cryptoparty istanbul_

11 Aralık 2019, TAK

Özcan Oğuz – Özgür Yazılım Derneği

ozcan@oyd.org.tr - 0x3D975818

Özgür Yazılım Derneği

- 2018’de kuruldu.
- İstanbul’da örgütlüdür.
- Kullan, araştır, paylaş, geliştir!
- Türkiye’de özgür yazılım aktivizmi
- Kişisel mahremiyet ve özgürlük
- *İnternet* özgürlüğü
- “Özgür yazılım, özgür toplum”
- Hackerspace Istanbul

Özgür yazılım nedir?

Dört temel özgürlük:

- Kullan
- Araştır
- Paylaş
- Geliştir

Bu özgürlüklerin hepsini sağlayan yazılımlar **özgür yazılımlardır.**

Çalışma alanlarımız neler?

- Özgür yazılım ve GNU
- Özgür donanım (tasarımı)
- Özgür lisanslar
- Özgür sanat
- Özgür *İnternet*
- Mahremiyet ve bireysel özgürlükler
- Ağ tarafsızlığı

Projelerimiz neler?

- Hackerspace Istanbul
- Özgürleşin.org
- Zarola
- CryptoParty Istanbul
- Anadilinde Bilişim
- ...

Kimler için?

- Özgürlük aktivistleri
- Bilişime ilgi duyan insanlar
- Sanatçılar
- Akademi müdahilleri
- Bilim insanları
- Gazeteciler, sendikacılar
- Bilgisayara dokunmuş herkes

Nasıl katkı verebilirsiniz?

İki temel ihtiyaç:
Para ve emek

Emeğim var!

- Toplantılara gelerek fikir ve çözüm önerebilirsiniz.
- Projelere kod, çeviri, sistem, belge ve çözüm katkısı verebilirsiniz.
- Faaliyetlerde görev alabilir, çevrenizi örgütleyebilirsiniz.
- Özgür yazılımı ve derneğimizi anlatabilirsiniz.

Param var!

- Destekçi üyemiz olabilirsiniz.
- **OYD** yazıp **8071**'e göndererek ayda 20 TL bağışta bulunabilirsiniz.
- Ayni veya nakdi bağışta bulunabilirsiniz.
- İlan edilen ihtiyaçları karşılayabilirsiniz.
- https://bagis.oyd.org.tr

Ne lazım?

- **Mekan**: hs.ist'in ve ÖYD'nin fiziksel mekana ihtiyacı var.
- **İnsan**: Emek gücüne ve örgütlenecek insanlara ihtiyacımız var.
- **Para**: Derneğimizin kendini devam ettirebilmesi için paraya ihtiyacı var.
- **Proje**: Aklıma bir şey geldi!

Nasıl üye olabilirim?

- Destekçi üyelik: **`OYD -> 8071`**
- Dernek üyeliği: Çalışmalara ve toplantılara düzenli katılım sağlamak ön koşuldur.
- `https://oyd.org.tr/uyelik`

Hackerspace Istanbul nedir?

- Aralık 2017’de kurulmuş bir hacker kıraathanesi.
- El birliği ile toplanan imkanların bir arada bulunduğu bir atölye (idi).
- Fiziksel olarak 15 Ekim 2018’de gözden kayboldu.
- Kültürel ve geleneksel olarak hala ayaktadır.

CryptoParty nedir?

CryptoParty, dünya çapında yürütülen gayrimerkezi bir harekettir. CryptoParty'lerin amacı, özellikle son kullanıcıların dijital alanlarda kendilerini ve mahremiyetlerini nasıl koruyacakları hakkında bilgi sahibi olmasıdır.

Dünyada CryptoParty

- https://cryptoparty.is
- Dünya çapında 6 kıtada yüzlerce şehirde sürekli olarak düzenlenmektedir.

Ön bilgiler

Şifre != Parola
Özgür yazılım != Açık kaynak
GNU/Linux != Linux
Mahremiyet != Gizlilik

Kriptoloji nedir?

- ΚΡΥΠΤΌΣ + ΛΌΓΟΣ
- *Trk.* Şifrebilim
- Kriptografi ve kriptoanaliz olarak iki alt alanda incelenir.

Temel amaçlar

- Gizlilik
- Bütünlük
- Kimlik denetimi
- İnkar edilebilme/edilememe

Temel kavramlar

- **Açık metin (plaintext)**: Herkes tarafından anlaşılabilir metin.
- **Şifreli metin (ciphertext)**: Şifrelenmiş metin.
- **Anahtar (key)**: Şifreli metni açık metne çevirmek için gereken veri.

Şifreleme çeşitleri

- Anahtarsız şifreleme
- Simetrik şifreleme
- Asimetrik şifreleme

Asimetrik şifreleme

- İki anahtar vardır (anahtar çifti)
- Bir genel anahtar (public key)
- Bir özel anahtar (private key)
- Bir anahtarın şifrelediğini sadece diğeri açabilir
- En yaygın uygulaması RSA’dır

Avantajları

- Anahtar değişimi için önden sözleşmeye gerek yok, genel anahtarlar yeterli
- İmzalama seçeneği

Nasıl çalışır?

- Ali, Bektaş'a bir mesaj gönderirken mesajı Bektaş'ın genel anahtarıyla şifreler.
- Bektaş kendi **özel anahtarıyla** mesajı açar ve okur.
- Bektaş, cevabını Ali'nin genel anahtarıyla şifreler ve gönderir.
- Ali, kendi **özel anahtarıyla** mesajı açar ve okur.

İmzalama nasıl olur?

- Ali, mesajı Bektaş'ın genel anahtarıyla şifreler.
- Ali, mesajın **özetini** kendi **özel anahtarıyla** şifreler ve gönderir.
- Ali'nin özel anahtarıyla şifrelenen bir metni yalnızca Ali'nin genel anahtarı açabilir, Bektaş imzayı doğrular.
- Özet değerinden yararlanarak mesajın bütünlüğünü doğrular.

Özet fonksiyonu

- *İng.* Hash function
- Sonsuz bir uzaydan sınırlı uzunlukta bir çıktı üreten fonksiyonlar
- En basit özet fonksiyonu -> f(x) = 5
- Bizim kullanacağımız özet fonksiyonları **kriptografik özet fonksiyonları**dır.

Özet fonksiyonu

- En yaygın bilineni MD5 ve SHA-1 (Bir dosya indirirken karşımıza çıkmıştır mutlaka)
- Her kriptografik özet fonksiyonunun bir ömrü vardır
- Güncel olarak kullanılan SHA-2 (SHA-256/384/512)

Ne işe yarar?

- Verinin bütünlüğünü doğrulama
- Verinin değiştirilmediğine emin olma

Nerede kullanılır?

- *İnternet* üzerinden bir veriyi indirirken doğrulama için
- Asimetrik şifrelemede imzalamada
- Web sistemlerinde parola güvenliği için
- Git, SVN, Bazaar gibi sürüm takip sistemlerinde
- ...

Nerede kullanılır?

- *İnternet* üzerinden bir veriyi indirirken doğrulama için
- Asimetrik şifrelemede imzalamada
- Web sistemlerinde parola güvenliği için
- Git, SVN, Bazaar gibi sürüm takip sistemlerinde
- ...

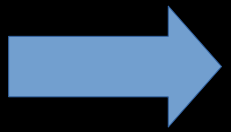
GnuPG Nedir?

- GnuPG, özgür bir kriptografik araçtır.
- Pek çok kriptografik işlem yapılabilecek çok amaçlı bir yazılımdır.

- E-posta şifreleme
- Dosya şifreleme
- Sayısal imzalama
- SSH yetkilendirme
- Güven dağıtımı

GnuPG ne yapar?

Güvenli iletişim haktır.
Haklar verilmez
mücadele ile kazanılır.
Mutlak güven sadece
kişinin kendisine aittir.

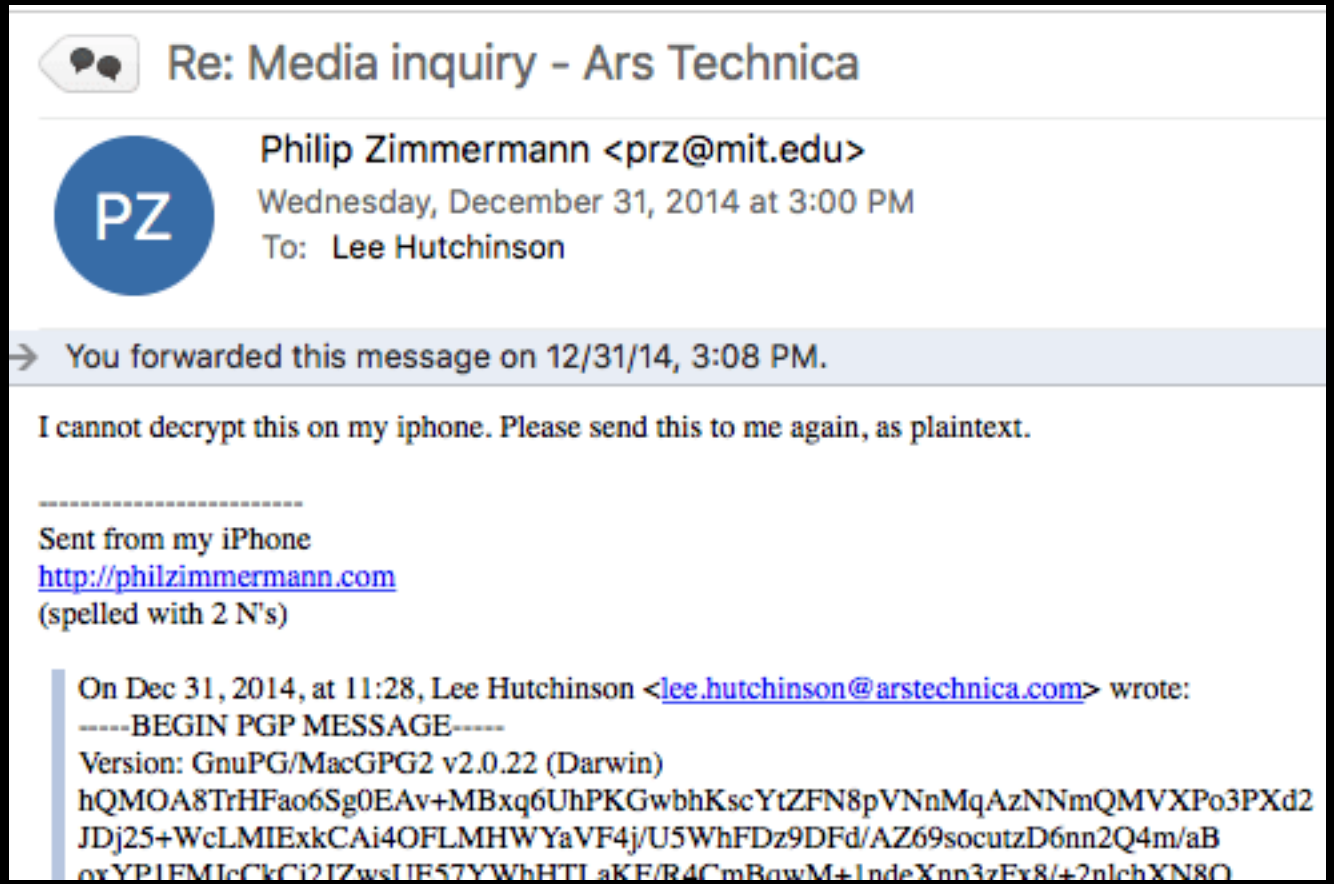


```
-----BEGIN PGP MESSAGE-----

jA0ECQMCcfgb7Vtz5xXu0pwB9pAL
V3Oi6eo7F1qWKepxlYtPPZsJOLO3
Uo+w6kMMH5jkSKU6STiwHBTO2Dxa
JBnFsg3LKL+1UAx0ydCr4vGauogU
f+LmbvyCVmbph+B9Y0Qa7FwR47Ji
44RweGle1d7MDWbfbc7i7StSloEe
fDxVkSOFGQXxCnfzUjT0wlzA4Opx
8aM7omEMekYk6ZcwFtSJ5xf2X5M7
Y/4c/fA==9ucX

-----END PGP MESSAGE-----
```

GnuPG’nin hikayesi

- Körfez savaşı zamanı, ABD’de şifreleme yasaklanmanın eşiğindedir. Bu süreçte Phil Zimmerman PGP’yi yazar ve arkadaşları ile paylaşır.
- PGP dışarı sızar ve tüm dünyaya yayınlanır.
- Amerika Birleşik Devletleri, kanunlarını ihlal ettiği gerekçesiyle; RSA A.Ş ise patent ihlali iddiasıyla Phil Zimmerman’ı dava eder.
- PGP’nin kaynak kodu kitap olarak bastırılır ve düşünce özgürlüğü kapsamında yayınlanır.
- PGP, Phil tarafından satılır ve topluluk GnuPG’yi yaratarak özgürlük mücadelesini sürdürür.

Bu yolda dönenler oldu...



Re: Media inquiry - Ars Technica

PZ

Philip Zimmermann <prz@mit.edu>
Wednesday, December 31, 2014 at 3:00 PM
To: Lee Hutchinson

You forwarded this message on 12/31/14, 3:08 PM.

I cannot decrypt this on my iphone. Please send this to me again, as plaintext.

Sent from my iPhone
http://philzimmermann.com
(spelled with 2 N's)

> On Dec 31, 2014, at 11:28, Lee Hutchinson <lee.hutchinson@arstechnica.com> wrote:
> -----BEGIN PGP MESSAGE-----
> Version: GnuPG/MacGPG2 v2.0.22 (Darwin)
> hQMOA8TrHFao6Sg0EAv+MBxq6UhPKGwbhKscYtZFN8pVNnMqAzNNmQMVXPo3PXd2
> JDj25+WcLMIExkCAi4OFLMHWYaVF4j/U5WhFDz9DFd/AZ69socutzD6nn2Q4m/aB
> oxYP1EMJcCkCi2IZwsUE57YWbHTLaKE/R4CmBqwM+lndeXnp3zEx8/+2nlchXN8O

Nasıl başlayacağız?

- Güvenli bir ortam ayarlayacağız
- Bir anahtar çifti üreteceğiz
- Anahtarımızın yedeğini alacağız
- E-posta şifreleyeceğiz
- İmzalama yapacağız

Güvenli ortam nedir?

- Güvenli ortam yoktur, sadece daha güvenli ortam vardır.
- Tehdit modeliniz neyse güvenli ortamınız ona bağlıdır.

- **Tehlikeniz nedir?**
- Devletler?
- Şirketler?
- Meraklı yakınlarınız?
- Çalıştığınız yer?
- Uzaylılar???

zarola

zarola.oyd.org.tr

Zarola; 7776 tane bilindik kelimeden oluşan bir liste ve zarlar kullanarak, gerçekten rastgele ve güvenli parolalar üretmenin en kolay yoludur.

Gerekli Yazılımlar

Masaüstü

- Kleopatra
- Thunderbird
    - Enigmail Eklentisi

Android

- F-Droid
- OpenKeychain
- K-9 Mail

11 Aralık 2019, Kadıköy
Mustafa Akgül'ün anısına...
Hepinize teşekkürlerle!