare.sourceforge.net/

Material from Göttingen:
http://cryptoparty-goettingen.de/
http://www.ich-hab-doch-nichts-zu-verbergen.de/

Blogpost about CryptoParty Stockholm on The Tor Blog
https://blog.torproject.org/blog/cryptoparty-stockholm (eng)

Press about Stockholm CryptoParty
DN (Dagens Nyheter) - http://blogg.dn.se/teknikbloggen/2013/11/19/tre-torsdagar-for-digitalt-sjalvforsvar/ (swedish)
Ny Teknik - http://www.nyteknik.se/nyheter/it_telekom/allmant/article3793001.ece#comments (swedish)

Video (with slides, in Swedish) from cryptoparty in Umeå:
http://umeahackerspace.se/2013/06/20/video-fran-cryptoparty-1/

http://cryptoparty.in/

https://www.schneier.com/solitaire.html (You can use a deck of cards to play this crypto *and* introduce Bruce Schneier) ((and Neal Stephenson's Cryptonomicon))

Some less technical OpenPGP introduction (sorry, in German language):
http://ubucon.de/2013/programm#openpgp

feminist cryptoparty-slides from vienna (in german) http://de.slideshare.net/Mahriah1/cryptoparty-email-verschlusselung

Agenda today:

- **Focus on which topics** (Where go the typical questions of guests?)
  - Generic crypto
    - What is "secure"? What is not. -> Dos and Don'ts.
    - Keys
    - Random numbers
    - Signatures
    - Hashes
    - MAC
    - Perfect forward secrecy
    - Symmetric/Assymetric Crypto difference
    - The evolution of crypto (ROT-13 ...)
  - PGP/GnuPG
    - enigmail
    - gpgtools
    - what metadata is still plaintext
    - web of trust
  - OTR
    - Pidgin
    - Adium
  - picking good passwords
    - how to remember good passwords
    - how to avoid pitfalls (password which *looks secure*)
    - password safes
    - password generators
  - all the other three letter acronyms :)
  - what to avoid
  - WiFi security
    - protect your network
    - your device is leaking SSIDs
    - rouge APs
    - wardriving
  - VPN
    - ipsec (any good tutorials?)
    - openvpn
    - tinc (I would not recommend it: http://www.tinc-vpn.org/security/)
  - HTTP proxies
  - Mobile phones
  - Smartphones
    - Are they "secure"?
  - git-annex (assistant) http://git-annex.branchable.com/assistant/
  - Cloud
    - CryptoBox
    - Boxcryptor
  - Full-disk encryption
    - TrueCrypt
    - dm-crypt Luks

        - Operating Systems with batteries included
            - Fedora
            - Ubuntu
    - BitLocker
    - FileVault and why not to use it
    - Tahoe-LAFS
- File Encryption
    - USBSticks
    - Dropbox
        - Alternative to Dropbox(spideroak?)
- TLS
    - CAs
    - HTTP(S)
    - StartTLS (SMTP)
- DNSSEC
- Webbrowser (Security)
    - What is a "secure browser"?
    - Plugins
        - HTTPS Everywhere
        - Adblocker
        - Ghostery
        - Javascript blocking
    - Cookies (evercookies... HTML5 file cache etc.)
    - Detect "bad" SSL
        - RC4
        - CAcert
- Secure backup
    - of keys
    - of data

- **Internet anonymity/privacy**
    - What is anonymity in the Inet
        - my Tracks
    - Why is anonymity needed!
    - Programs
        - Tor (be prepared for it, because your attendees will ask for it) (https://www.torproject.org)
        - I2P (www.**i2p**2.de)
        - Freenet (https://**freenet**project.org)
        - Tails (https://tails.boum.org/)
    - Cloudcomputing
    - Do not mix identities
- **Organisation**
    - Prepare your topics
    - Use the existing resources (Like documentation, slides and so on)
    - Tell them why it is important. Be conscious why and when to use crypto.
        - Prepare examples, demos of how easy things are broken.
    - Which type of protection you need for what you want to do.
    - Room
    - Internet connection
    - Place for people to sit
    - Invite the media (including preparation of the recording crew)

        - why not using a "Volkshochschule"/community college as a platform
        - enough laptops/computers
            - OS (Both Worlds)
            - Application
        - code of conduct
        - invite not only friends, invite your mother, daughter, nurses, journalists, teachers of your kids
        - club mate
        - estimate the size of your cryptoparty: how many supporters for how many attendees?
        - food: pizza, pie, soup, cookies :)
- **How to do it**
    - Avoid spreading false premises which would give a false sense of security
    - Make people feel welcome to the cryproparty.
    - Avoid jargon at all cost: It will scare away our target audience.
    - Explain how Public Key encryption works in an easy way: Multiplying two prime numbers creates a secret number because it is hard to find original prime numbers if you only have the product. Not much more is needed in my experience.
    - Try to reuse your (good) examples - once understood it is a base to dig deeper.
    - Explain other "computery" subjects also simply, also without math and jargon. (Example: what are the entitites involved in e-mail?)
    - Use pictures or diagrams!
    - Don't explain to much. Better few things understood than to overwhelm people.
    - Make easy examples for the encryption mechanis. Keep to practicalities, what is usable? For what? (with sticky paper and pens, i.e. ROT13)
    - (Possibly) Keep to practicalities, what is usable? For what?
    - Have people ready to explains many different topics
    - Keep the math simple, usually it's fine to use basic operations.
    - Use the attendees as a resource as supporters: Ask how knows what, and who doesn't know anything about said topic. Assign the expereienced users to support the less experienced ones.
    - Be ready to give background and historical info to unexperienced users to bring them closer to the topics.
    - **do talks together - a non tech and a tech person can be the bridge to everyone ;)**
    - Pickup the attendees where their knowledge is solid.
- **Audience**
    - "crypto party for xxxx" could be an interesting recipe/marketing trick/way to focus on your audience's needs
    - Example: Crypto party organised by Bits of Freedom in Amsterdam specifically for journalists: https://decorrespondent.nl/483/cryptoparty-gemist-hier-twaalf-tips-om-je-digitale-ik-te-beveiligen/14855148-3d809f3c
        - find the journalists writing about tech and privacy
        - organise it as a joint project of your hackerspace and this media outlet
        - Yes, it was a success with 120 participants. Organized by @xbouwman (me). Not a classical lecture setup, but a 30 min talk followed by a open workshop where people could ask questions based on our handout (Dutch) http://we.tl/5pTck5WnVE
    - "CryptoParty als Volkshochschulkurs" (CP as evening school lessons) in contrast to press/ media conveying CryptoParty as something very difficult? (cf. http://www.faz.net/aktuell/rhein-main/crypto-party-anleitung-zur-digitalen-selbstverteidigung-12309561.html). Only suggesting...

20:25 < x> "How to host a cryptoparty": if you are going to be talking about something make sure your explanation is really refined, trying
explaining Tor/Bitcoin/Whatever to a non-technical relative

20:25 < x> if they find it interesting, you're good to go
20:25 < x> it took me ages to work that out and I think I just assumed because I knew what was going on that knowledge would magically
translate into being a good teacher

How to enhance the usability of enigmail???????

Agenda for tomorrow:

- 2013/12/29, 10:00, Early Bird: A Beginner's Guide to Encrypted Communication with CAcert (Hall 14)
  - https://events.ccc.de/congress/2013/wiki/Session:Early_Bird:_A_Beginner%E2%80%99s_Guide_to_Encrypted_Communication_with_CAcert
  - Notes for this session: http://hwz.edupad.ch/cacert
  - PS: Feel free to delete this announcement if you feel it doesn't belong here ;-)

Shameless plug: #PrismCamp (17/18 May 2014, Stuttgart) will provide time & space for a two-day non-stop #CryptoParty

Is there a "one true way" for creating gpg keypair? Maybe follow this blog post:
https://alexcabal.com/creating-the-perfect-gpg-keypair/
Swedish: https://www.dfri.se/dfri/work-in-progress/gpg/gpg-huvudnycklar/ and
https://www.dfri.se/dfri/work-in-progress/gpg/gpg-privatnyckel/
Any further strategies, after creating a good master key, for maintaining a subkey structure (granity, expiration, hierarchy depth) would be nice to have in a write-up.
openpgpg-schulungen explains it in quite some detail.
cryptoctcryp//cr

gpg/Retroshare keys:
Add me as your friend(enemy?)
Philip->

-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: OpenPGP:SDK v0.9

xsBNBFKnh5IBCADEQ+tGk9SYFA7tYHTEZmKMGUgnK469fSIiL/kxX9XdumTkdn7I
HW+xd8/PMh7vsDBzQffMS4xucmn6rtv4bxOefuWueljN+9Fl2ZEqUZxH3JDibPWM
AqFM2tO7KjT6O+GmeGL61jVfa0Stl6svT6QNOTlm/RCbPKJcH+Ue11dalD5p16JW
KxfDZ8IXriJAHGYt4KZ1qh5hutagENDjOKIdncQkuUDSVLKGA13vUON9gvOoXJsJ
ZCuEE0p154FXR7SraJ7yTxpXHXhaVXwLUiKrUY3rWQ4Bgs5hFcR1pyd4O3x0poHq
BVdpB+Crwdyz2SbCbd4jtHqh49ONz/DQgb8xABEBAAHNLFBoaWxpcCBTY2h1YmVs
bCAoR2VuZXJhdGVkIGJ5IFJldHJvU2hhcmUpIDw+wsBfBBMBAgATBQJSp4eSCRAx
h7UPmGRXCwIZAQAAvysH/RrS5uRaUpE9t9uPdDqhePI4F8tvZO/8rnhcNScgKaUl
E8upABIRYLw91O2U5+lL9HtBsZW0RCn2er283H3G5eDXQfObxzwujRJbpYCdIm3s
QEiIU3HAhTFGeFQAohHX9j4mgqTBFawfILkv4pbk6Ufuva8kaMOuUR9mx12qSh2O
PGlXwXIonfGmVKKQMhzrtVefis0QJKksOMui8YV2/Y/4sf6AysZj8Le3djvohhNz
DM2SHLHuhayWsUl56yIS75mREh8y+95Zbuqz1MbDHekinBkjT+5HO9fafReyuoR5
xcEIwv9IjSe4snIdczw6wy5yDIUU+kN/9sBj5uPWR8U=
=NytU
-----END PGP PRIVATE KEY BLOCK-----
--SSLID--238fe6b3ad4000d1d32183df7168cc87;--LOCATION--Laptop;
--LOCAL--151.217.230.144:36278;--EXT--151.217.230.144:36278;

--> seems to be broken

Group from the edge, some feminists

- talk to people
- ask people for their opinions
- CryptoParties for women only (feminist CryptoParty), attracts many women
- small groups, max. 20 people
- one angel per 5 people
- arguments, lawyers, journalists should use encryption because of their function
- https://www.tacticaltech.org/