

Parola Güvenliği ve Şifreleme

Bilgi güvenliği AKADEMİSİ

Amaç

- Şifrelemenin güvenlikteki yeri ve algoritma çeşitlerinin öğrenilmesi
- Günümüzde yoğun kullanılan şifreleme algoritmalarının çalışma mantığı
- PKI, sayısal sertifika, zaman damgası gibi kavramların arkaplanı

İçerik

- Şifreleme ve Şifre Çözme
- Şifreleme Algoritmaları
- Şifreleme Çeşitleri
- Tek yönlü şifreleme fonksiyonları
- Encoding/Decoding
- Şifreleme Encoding farkları
- Disk Şifreleme/Stenografi
- Windows/Linux/Cisco parola güvenliği



Genel Terim ve Tanımlar

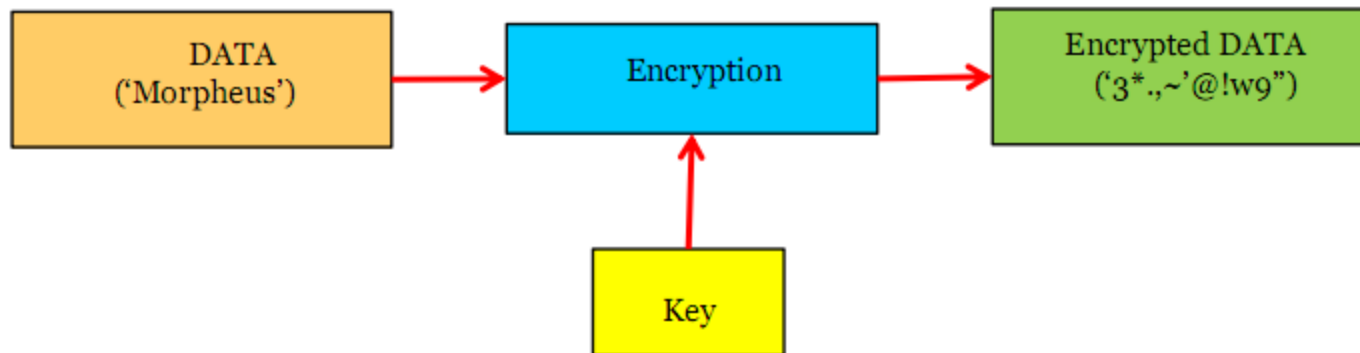
- Kriptografi:
- Şifreleme
- Anahtar:
- Hash:
- PlainText/ChipherText
- Message Digest

Şifre Bilim(Cryptography)

- Düz okunabilir/binary dosyaları başlarının anlayamacağı şekle sokma sanatı(şifreleme)
- Tabanı matematiksel algoritmalara dayanır
- Şifreyi çözme için bir ya da birden fazla anahtar gerekebilir

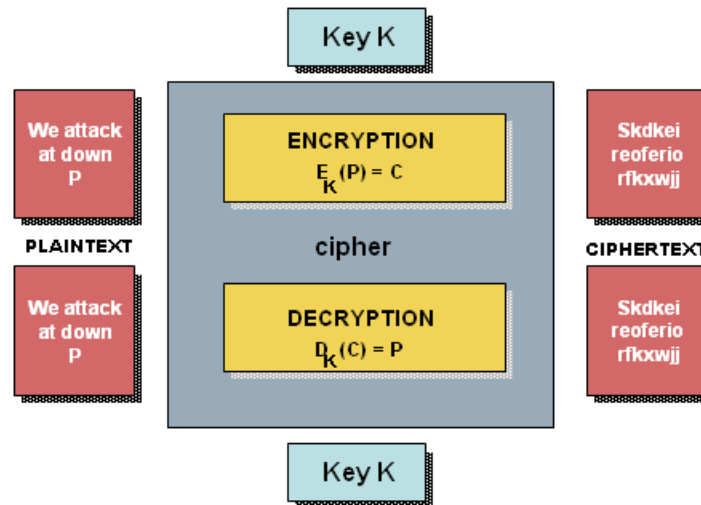
Şifreleme

- Plain Text= Şifrelenmemiş veri
- CipherText Şifrelenmiş veri
- Şifreleme ve şifreyi çözmek için anahtar kullanılır. Bu anahtar aynı olabileceği gibi farklı da olabilir



Şifre Çözme

- Şifrelenmiş veriden orjinal veriyi elde etme yöntemi
- Şifrelenmiş veri anahtar kullanılarak orjinali elde edilir.



Şifreleme Algoritmaları

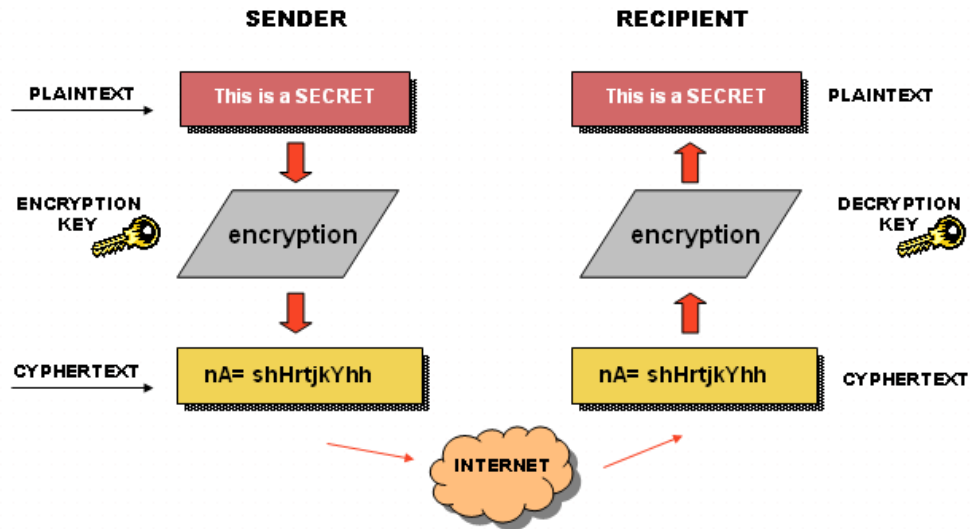
- Simetrik Şifreleme
- Açık/Gizli Anahtar Altyapısı(Asimetrik şifreleme)
- Tek yönlü şifreleme(Hash fonksiyonları)
- Şifrelemenin güvenlik derecesi?
 - Hangi şifreleme daha güvenlidir? Neden?
- Şifrelemede Performans/hızın önemi

Şifrelemenin Kuvveti

- Şifrelemenin sağlamlığını ölçme
 - Anahtarı kırma(kaba kuvvet)
 - Anahtarı matematiksel olarak elde etme yollarıyla yapılır
- Anahtar uzunluğu bit ile ölçülür
- Anahtar uzunluğu sabit ya da değişken olabilir(DES vs RC5)
 - DES(56 bit) 2^{56} olası değer = 72 quadrilyon

Simetrik Şifreleme

- Şifreleme ve çözme için eş anahtar kullanımı
- İlk şifreleme yöntemlerinden
- Anahtar gizli tutulmalı ve gizli yollardan paylaşılmalı
- DES



DES(Data Encryption Standart)

- Simetrik şifreleme için kullanılan defakto algoritma
- DES kırıldığı('88) için 3DES kullanılır
- Block size 64 bitdir, bunun 8 biti hata yakalama için kullanılır. Gerçek block size 56 bit.
- Günümüzde DES yerine daha hızlı ve güvenilir olan AES kullanılmaktadır

OpenSSL DES Uygulaması

```
root@bt:~# cat secret
Burada anahtar var ama cok gizli
root@bt:~#
root@bt:~#
root@bt:~# openssl enc -e -des -in secret -out secret.des
enter des-cbc encryption password:
Verifying - enter des-cbc encryption password:
root@bt:~#
root@bt:~# cat secret.des
Salted__yİ/Q
éK=HD·î^J,0ç8FMpñ\úi°xăúûöøöiém;-
root@bt:~#
```

Dosya içeriği anlaşılmaz

```
root@bt:~# openssl enc -a -des -in secret -out secret_text.des
enter des-cbc encryption password:
Verifying - enter des-cbc encryption password:
root@bt:~#
root@bt:~#
root@bt:~#
root@bt:~# cat secret_text.des
U2FsdGVkX18JVhNqE5xEakbJC70hDiKqjCP6S00BAv1Ga62cD+dKFOqKp0S3oabN
wcD/Lwnvt1s=
root@bt:~#
```

Şifreli dosya içeriğinin text olması istenirse -a eklenir.

Şifrelenmiş dosyayı openssl ile açmak için -d parametresi kullanılır

AES(Advanced Encryption Standard)

- DES yerine kullanılmaktadır
- Anahtar uzunlukları:128, 192 ve 256 bit olabilmektedir.
- Matematiksel algoritma olarak Rjindael kullanılmaktadır

OpenSSL AES Uygulaması

```
root@bt:~# cat secret
Burada anahtar var ama cok gizli
root@bt:~#
root@bt:~#
root@bt:~# openssl enc -a -aes128 -in secret -out secret_text.des
enter aes-128-cbc encryption password:
Verifying - enter aes-128-cbc encryption password:
root@bt:~#
root@bt:~#
root@bt:~#
root@bt:~# cat secret_text.des
U2FsdGVkX1+emfYVEH3c6JPIjYD+xkCoRmMnCtNpqWu2aRG7iQY8jJuPZ7KjC60G
vBC54tVv0uokBD0GZxygsQ==
root@bt:~#
```

AES Çeşitleri

Cipher Types

-aes-128-cbc	-aes-128-cfb	-aes-128-cfb1
-aes-128-cfb8	-aes-128-ecb	-aes-128-ofb
-aes-192-cbc	-aes-192-cfb	-aes-192-cfb1
-aes-192-cfb8	-aes-192-ecb	-aes-192-ofb
-aes-256-cbc	-aes-256-cfb	-aes-256-cfb1
-aes-256-cfb8	-aes-256-ecb	-aes-256-ofb
-aes128	-aes192	-aes256

Diffie Hellman

- Nedir?
 - Anahtar değişim algoritmasıdır
- Neden kullanılır?
 - Simetrik şifreleme kullanılan ortamlarda gizli anahtarın iki taraf arasında başkaları ele geçiremeyecek şekilde paylaşılması
- Matematiksel ifadesi
 - İki taraf anahtarı paylaşırken ortadaki adam saldırılarından etkilenmemesi gerekir



Simetrik Algoritma Değerlendirme

- Avantajları:
 - Matematiksel olarak hızlı hesaplanabilme özelliği
 - Kullanım kolaylığı
 - Daha az kaynak tüketimi
- Dezavantajları
 - Anahtar gizliliği ve dağıtım zorluğu
 - Onlarca insanın erişmesi gereken bir veriye sadece tek bir “ortak” anahtarla erişme zorunluluğu.

Açık Anahtarlı Şifreleme

- **(PKI: Public Key Infrastructure)**
- Veriyi şifrelemek ve çözmek için farklı anahtarlar kullanılır.
- Matematiksel olarak açık anahtardan gizli anahtar elde edilemez.
- Açık anahtar kullanılarak şifrelenen veri gizli anahtar kullanarak açılabilir.
- Priv. Key kullanarak imzalanan veri pub key kullanarak kontrol edilebilir.
- En bilineni RSA'dır.

Anahtarlar

- Gizli anahtar:
 - Gizlenmeli ve sadece sahibi tarafından bilinmeli
 - Mümkünse Token/smartcard gibi güvenilir ortamlarda saklanmalı.
- Açık anahtar:
 - Herkese açık, ulaşılabilir yerlerde bulunmalı.
 - İletişimde bulunacak iki kişinin mutlaka açık anahtarlarını biliyor olması gerekir.

RSA

- Ron Rivest, Adi Shamir ve Lenoard Adleman tarafından bulunmuş ve aynı isimde şirket kurulmuştur.
- Günümüzde en sık kullanılan açık anahtarlı şifreleme altyapısı.
- Güvenliği, tam sayıları çarpanlarına ayırmanın algoritmik zorluğuna dayanır.
- Şifreleme ve sayısal imza amaçlı kullanılabilir.

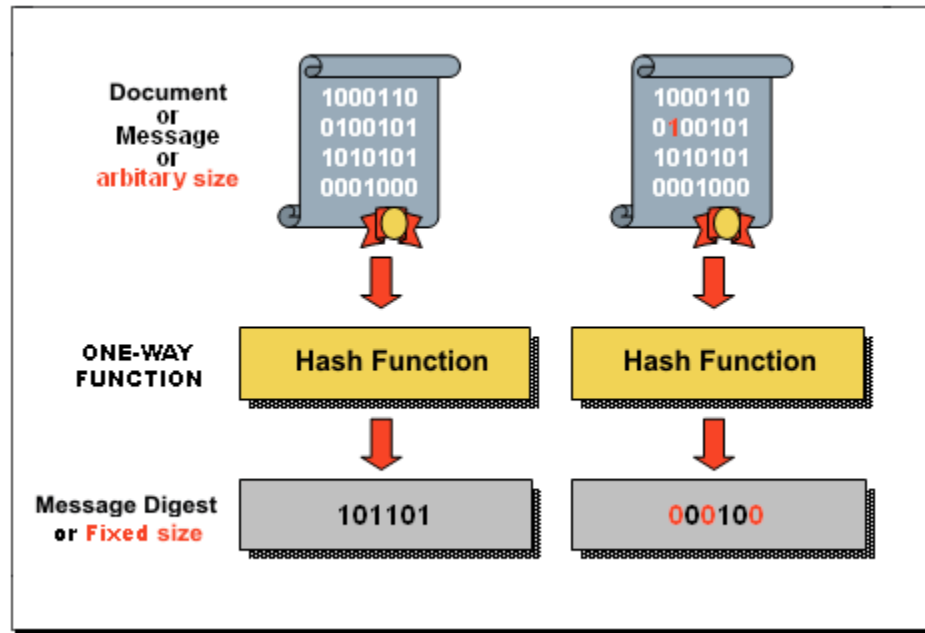
Açık/Gizli Şifreleme Değerlendirme

- Avantajları:
 - Anahtar dağıtımı kolay
 - Anahtar gizliliği sağlanmakta ve her birey kendi anahtarıyla veriyi şifreleme/çözme yapabilmekte.
- Dezavantajları
 - Daha fazla kaynak gereksinimi.
 - Şifrelenen verinin boyutunun artması.

Tek yönlü şifreleme(Hash fonksiyonları)

- Matematiksel olarak tek yönlü hesaplanan algoritmalarıdır.
- Bütünlük doğrulama için kullanılır.(Integrity)
- Verilen bir text/verinin özetini alır ve verinin boyutundan bağımsız olarak aynı uzunlukta çıktı üretir.
- Şifreleme için kullanılmazlar(Gizlilik sağlamaz).
- Sayısal imzalama (Digital signature) için kullanılır, Message Authentication Code(MAC)
- “Message digest”, “One way hash” olarak da adlandırılır.

Message Digest/Hash



```
root@bt:~# echo huzeyfe|md5sum
cc33aa30e69ff51055dd3fb12e148f35 -
```

Bir “bit” in değişmesi özütde %50 değişikliğe sebep olur

Hash Fonksiyonlar

- dgst, md5, md4, md2, sha1, sha, mdc2, ripemd160
- Md5=128 bit çıktı üretir
- Sha1=160?
- Sha512

```
root@bt:~# md5sum /etc/passwd
86f51692f6fecba888794d16f4b058ce /etc/passwd
root@bt:~#
root@bt:~#
root@bt:~# sha256sum /etc/passwd
d3f726278c5d6d908c15f2356eae145361658a50c3309ff3dba1262477b2cf83 /etc/passwd
root@bt:~#
root@bt:~#
root@bt:~#
```

Hash Hesaplayıcı

HashCalc

Data Format: File Data: []

☐ HMAC Key Format: Text string Key: []

☒ MD5 []

☐ MD4 []

☒ SHA1 []

☐ SHA256 []

☐ SHA384 []

☐ SHA512 []

☒ RIPEMD160 []

☐ PANAMA []

☐ TIGER []

☐ MD2 []

☐ ADLER32 []

☒ CRC32 []

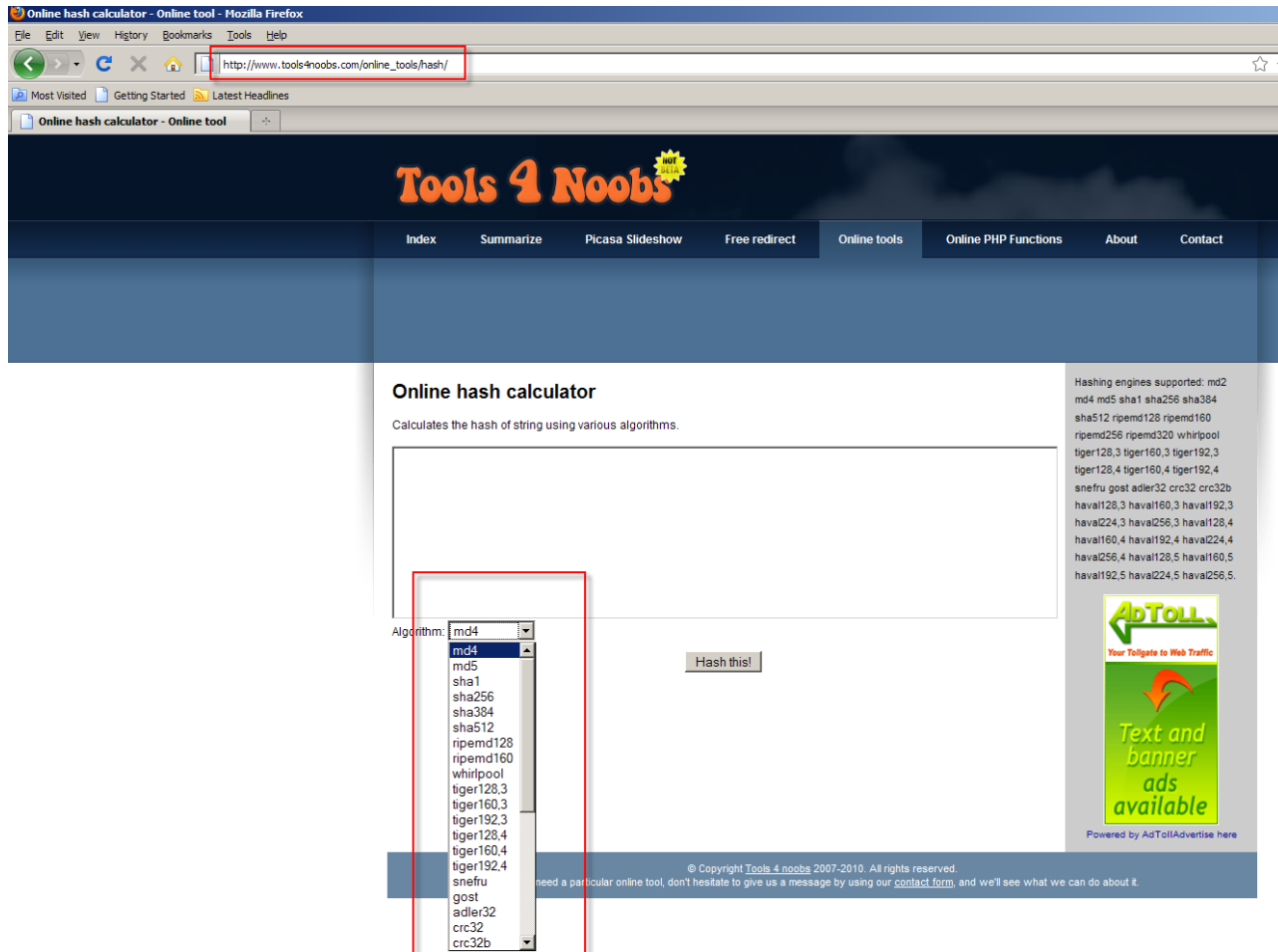
☐ eDonkey/
eMule []

SlavaSoft **HashCalc** - Hash, CRC, and HMAC Calculator - [[Bu sayfanın çevirisini yap](#)]

Calculator to compute message digests, checksums and HMACs for files, as well as for text and hex strings.

www.slavaSoft.com/hashcalc/index.htm - [Önbellek](#) - [Benzer](#)

Online HASH Hesaplayıcılar



Online Hash Cracker

Hashkiller

Welcome, [Guest](#). Please [login](#) or [register](#).
Did you miss your [activation email](#)?
January 26, 2010, 18:09:01 pm

[Webcrack](#) [Opencrack](#) [Forum](#) [Hashes](#) [Downloads](#) [Chat](#) [About](#) [Stats](#)

[Register](#) [Login](#)

Letzte Beiträge - Subject	Board name	Author	Date	Replies	Views
◆ small and good wordlist	Wordlists	-\$plc3-	Today at 16:36:04	5	488
◆ a few ipb hashes	salted MD5	lawlwtf	Today at 13:48:02	0	10
◆ Habe eine "Datenbank" aber wüsste genaueres	Hashcracking Allgemein	Hans	Today at 12:50:32	1	33
◆ 10X md5	MD5	falw	Today at 08:27:52	0	31
◆ Which type of these hashes and who can crack them?	OpenCrack	scibailstein	Today at 07:37:56	0	15
◆ Which type of these hashes and who can crack them?	OpenCrack	scibailstein	Today at 07:35:16	0	7
◆ wordpress 3xhash help	salted MD5	kkss2008	Today at 05:07:31	0	13

Hashkiller

Hashcat

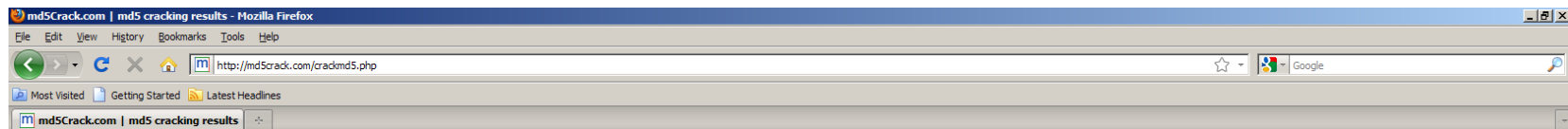
◆ Announcements Release Notes and Info like that goes in here <i>Moderators: atom, hakre</i>	18 Posts 5 Topics	Last post by K9 in Re: hashcat-gui v0.2.419 on January 23, 2010, 12:35:59 pm
◆ General all the general discussion goes in here	68 Posts 21 Topics	Last post by fooble in Re: Closing without erro... on Yesterday at 15:10:12
◆ Feature Requests Want hashcat to cook for you or carry the trash out? Request it here! :)	39 Posts 11 Topics	Last post by Sc00bz in Re: Precompute dictionari... on January 24, 2010, 00:22:44 am

English

◆ Site: News site-related News	4 Posts 2 Topics	Last post by legion in Problems with registerin... on January 24, 2010, 12:53:28 pm
◆ Site: Feedback Post your feedback about this site here	40 Posts 7 Topics	Last post by fooble in Re: Bug at Opencrack on January 23, 2010, 01:55:25 am
◆ OpenCrack Everyone cracks a piece... :)	207 Posts 79 Topics	Last post by scibailstein in Which type of these hash... on Today at 07:37:56
◆ Hashcracking Here you can ask others to help you with specific, hard hashes	2691 Posts 1067 Topics	Last post by lawlwtf in a few ipb hashes on Today at 13:48:02

Child Boards: MD5, salted MD5, common Web Software, LM / NTLM, other Hashes

Google Md5Crack



md5crack

Using Google to crack passwords.

0192023a7bbd73250516f069df18b500

Crack that hash baby!

Generate MD5 Hash

Your Results

Found: md5("admin123") = 0192023a7bbd73250516f069df18b500

Don't know your md5 hash is? [Read here!](#)

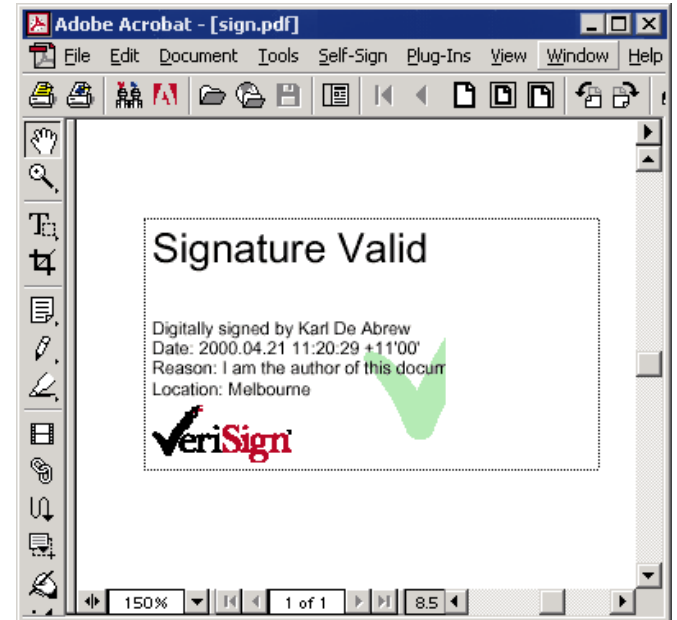
[Whats my md5?](#) - [md5 Calculator](#)

[md5, md4, sha-1 Calculator](#) - [md5 Hash Algorithm](#) - [About md5Crack.com](#)

©2008 [Md5Crack.com](#)

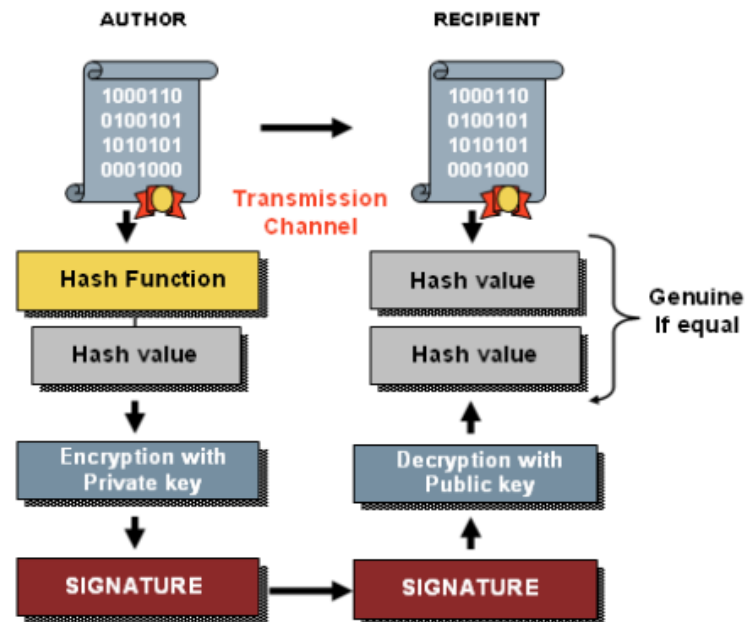
Sayısal İmza Kavramı

- Sayısal imza;
 - Mesajın kimden geldiğinin doğrulanmasını,
 - Mesajın içeriğinin değiştirilmediğini,
 - İmzalanan mesajın red edilememesini sağlar.

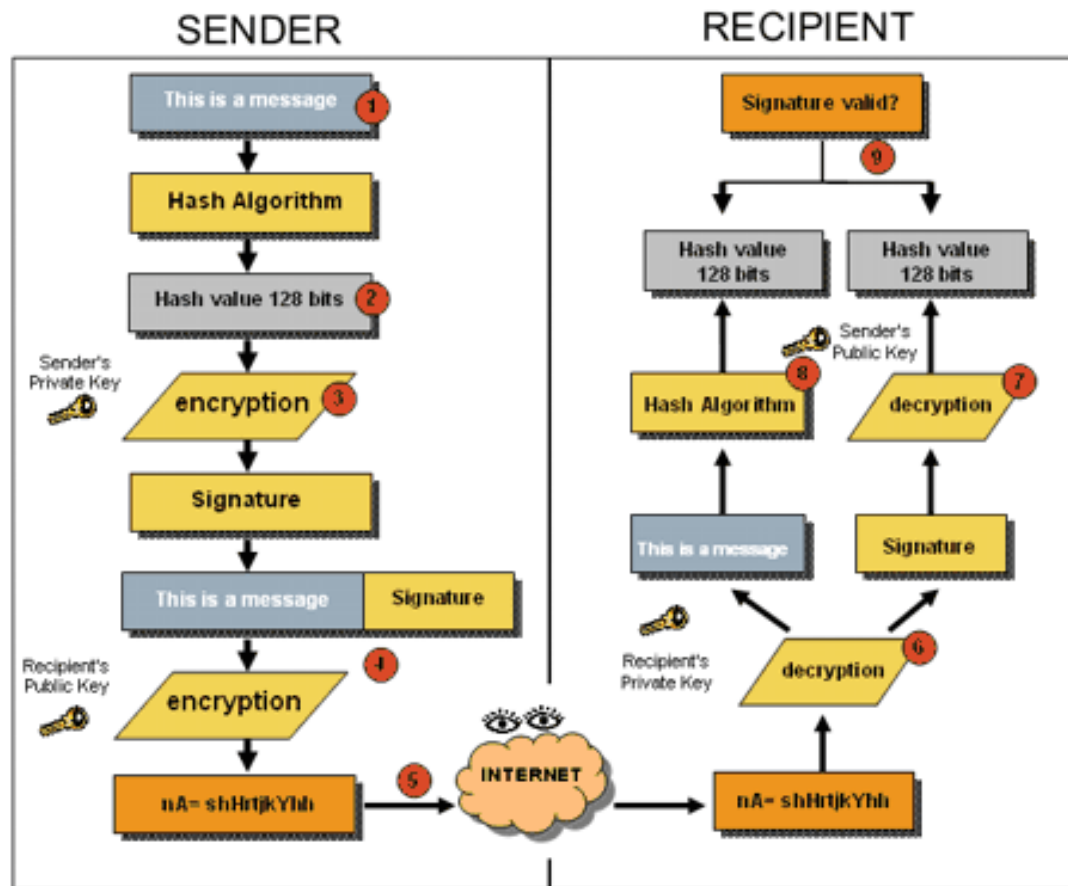
A handwritten signature in black ink, appearing to be 'Karl De Abrew', is shown on the left side of the diagram.

Teknik Olarak Sayısal İmza

- Sayısal imza: Bir verinin hash değerinin gizli anahtarla şifrelenmesi.
- Sayısal imzalı veri imzalayanın açık anahtarı elde edilerek kontrol edilir.



Şifreleme ve İmzalama

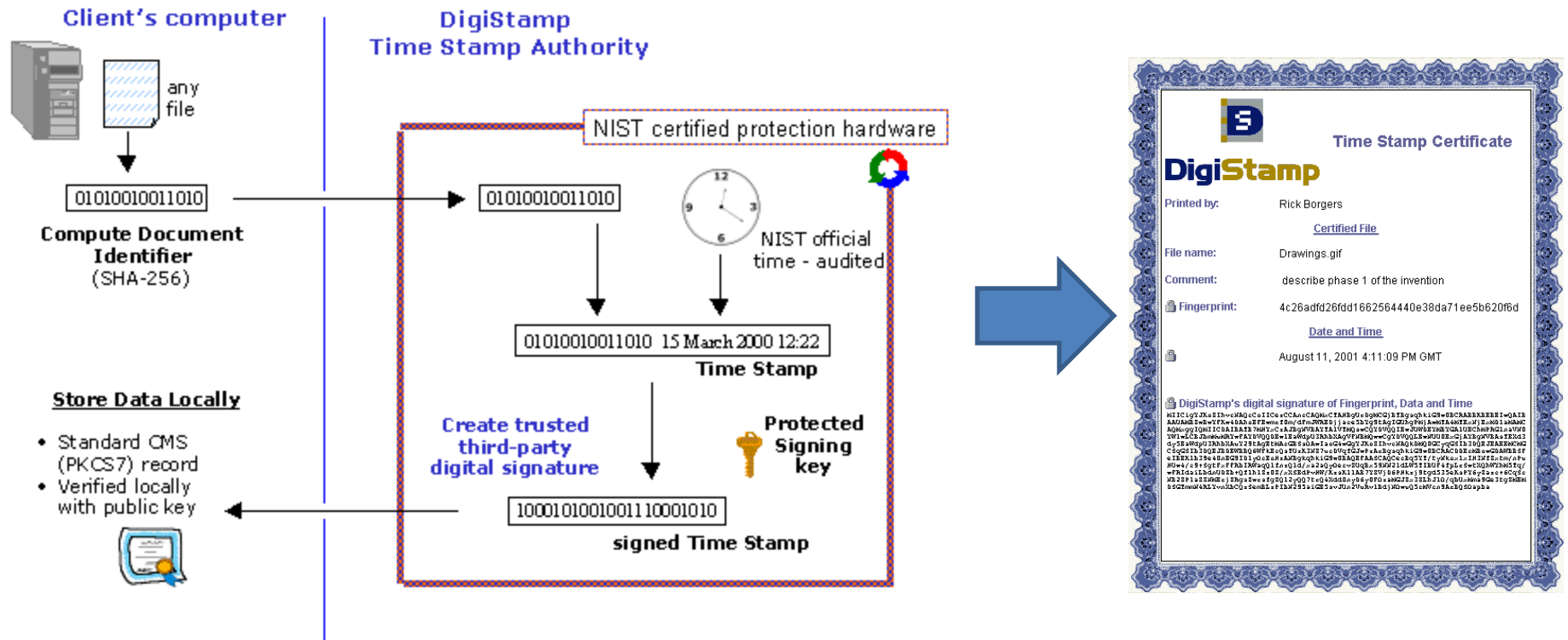


Sayısal Zaman Damgası

- 5651 sayılı kanunla hayatımıza giren tanım...
 - Internet logları* çeşitli sistemlerden alınıp zaman damgası eklenerek saklanmalı
- Amaç?
 - Sayısal olarak yapılan bir işin X zamanında yapıldığı ve o tarihten sonra değiştirilmediğini belirlemek.
- Nasıl Çalışır? ->



DTS Nasıl Çalışır?



DTS=Digital TimeStamp Service

Openssl ile zaman damgası

- <http://blog.lifeoverip.net/2008/11/10/5651-sayili-kanun-gereksinimleri-icin-loglari-imzalamak/>

Bölüm:z Encoding

- Bir veriyi başka formatlarda gösterme işlemidir
- Geriye çevrilebilir algoritmalarıdır.
- Encoding algoritması ek bir gizlilik sağlamaz.
- Base64 encoding, url encoding, hex encoding en sık karşılaşılan çeşitlerdir.

base36	base62	base64	base999	dec	dec_ent	double_nibble_uri	double_uri	enc_uri
enc_uri_comp	first_nibble_uri	hex	hex_ent	htmlent	malformed_uri	oct	overlong_utf8	
punycode	realurlenc	reverse_hex	rot13	rot47	second_nibble_uri	uni	uni_hwfw	
uni_hwfw_chars	urlenc	us_ascii	utf16	utf7	utf8	uuencode	xor	xor_range_encode

Binary-Ascii Çevrimi

Binary	ASCII	Binary	ASCII	Binary	ASCII	Binary	ASCII
000000	A	010000	Q	100000	g	110000	w
000001	B	010001	R	100001	h	110001	x
000010	C	010010	S	100010	i	110010	y
000011	D	010011	T	100011	j	110011	z
000100	E	010100	U	100100	k	110100	0
000101	F	010101	V	100101	l	110101	1
000110	G	010110	W	100110	m	110110	2
000111	H	010111	X	100111	n	110111	3
001000	I	011000	Y	101000	o	111000	4
001001	J	011001	Z	101001	p	111001	5
001010	K	011010	a	101010	q	111010	6
001011	L	011011	b	101011	r	111011	7
001100	M	011100	c	101100	s	111100	8
001101	N	011101	d	101101	t	111101	9
001110	O	011110	e	101110	u	111110	+
001111	P	011111	f	101111	v	111111	/

Base64

- “Base64 binary(ikili) verilerin ASCII karakterlerin kullanıldığı ortamlarda iletilmesine ve saklanmasına olanak tanıyan bir kodlama şemasıdır.

Base64 Binary Encoding

Translator

Use this tool to create data streams for embedding images (or any type of file) in (X)HTML, CSS and XML.

Encode file from URL

URI:

Results of loading <http://www.guvenlikegitimleri.com/images/websecp.gif>

```
data:image/gif;base64,R0lGODlh1AE8AIdOABAUFYhJCIEGjQhNirKNHYjK7FyMlNTDnIZgQ8bFyLlpHkVzK
M
/i5xVzuefj2aiFYoZmI+Tk5V9FHxxmmMupiOzx6h+R39V7JuKdUSH2ukdGUVSYzo5YJoetxLtwLKR1Ixp60vr36
uGIMi2fjw5doej2zCpoliaa7adpMvq1RRB6w6BYF4uem+auXglFdGJhSsTEvPTz9PWUNRVogMq4qrhzR798N8fW
4ObIqBp1scSKUg1YlTOg7aXG1PPu6j48SBtOud60ivjlyr5zIx9vropTGExmcRZNeKJ8FaqknGVZKimp+9Wkdq5
1G/7//u3u8dHR0+nWuKjQ5a10OcKWcaBcJt6MPoN
/d8bp9VO266uvtxhiogdFffbg2Gdlb+vs69uxeaSQtR+MglOiqiorHl4fWh7h+v3+atdGk1AL
/OkUM10LCaf+RdusKNzRRN0xBBhrOPe3x17wsp7MGmQocSxmvSZQq9nJZWVmsVtIjiT1FVTV5ZWF+SYRgpKfxKI
1Sc1MiFMdVSHq3VQLGqUsnSz27OJOHpZJLeCYHwozEWRwS0wJYi21C9zpKOLd3bI8XeqwqKBaZJkNazd8HNuYXZ
jOVVMMpnX8PDGinVKDtOAQ82FOY9zVGeKo1V2kTU0QKy/2eqzeeC7mzB+uWOk0LnExNf2/S1ce52hp
/mwVJvE2trEqZ2F2H+f0tjai4ol6M6J6V11YYlmTtXyVnnuiV9MGFBIP4tcOJiywrfS4X1+hpi80r+9wHh1LZCO
kdqeYcWSYsaheUmHun7K47ORbtTMyNra3OzGm3dMHleCnjqFvdK0jeY7i6yyovTauDthjWBXPjZ8qx0bKWR1YlX
J1suHKZ2foB1bjWFibGK35rWzr
/OoY9K4nFWr3LOyt9jr89fHufuxSTWs8eOpbnJxeLWZhGmcwN3j5fLayvPQp8lzI7zi7
/LAeDhqkdfV1Kt7R5JmSseV4eF+I+mUMrZ+SEk8OpdjJceIRZRMdbGIXf703B2G1CiJyvWyY5XN7gAAACH
/C05FVFNDQVBFMi4wAwEAAAAh+QQFDwD/ACwAAAAIAE8AAAI
/wCdBxIsKDBgwgTK1zIcKC+dJjYYXLWJURDgV4oXdzIsaPHjyBDihxJsqtJkyhTqlzJsqa+KmlmyQinRo0QJZe
aTiPXsqfPk08SePOWICjRnD+TGjR6lG1RgzGEDj2qVGTUqVSrat2KEMcUdfLEWBEhD4y+i154cl17FevUBEhxSn
Wb9WICAV68CPCGV0ACq3PpPl3r5G7evXwP/yloOK9euFvbDoWcsLHiuIQz
/yxhT4GCO1NsrAmmyLDnZq1WnaseOBq1n45evMiTzpj295EvnaMLTbh2dIAsa7tJXfB2T+I7nm8dbVvhMh58Vr
+PLV1lfqIcVixAk2VKsVMK/+MEeFKmC+Yr6+c
```

Hex Encoding

The screenshot displays the Hackvortor web application interface. On the left, the 'hackvortor' logo is visible above a 'Log window' and an 'Input' field containing the text '<@hex_3>Guvenlikegitimleri</hex_3>'. Below the input field are buttons for 'Clear', 'Clear tags', 'Swap', 'Select input', 'Select output', and 'Convert'. A 'Help - Hackvortor videos' section lists links for 'General demo', 'Encoding demo', 'Decoding demo', 'IP conversion', and 'More soon...'. A 'Spread the word' section includes links for 'Hackvortor graphic' and 'Hackvortor background'.

On the right, a toolbar at the top includes options like 'Show DOM browser', 'HVURL', 'Log', 'Clear Log', 'Inspect', 'Execute', 'Alert', 'Inspect HTML', 'HTML Test', 'Execute/HTML Test', 'Compare', 'Turn Realtime ON', and 'Hackvortlet'. Below this is a dropdown menu set to 'Encode', followed by a grid of encoding options: 'base36', 'base62', 'base64', 'base999', 'dec', 'dec_ent', 'double_nibble_uri', 'double_uri', 'enc_uri', 'enc_uri_comp', 'first_nibble_uri', 'hex' (highlighted with a red box and a red arrow), 'hex_ent', 'htmlent', 'malformed_uri', 'oct', 'overlong_utf8', 'punycode', 'realurlenc', 'reverse_hex', 'rot13', 'rot47', 'second_nibble_uri', 'uni', 'uni_hfwf', 'uni_hfwf_chars', 'urlenc', 'us_ascii', 'utf16', 'utf7', 'utf8', 'uencode', 'xor', and 'xor_range_encode'. Below the grid is an 'Output' field showing the hex-encoded result: '\x47\x75\x76\x65\x6e\x6c\x69\x6b\x65\x67\x69\x74\x69\x6d\x6c\x65\x72\x69'. At the bottom right, there is a 'JavaScript/HTML shortcuts' section with various dropdown menus and a 'Send output to url:' field with the value 'http://demo.phpids.org?test=' and buttons for 'Send', 'Send to iframe', and 'Send to PCE'.

Hackvortor Hizmeti

The screenshot shows the Hackvortor web application running in a Mozilla Firefox browser. The browser's address bar displays the URL <http://www.businessinfo.co.uk/labs/hackvortor/hackvortor.php>. The application interface includes a logo, a "Log window" section, an "Input" field, and a "Convert" button. A dropdown menu is open, showing a list of encoding and decoding options such as "Encode", "Decode", "Compression", "IP", "Code Morphing", "Filter Evasion", "Math", "String", "Script", "Fuzzing", "Hashing", "Common Inputs", "XSS", "SQL", "Date", "Encrypt", "Char Tables", and "Hacker tags". Below the dropdown, there are "Javascript/HTML shortcuts" and a "Send output to url:" field with a "Send" button. The Businessinfo logo is visible in the bottom right corner.

I-Packer

I-Packer (A Packer/Unpacker Javascript Tool using [packer](#))

bedirhan urgun, 06/30/2008 (Yenileme: 07/01/2008)

Input:

```
eval(function(p,a,c,k,e,r){e=function(c){return c.toString(a)};if(''.replace(/^\./,String))
{while(c-->r[e[c]]|e[c]|c|k){function(e){return r[e]};e=function(){return'\w+'};
c==1;while(c-->1)if(k[c])p=p.replace(new RegExp('\\"b'+e(c)+'\\"b', 'g'),k[c]);return
p}(')(k(\"\"b1d1t1m9n1k1f1o1p1q1r1f1g1s1a1g121o101g1d1211o101013171211o101013131211010101415121101010131h1
```

PACK

UNPACK

EVAL TO OUTPUT

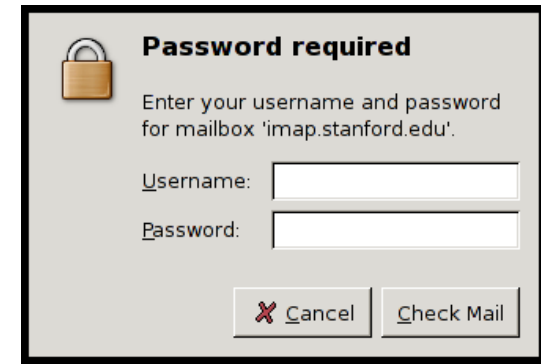
PASS OUTPUT TO INPUT

Output:

[illegible]

Bölüm-K:Kimlik Doğrulama ve Çeşitleri

- Kimlik doğrulama nedir?
- Günümüzde nerelerde kullanılır?
- Kimlik doğrulama çeşitleri:
 - Basic Authentication.
 - Digest Authentication.
 - Windows Integrated Authentication.
 - Negotiate Authentication (**Kerberos**).
 - Sertifika Kullanımı.
 - Form Based Authentication.
 - Bio Authentication



Password required

Enter your username and password for mailbox 'imap.stanford.edu'.

Username:

Password:

Kimlik Doğrulama

- Bir sisteme girişte kimlik tespiti
 - Bir sonraki adım authorization
- Sistemlere yapılacak yetkisiz girişleri engelleme amaçlıdır
- Ortama göre çeşitleri vardır
 - Pin, otp, sms, iris, parmak izi

Basic Authentication

- En düşük seviye güvenlik doğrulamasıdır.
- Kullanıcı adı ve parola bilgisi sadece base64 ile şifrelenir.
- Kullanım sebebi: Bir çok platform tarafından destekleniyor olması.
- Kullanıcı ağını dinleyen saldırgan rahatlıkla kullanıcı adı ve parola bilgilerini elde edebilir.
- **SSL/TLS kullanımı ile güvenli hale getirilebilir.**

Basic Authentication ekran görüntüsü



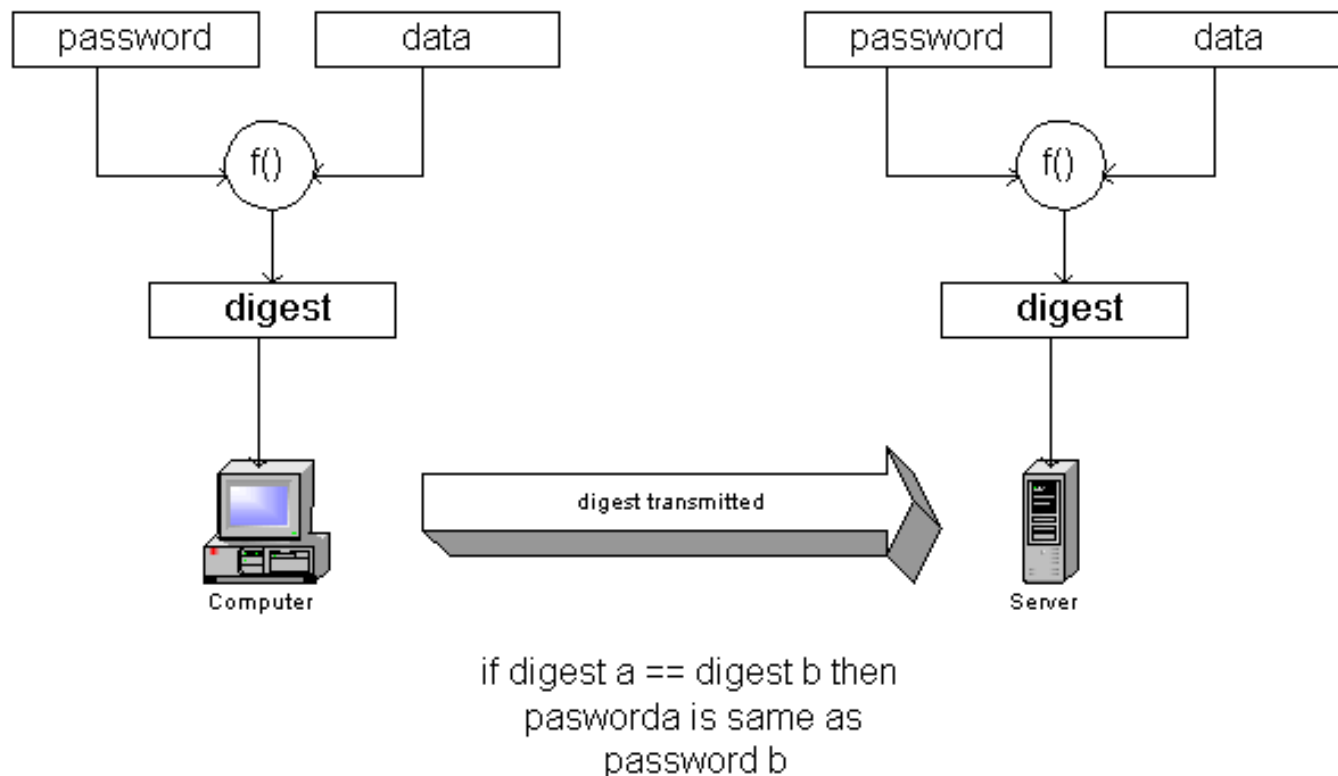
```
HTTP/1.1 401 Authorization Required
Date: Sat, 27 Mar 2010 06:12:52 GMT
Server: Apache/2.2.9 (FreeBSD)
WWW-Authenticate: Basic realm="Sadece Adminlere aciktir "
Content-Length: 401
Keep-Alive: timeout=5, max=50
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Authorization Required</title>
</head><body>
<h1>Authorization Required</h1>
<p>This server could not verify that you
are authorized to access the document
requested. Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.</p>
</body></html>
GET /wp-admin HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
powerpoint, application/msword, application/x-ms-application,
Accept-Language: tr
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1
Host: blog.lifeoverip.net
Connection: Keep-Alive
Authorization: Basic aHV6ZXl[REDACTED]aGVkQQ==
```

GET /private/index.html HTTP/1.0 Host: localhost Authorization: Basic QWxhZGRpbjpvGVulHNlc2FtZQ==

Digest Authentication

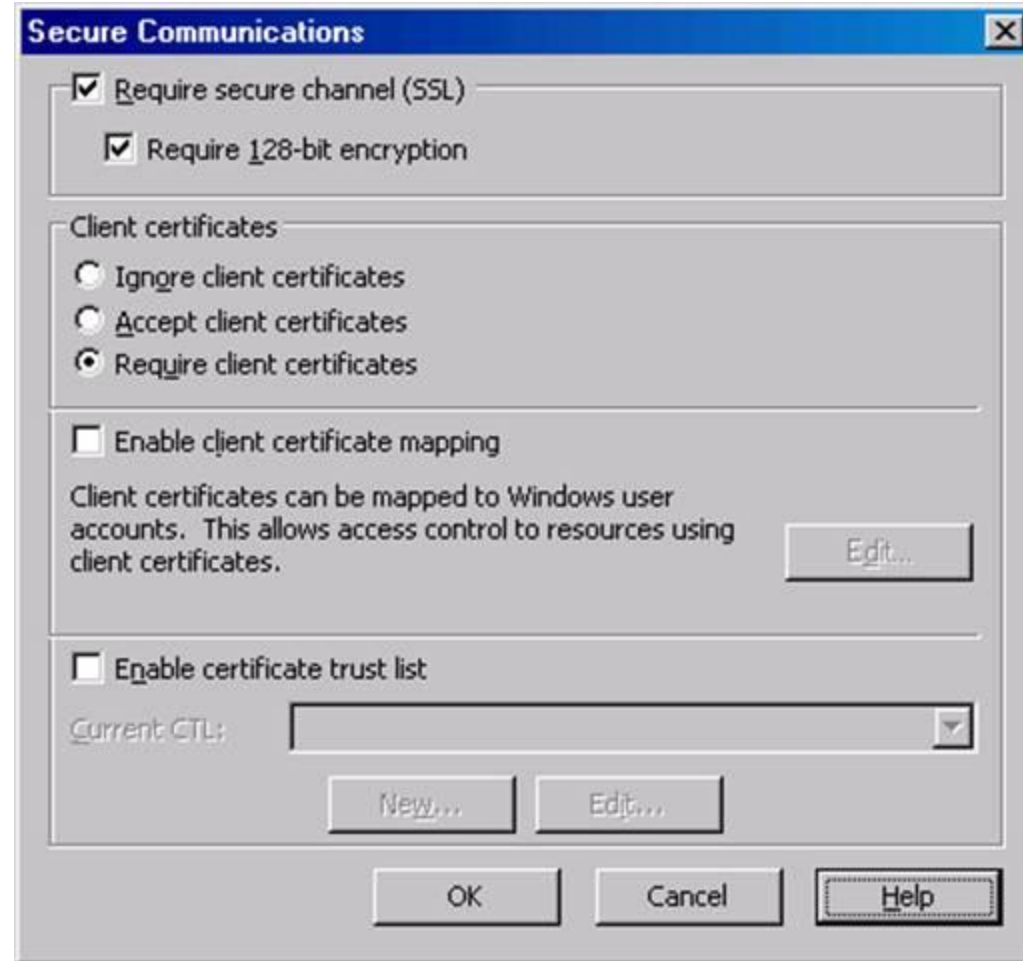
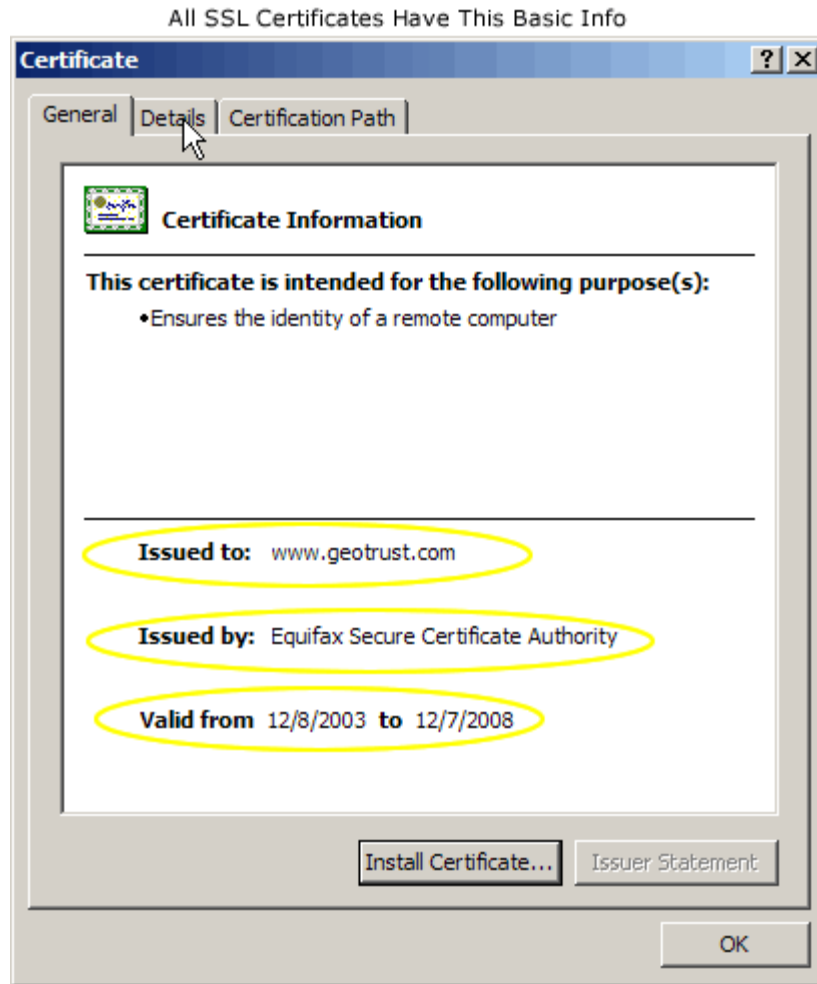
- Kullanıcı adı ve şifre ağ üzerinden taşınmaz. Sadece bu ikilinin hash değeri taşınır .



Digest Authentication-II

- Basic Authentication 'dan daha güvenlidir.
- Active Directory ile beraber çalışır.
- IE 5.0 ve üzerin platformlarda çalışır.
- LDAP ,IMAP, POP3 ve SMTP protokolleri ile sıkça kullanılır.
- Tek yönlü(Simetrik) şifreleme kullanır, şifrelenmiş bilgiler Active Directory veritabanında tutulur(NTDS.DIT)

Sertifika Kullanımı



Form Based Authentication



WORDPRESS.COM

ERROR: Cookies are blocked or not supported by your browser. You must [enable cookies](#) to use WordPress.

Username

Password

☐ Remember Me

Log In

[Get a free WordPress account](#) | [Lost your password?](#)

```
<link href="https://wordpress.com/wp-admin/css/wpcom.css?m=1266260714g&on=MU" type="text/css" />
</head>
<body class="login">

<div id="login"><h1><a href="http://wordpress.com/" title="Powered by WordPress">WordPress.com Blog</a></h1>
<div id="login_error"> <strong>ERROR</strong>: cookies are blocked c
supported by your browser. You must <a
href='http://www.google.com/cookies.html'>enable cookies</a> to use
WordPress.<br />
</div>

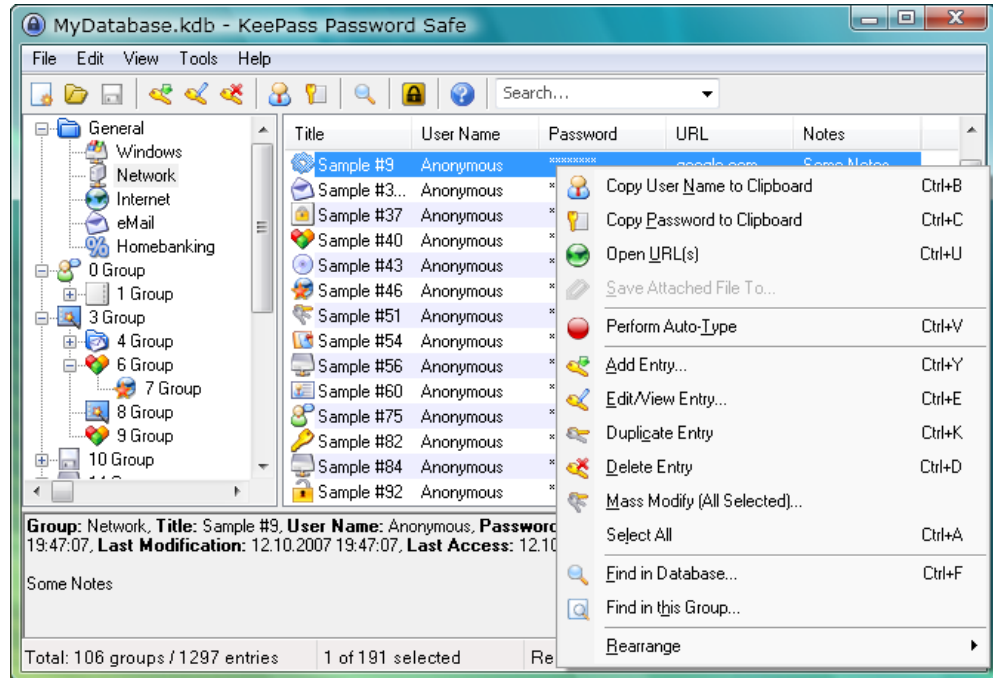
<form name="loginform" id="loginform"
action="https://wordpress.com/wp-login.php" method="post">
  <p>
    <label>Username<br />
    <input type="text" name="log" id="user_login"
class="input" value="" size="20" tabindex="10" /></label>
  </p>
  <p>
    <label>Password<br />
    <input type="password" name="pwd" id="user_pass"
class="input" value="" size="20" tabindex="20" /></label>
  </p>
  <p class="forgetmenot"><label><input name="rememberme"
type="checkbox" id="rememberme" value="forever" tabindex="90" /> Reme
Me</label></p>
  <p class="submit">
    <input type="submit" name="wp-submit" id="wp-submit"
class="button-primary" value="Log In" tabindex="100" />
    <input type="hidden" name="redirect_to"
  </p>
</form>
```


- Ağ üzerinden celartext gider
- SSL ile kullanılmalıdır



Güvenli Parola Saklama Yöntemleri.

- Parola nasıl ve nerede saklanmalı.
- Parola saklama araçları ve kullanımları.
 - PGP
 - True Crypt
 - Keepass



Distributed Password Recovery teknolojisi

- Çalışma mantığı nedir.
 - 5 karakterliler 1. makine, 6. karakterliler 2. makine...
- Paralel şifre kırma teknolojileri
 - Cuda Kullanımı
 - Pyrit
 - Botnet kullanımı
- Elcomsoft aracının kullanımı

Bölüm-S: Stegenography(Stegonafi)

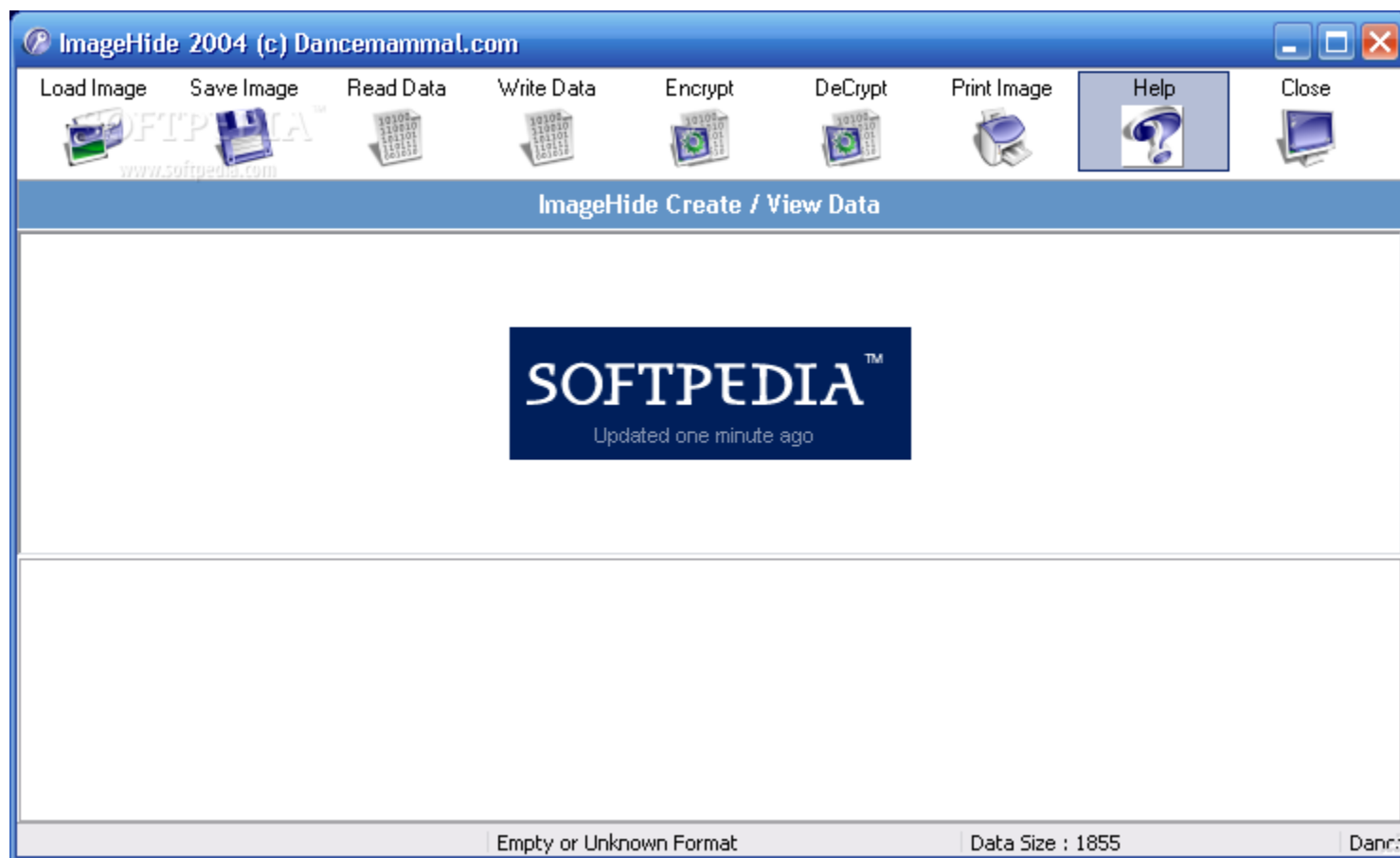
- **Steganografi**, eski [Yunanca](#)'da "*gizlenmiş yazı*" anlamına gelir ve bilgiyi gizleme ([şifreleme](#) değil) bilimine verilen addır. wikipedia



Resim dosyalarına veri saklama

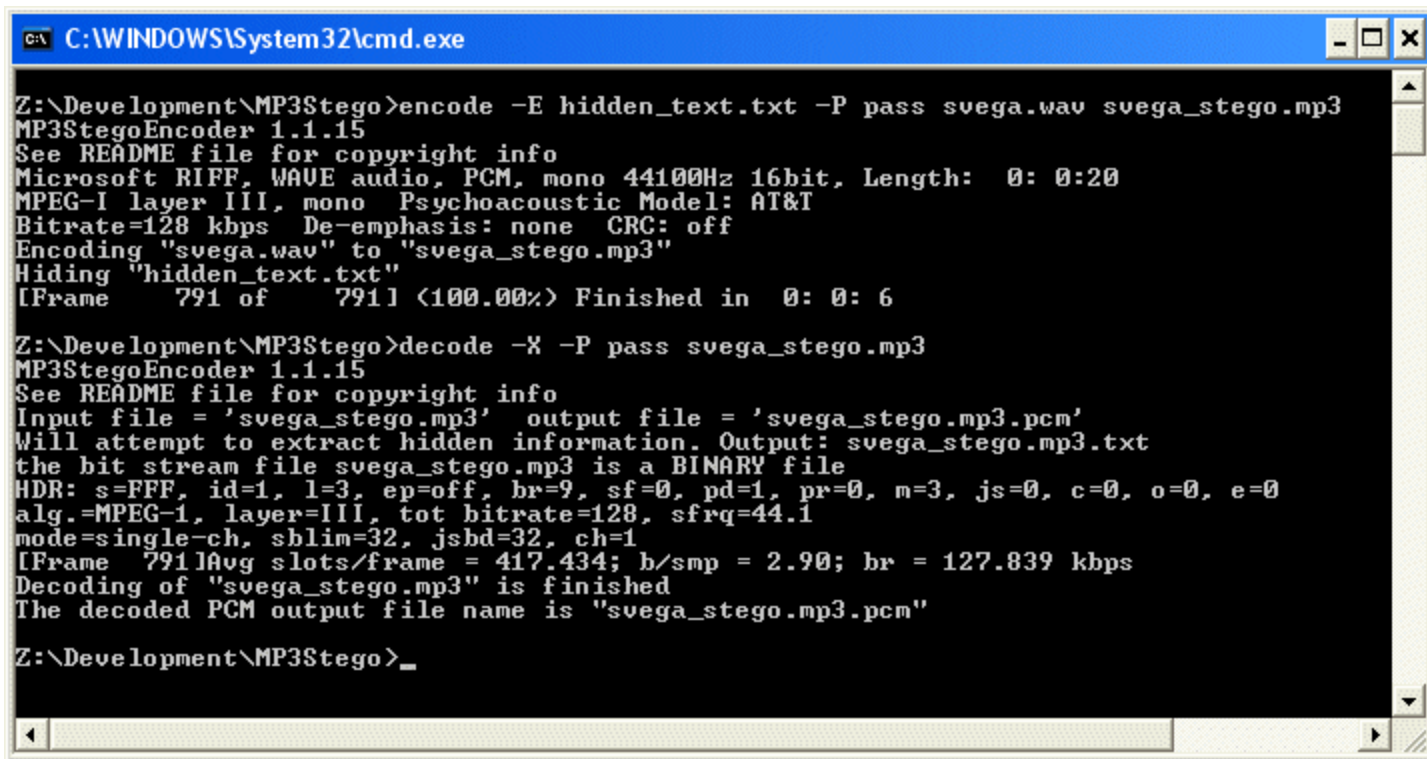
- Resim dosyasında çıplak gözle anlaşılabilecek bir değişiklik olmaz
- Boyut ve hash değişikliği
- Özel yazılımlar kullanılarak saklanan veri şifrelenebilir
- Veriyi geri getirmek için anahtar kullanılır
 - Anahtara yönelik bruteforce saldırıları düzenlenebilir

ImageHide



Ses dosyalarıyla stegonagrafi

- Ses dosyaları içerisine veri gizleme
- **mp3stego**



```
C:\WINDOWS\System32\cmd.exe

Z:\Development\MP3Stego>encode -E hidden_text.txt -P pass svega.wav svega_stego.mp3
MP3StegoEncoder 1.1.15
See README file for copyright info
Microsoft RIFF, WAVE audio, PCM, mono 44100Hz 16bit, Length: 0: 0:20
MPEG-I layer III, mono Psychoacoustic Model: AT&T
Bitrate=128 kbps De-emphasis: none CRC: off
Encoding "svega.wav" to "svega_stego.mp3"
Hiding "hidden_text.txt"
[Frame 791 of 791] (100.00%) Finished in 0: 0: 6

Z:\Development\MP3Stego>decode -X -P pass svega_stego.mp3
MP3StegoEncoder 1.1.15
See README file for copyright info
Input file = 'svega_stego.mp3' output file = 'svega_stego.mp3.pcm'
Will attempt to extract hidden information. Output: svega_stego.mp3.txt
the bit stream file svega_stego.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=3, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=single-ch, sblim=32, jsbd=32, ch=1
[Frame 791]Avg slots/frame = 417.434; b/smp = 2.90; br = 127.839 kbps
Decoding of "svega_stego.mp3" is finished
The decoded PCM output file name is "svega_stego.mp3.pcm"

Z:\Development\MP3Stego>_
```

Online Steganography

Steganogravate online !


Picture (jpg when encoding, png when decoding)

File to be hidden (Do not use when decoding)

Test encoding ?	Test decoding ?
<ul style="list-style-type: none">o Open your text editor and create a file.o Save this file.o Click above at "picture" on "browse"o Take a picture at random on your hard disk and select ito Click above at "file to be hidden" at "browse"o Select your text file on your hard disko Click on "Start"o You now get your picture back in .png format with your text file hidden in it.	 <ul style="list-style-type: none">o Click on this picture with your right mice keyo Select "save image as"o Save the picture on your hard disko Click above at "picture" on "browse"o Select the picture (vis.png) on your hard disko Click on "Start"o You can try it also with the background of this site.

VeriGizle.Com

GOOGİE Reklamları

**Veri Gizle**


Önce taşıyıcı olarak kullanacağınız yani içine veri gizleyeceğiniz resmi seçin, daha sonra anahtar kelimeyi giriniz şifreleme işlemi bu anahtara göre yapılacak, son olarak gizlemek istediğiniz yazıyı yazın ve veri gizleme işlemini başlatın.

Hedef Resim Bilgisayarında:

(sadece .bmp resim seçin!)

Anahtar :

Gizlenecek Yazı:

**Veri Çöz**

Önce içinde gizlenmiş veri olan taşıyıcı resim dosyasını seçin, daha sonra anahtar kelimeyi girip veri çözme işlemini başlatın.

Kaynak Resim Bilgisayarında:

(sadece .bmp resim seçin!)

Anahtar :


TinEye:Reverse Image Search

- Verilen bir imajın başka hangi sitelerde geçtiğini bulmaya yarar

Home FAQ API Plugin What's New Forums **NEW!** More ▾

idée **TinEye**^{beta}
REVERSE IMAGE SEARCH


Upload image or

 **Your image**
JPEG image, 200x168, 7.4 KB

1 result [Facebook](#) [Twitter](#) [Share](#) [More](#)

searched over [1.3059 billion](#) images in 1.339 seconds

Sort order: [best match](#)

 **blog.lifeoverip.net**
[huzeyfe.jpg](#) → <http://blog.lifeoverip.net/2010/01/17/bir-hafta...>
[huzeyfe.jpg](#) → <http://blog.lifeoverip.net/2010/01/27/turkiyede...>

Same file
JPEG image
200x168, 7.4 KB

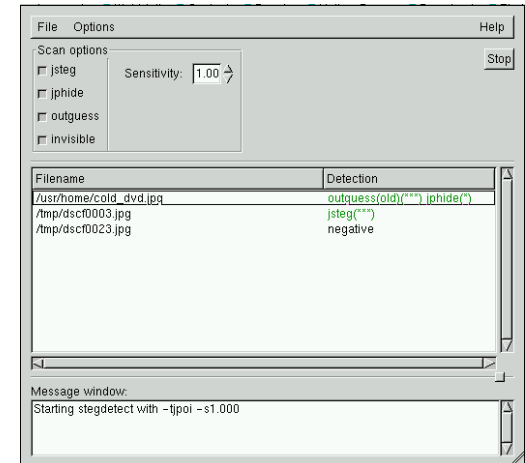
Steganografi Algılama

- Herhangi bir imajın içerisinde başka dosya saklımı bulmaya yarar.
- **stegdetect**
- `$ stegbreak -tj dscf0002.jpg`

Loaded 1 files... dscf0002.jpg : jsteg(wonderland)

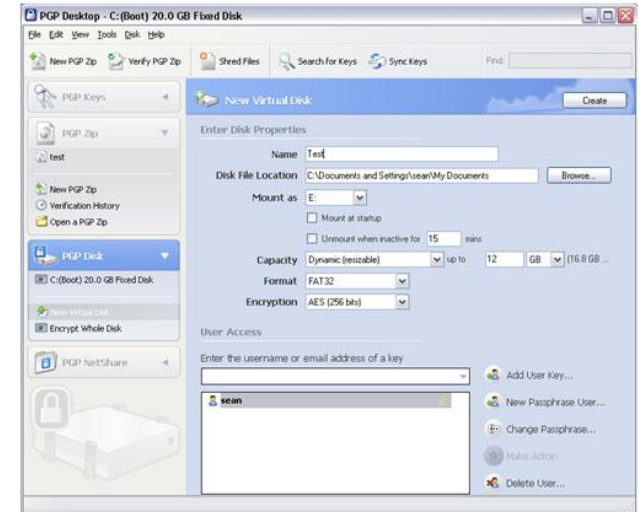
Processed 1 files, found 1 embeddings.

Time: 36 seconds: Cracks: 324123, 8915 c/s



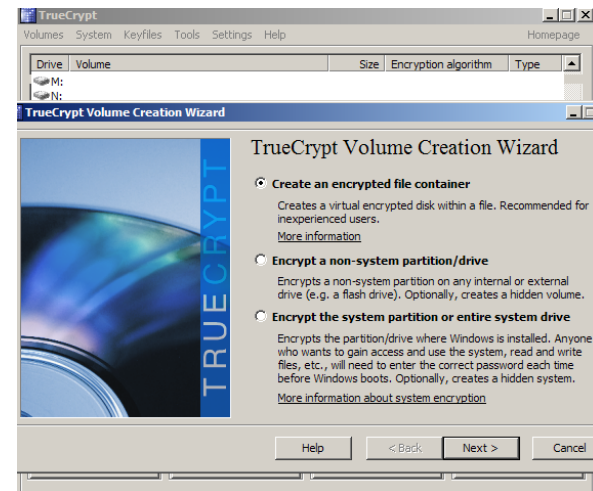
Bölüm-D:Dosya/Disk Şifreleme

- Truecrypt, masaüstünde kullandığım program
- Disk şifreleme çeşitleri
 - Tam(Full) disk şifreleme
 - Dosya şifreleme
 - Partition şifreleme
- Gizli alan oluşturarak şifreleme
 - Disk üzerinde şifreleme olduğunu saklama
 - Gizli servislerin kullandığı yöntem

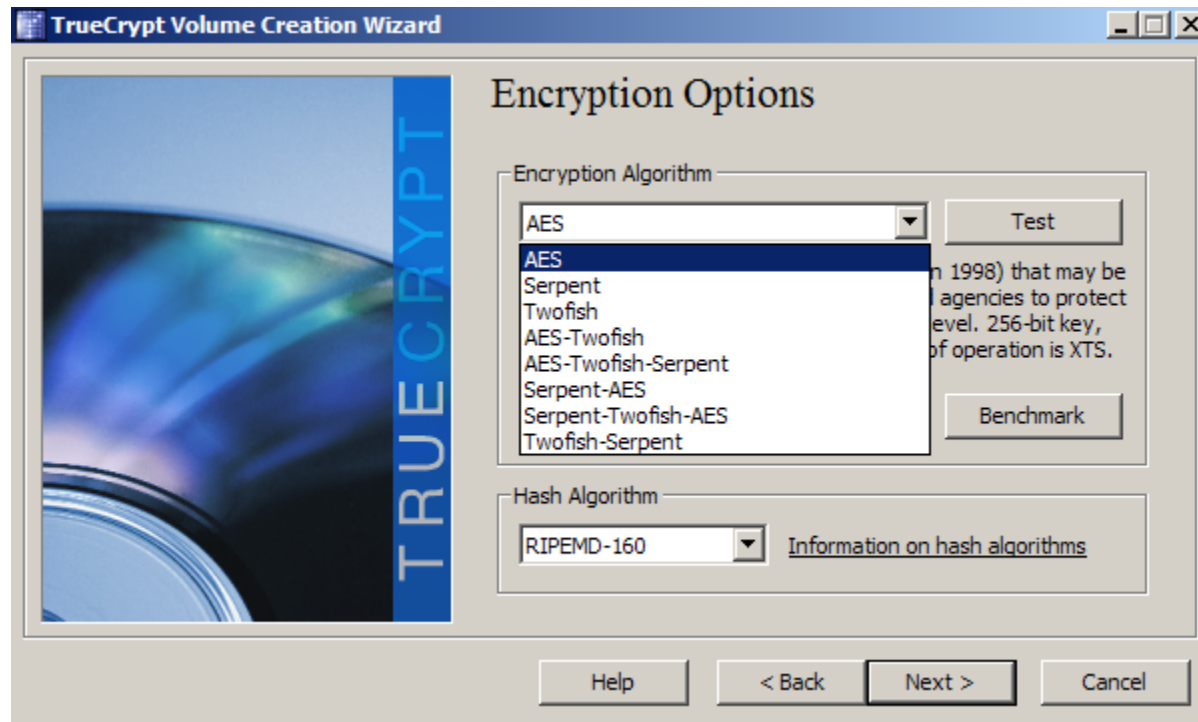


TrueCrypt

- Ücretsiz Disk şifreleme programı
- Linux, Windows üzerinde çalışma özelliği
- Sertifika, parola kullanımı

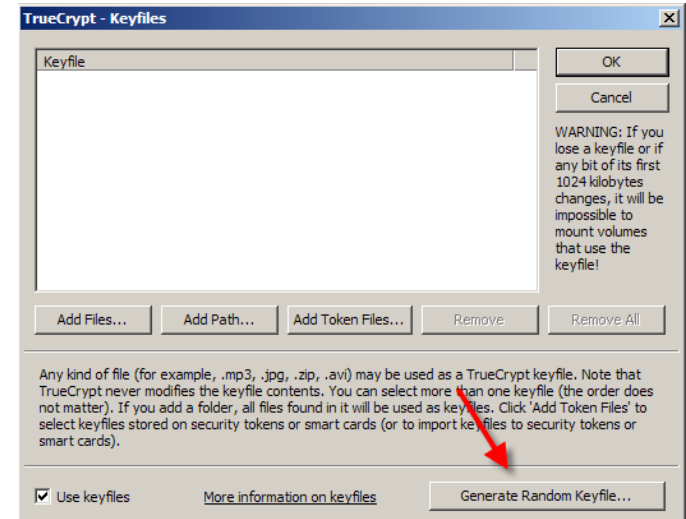
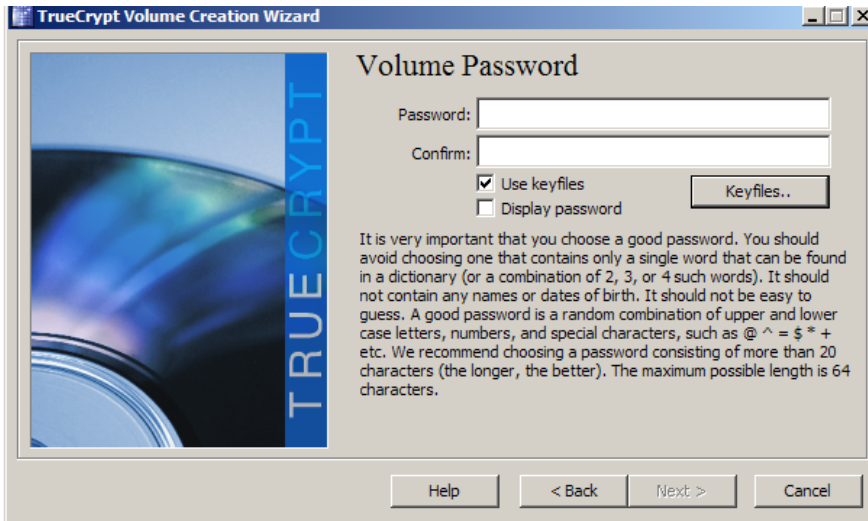


TrueCrypt Şifreleme Desteği



TruCrypt Anahtar Desteđi

- Disk şifreleme için kullanılacak anahtar:
 - Parola olabilir(12€dfdf_*0\$ gibi)
 - Anahtar dosyası olabilir



BruteForce Saldırıları

- Disk şifreleme yazılımlarının temel zaafiyeti parola kullanılmasıdır
 - Sertifika kullanıldığı durumlarda çok daha zorlaşır
- Kullanılan anahtarı bulmak için şifreleme algoritmasına özel programlar yazılarak anahtar elde edilmeye çalışılır

Bölüm-O:OneTimePassword

- Tek kullanımlık şifre
 - Şifreleme özelliği değildir, şifrenin tek seferlik kullanılmasını sağlar
 - Şifrelemeyi başka katmanlar(SSL/TLS) sağlamalıdır
- Donanımsal ya da yazılımsal olabilir
- Türkiye online bankacılık sistemi SMS üzerinden OTP'e geçiş yaptı

OTP Çeşitleri

jsotp: JavaScript OTP

This calculator generates passwords for the OTP or S

Challenge: (e.g., 98 seed123)

Secret: (i.e., your passphrase)

Display results in: ☐ Six-word format ☐ Hex format ☒ Both

Compute password(s) (If more than 1, results will be displayed in a new window.)

Compute with:

Response (i.e., your one-time password)

TUSK KURT DISH ORR TOY KEN (F195 15D0 1804 2043)



Menu **citi** Logoff

One-Time PIN Authentication

To proceed with your transaction, please enter the One-Time PIN displayed on your Online Security Device.

 Request for a One-Time PIN via SMS

OR

Please enter your One-Time PIN.



> Need Help?

Citibank Singapore Ltd
Co. Reg. No. 200300485K



Citi Mobile
mobile.citibank.com.sg... Google


Menu **citi** Logoff

One-Time PIN Authentication

One-Time PIN has been sent to your registered phone.

Your One-Time PIN is 766292. It will expire in 5 minutes.

Please enter your One-Time PIN below, then click "Continue" to proceed.

 One-Time PIN

> Need Help?

> Missed the last SMS?
Request for a One-Time PIN via SMS