cryptoparty istanbul_

5 Ekim 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
- ...

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.

Akış

- Kriptoloji nedir?
- Tarihten bugüne şifreleme
- Caesar şifreleme yöntemi
- Vigeneré şifreleme yöntemi
- Simetrik şifreleme (AES)
- Diffie-Hellman anahtar değişimi
- Asimetrik şifreleme (RSA)

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.

Kriptografi nedir?

- İlgili verinin, üçüncü şahıslar tarafından anlaşılamayacak biçime dönüştürülmesi için kullanılan yöntemler ve teknikler.

Kriptanaliz nedir?

- Kriptografik sistemlerin ve şifrelenmiş metinlerin çözülmesi, ilgili sistemlerin güvenliğinin araştırılması ve zayıflıklarının tespitini yapan bir dal.
- Anahtara sahip olmaksızın bir şifrelenmiş veriyi çözme bilimi.

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

Caesar şifreleme yöntemi

- Açık metindeki her harf alfabede n kadar kaydırılarak şifreli metin elde edilir. Anahtarsız bir yöntemdir.
- M.Ö 100-44 yılları arasında ortaya çıktı.

Caesar şifreleme yöntemi

ABCDEFGHIKLMNOPQRSTVYZ
DEFGHIKLMNOPQRSTVYZABC

n=3 için;

CRYPTOPARTY -> FVBSZRSDVZB

Vigènere şifreleme yöntemi

- Giovan Battista Bellaso tarafından ilk defa 1553’te ortaya atıldı.
- 19. yüzyılda Blaise de Vigènere’in adı verildi.
- Polialfabetik şifreleme olarak anılır. Anahtarlı bir yöntemdir.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigènere şifreleme yöntemi

- Tekrarlar sayesinde kriptanalistler tarafından bilgisayarların yardımıyla çok rahatlıkla kırılabilmektedir.
- Gilbert Vernam tarafından 20. yüzyılın başında genişletilmiştir.

Vernam şifreleme yöntemi

- Gilbert Vernam tarafından Vigenere üzerine geliştirilmiştir.
- Kırılması teorik olarak **imkansızdır**.
- Anahtar uzunluğu ile açık metin uzunluğunun eşitliğine ve mantıksal “ya da” (XOR) işlemine dayanır.

Vernam şifreleme yöntemi

p	q	p⊕q
1	1	0
1	0	1
0	1	1
0	0	0

açık metin: 1101011001
anahtar : 1011100010

şif. metin: 0110111011

Simetrik şifreleme

- Simetrik şifrelemede aynı anahtar hem şifreler hem çözer
- En yaygın uygulaması AES (Advanced Encryption Standard)
- Blok şifreleme ve akan şifreleme kavramları

Temel eksikler

- Anahtar değişimi sorunu
- Anahtar olmaksızın şifreleme gerçekleşemiyor
- Taraflar önceden anlaşmak zorunda

Diffie-Hellman

- Anahtar değişimi sorununa bir çözüm getiriyor
- Mod işlemine dayanır
- Güvenli olmayan bir yol üzerinden simetrik bir anahtarı değiştirmek için kullanılır

Diffie-Hellman

- Ortak bir renk belirlenir (Sarı)
- Ali ve Bektaş birer özel renk belirler (Kırmızı ve Mavi)
- Bu renklere ortak rengi eklerler (Turuncu ve Yeşil)
- Bu oluşan renkleri birbirilerine gönderirler
- Her biri kendi özel rengini bu gelen renklere ekler
- İki taraf da aynı rengi elde eder (Kahverengi)

Diffie-Hellman

- İki taraf da ortaya iki adet sayı atar (p=23 g=5)
- Ali, kendine özel bir sayı (a) seçer ve g^a mod p işlemini yaparak Bektaş'a gönderir (5^6 mod 23 = 8)
- Bektaş da kendine özel bir sayı (b) seçer ve g^b mod p işlemini yaparak Ali'ye gönderir (5^15 mod 23 = 19)

Diffie-Hellman

- Ali, Bektaş'tan gelen anahtarı (x) kullanarak x^a mod p işlemini yapar (19^6 mod 23 = 2)
- Bektaş, Ali'den gelen anahtarı (y) kullanarak y^b mod p işlemini yapar (8^15 mod 23 = 2)
- Her iki taraf da aynı sayıyı elde eder
- Dışarıdan bakan birisi 23, 5, 8 ve 19'dan başka bir veri elde edemez

Eksikleri

- İki taraf da anahtar değişimine dahil olmak zorunda
- Yine anlaşma ve kararlaştırma gereksinimi var

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
- ...

Birkaç küçük tavsiye

- Özgür yazılımlar kullanın
- Parola yöneticisi kullanın
- Parola yöneticinizi bir Zarola ile koruyun
- Sabit diskinizi şifreleyin
- GNU/Linux’a geçin!

5 Ekim 2019, Kadıköy
Mustafa Akgül'ün anısına...
Hepinize teşekkürlerle!