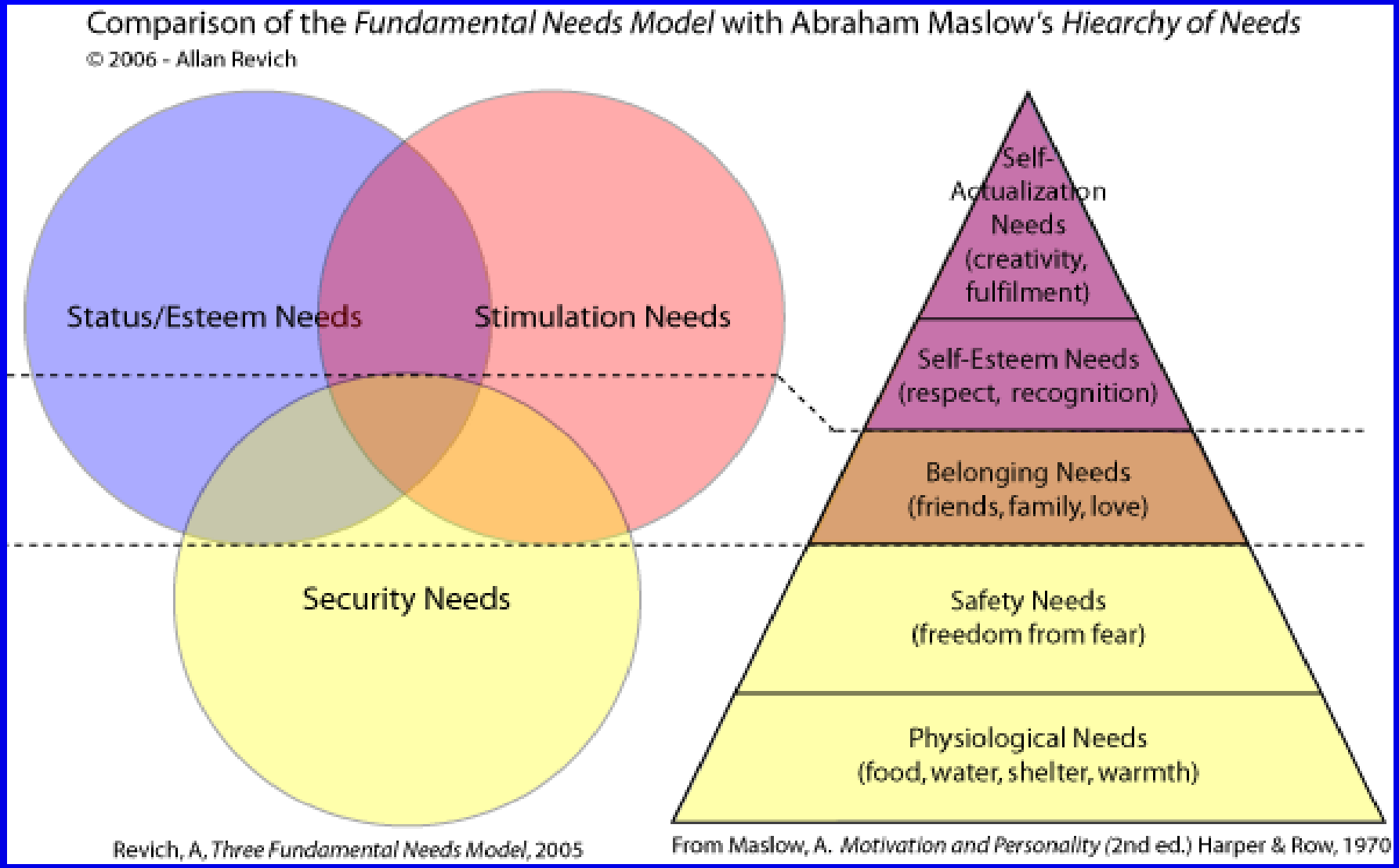
# Internet'te Veri Güvenliği

**Umut Al**
**H.Ü. Bilgi ve Belge Yönetimi Bölümü**
**umutal@hacettepe.edu.tr**

# Temel Kavramlar

- Güvenlik

# Gereksinim Modelleri



# Temel Kavramlar

- Kriptografi
  - Kript (gizli) graf (yazı) = kriptografi
- Kriptoloji (şifrebilim)
- Kriptanaliz
  - Amaç: Mevcut şifreleri çözmek
- Hacking

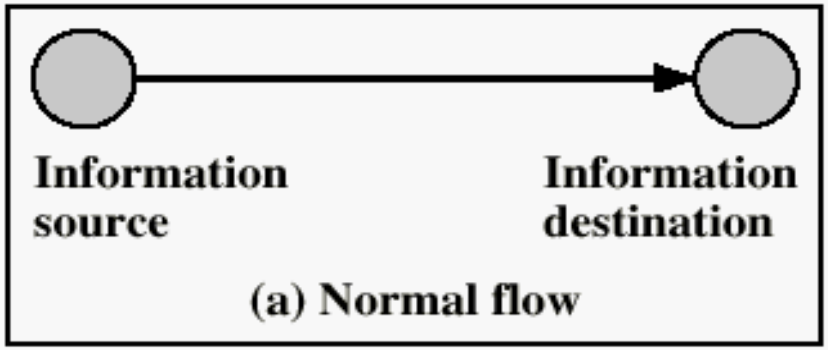
# Kişiler

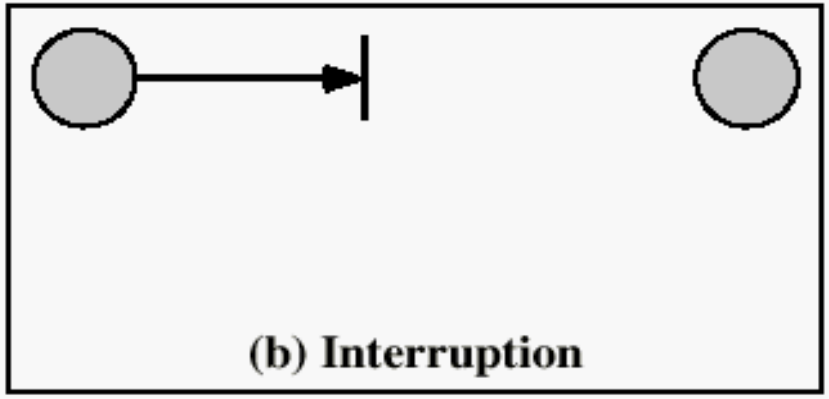
- Hacker
- Cracker
- Phreaker
- Lamer
- Script Kiddy
- Newbie

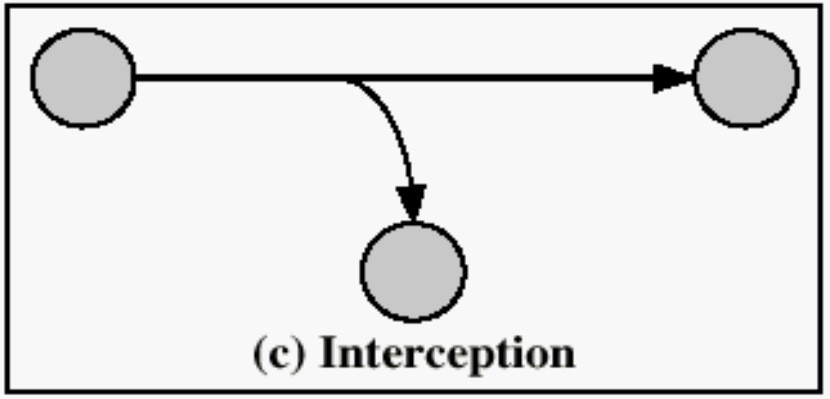
# Bir Bilgisayar Sistemini Tehdit Eden Öğeler

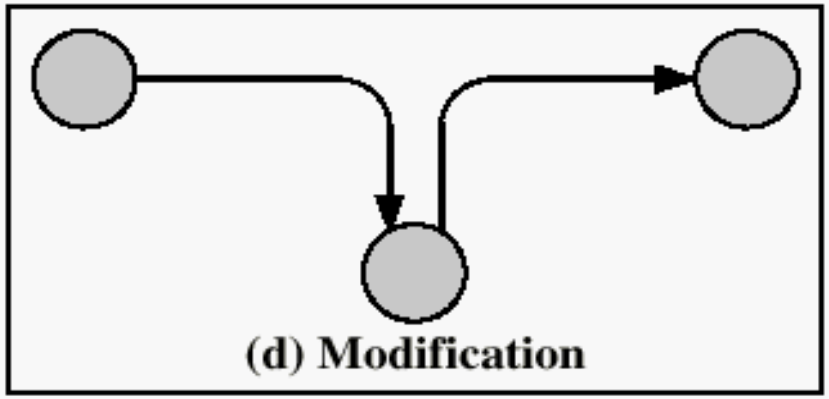
- Düzenini bozma (interruption)
- Durdurma (interception)
- Değiştirme (modification)
- Fabrikasyon (fabrication)

(Pfleeger 1997)



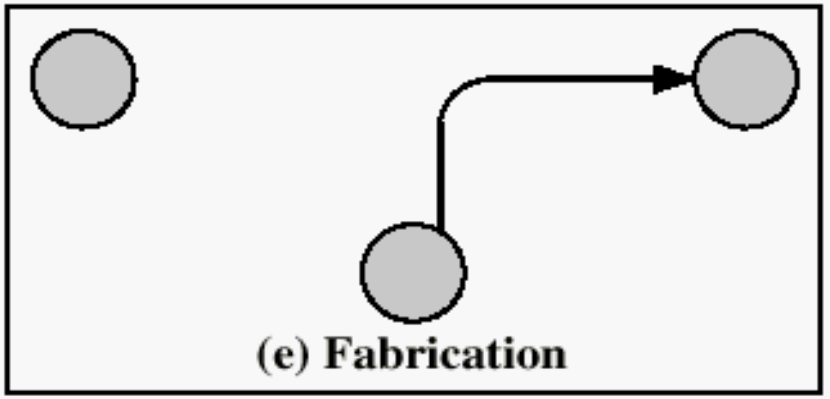




**Figure 1.1 Security Threats**

# Sitelerdeki Güvenliği Sarsan Faktörler I

- Ağ güvenliğine yeterli kaynak ayrılmaması
- Gerekli güvenlik önlemlerini almaya yetkisi olmayan veya üst yönetim desteği olmayan destek personeli
- Güvenlik açıkları için yama kullanılmaması

# Sitelerdeki Güvenliği Sarsan Faktörler II

- Halen gizleme ile güvenlik düşüncesine inanarak hareket edilmesi
- Ağlara kurulan yeni cihazlarda prosedür ve standartlara uyulmaması
- Kötü amaçlı ek dosyalar bulundurabilecek mesajların filtrelenmemesi
- Anti-virüs yazılımlarının düzenli olarak güncellenmemesi

# İletişim Güvenliği İçin Gerekenler

- Kimlik
- Bütünlük
- Gizlilik

# Güvenlik Gereksinimleri

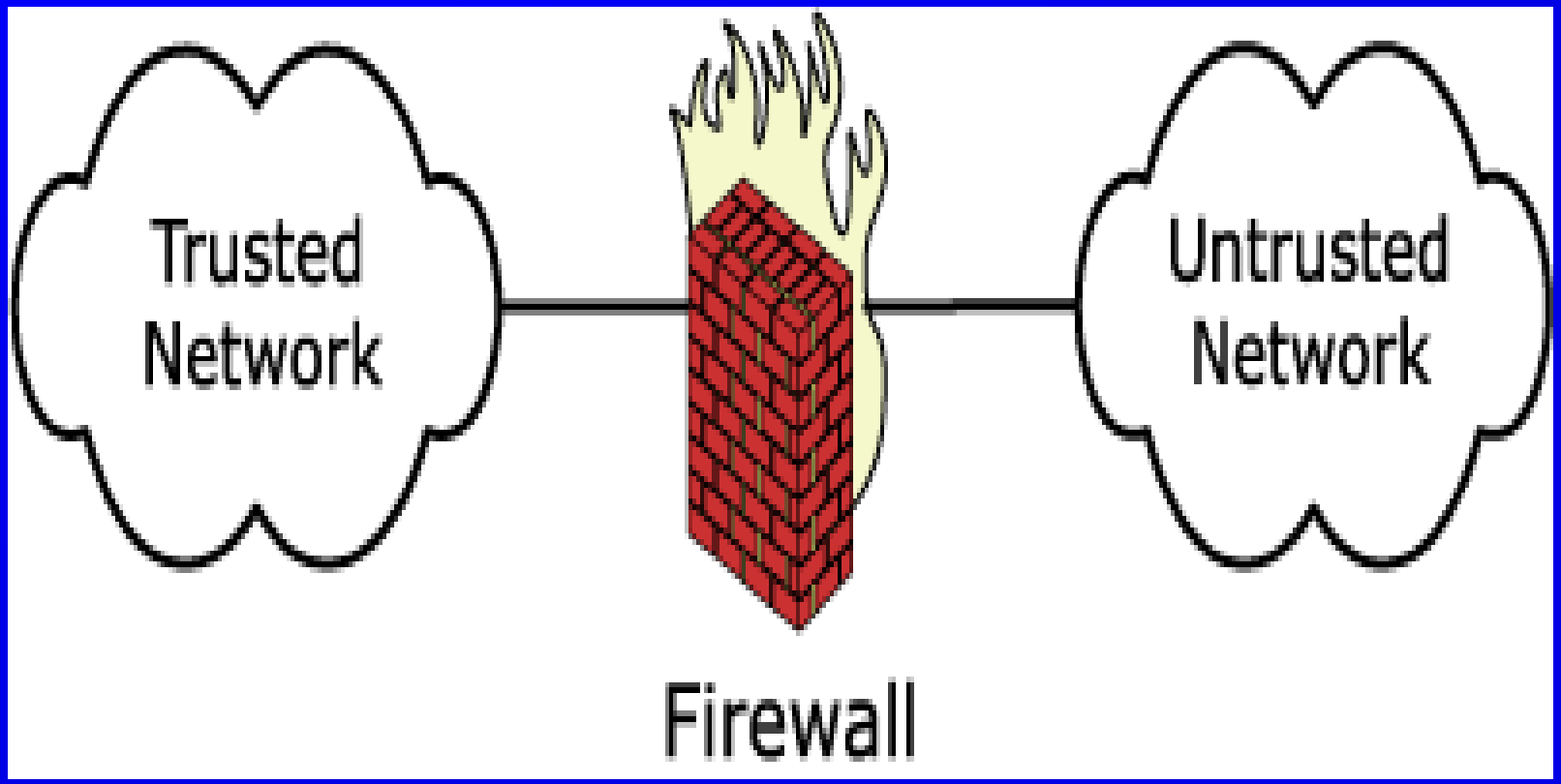
- **İstek**

1. Müşteri ve merkezleri Internet üzerinde birleştirme
2. E-posta sadece gönderdiğim kişi tarafından okunsun
3. İstemediğiniz sayfalara girilmesin
4. İstenmeyen ağa giriş
5. Ağdaki olası tehlikeleri saptamak
6. Saldıranları görmek
7. Virüs bulaşmasın
8. Ağdaki olan biteni izlemek

- **Çözüm**

1. VPN (Virtual Private Network) – Sanal Özel Ağ
2. PGP (Pretty Good Privacy) – Mükemmel Şifreleme
3. Content filter – İçerik Kontrolü
4. Firewall
5. Otomatik açık tarama programları
6. IDS (Intrusion Detection System) – Saldırı Tespit Sistemi
7. Antivirüs yazılımları/sistemleri
8. Raporlama yazılımları

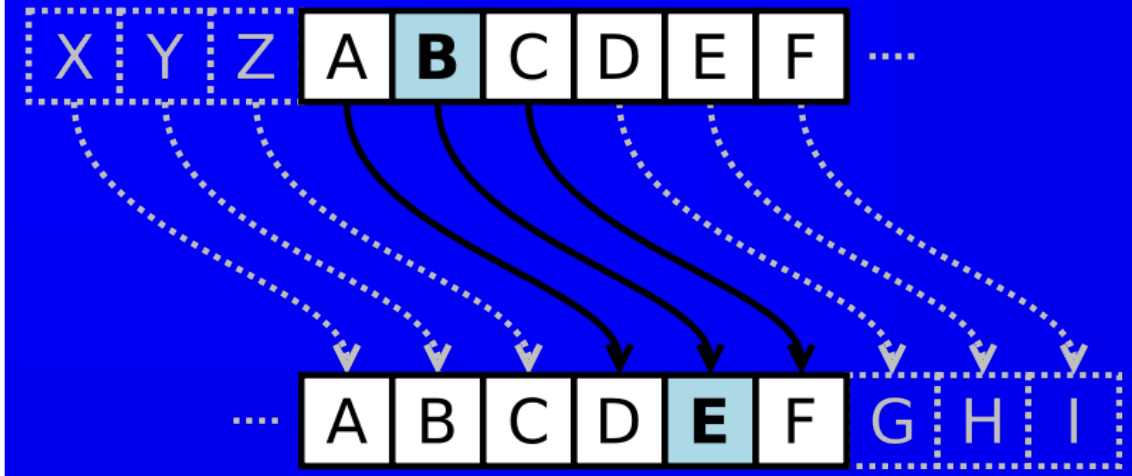
# Ateş Duvarları (Firewalls)

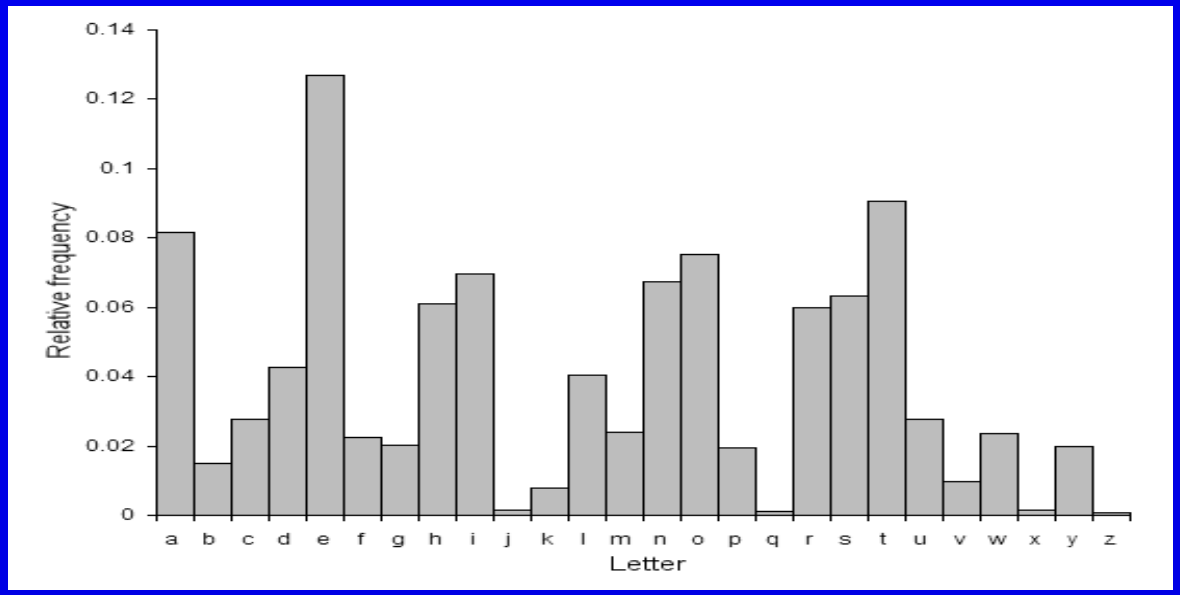


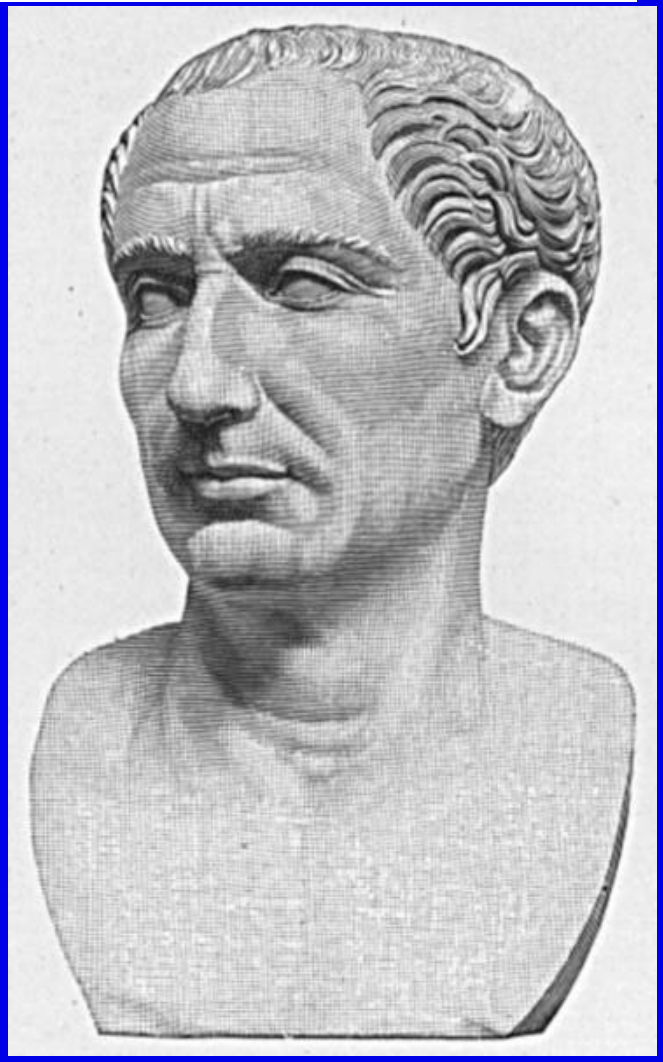
# Ateş Duvarı Türleri

- Packet filtering firewall
- Dual-homed gateway
- Screened host firewall
- Application level firewall
- Stateful firewall

# Sezar Şifresi



# Enigma

# TÜBİTAK UEKAE



*Yolunda yürüyen yolcunun yalnız ufku görmesi yeterli değildir. Muhakkak ufkun ötesini de görebilmesi gerekir.*

Hakkımızda
Faaliyet Alanlarımız
Ürünlerimiz
İletişim
Kamu Sertifikasyon Merkezi
Pardus
İhaleler
Arama
İş Olanakları

Enstitümüz; ISO9001:2000, AQAP-2110, AQAP-2130, AQAP-150, ISO17025 ve BS7799-2 belgelerine sahiptir.

## ULUSAL ELEKTRONİK ve KRİPTOLOJİ ARAŞTIRMA ENSTİTÜSÜ



Son güncelleme: 27 Kasım 2006

# En Çok Kullanılan Şifreler

- Şifresiz - sadece enter ☺
- Şifre olarak "password" kelimesi
- Kullanıcının kendi ismi (user name)
- abcd
- aaaa
- 1234
- 1111

# İçişleri Bakanlığı'nın şifresi tanıdık çıktı

Yazıya oy verin :

Giriş Tarihi: 22.04.2012, 13:59
Güncelleme Tarihi: 22.04.2012, 14:02

Etiketler:
redhack içişleri bakanlığı hack hacker kızıl hacker 123456 şifre türk hacker




Emniyetin şifresinin '123456' olduğunu ortaya çıkaran RedHack dün de İçişleri Bakanlığı'nı hack'ledi. Şifre çok tanıdık çıktı.

# Şifre Kırma Üzerine ☹

- abcd = 4,57 saniye
- Abcd = 1,22 dakika
- W7r&cE4 = 20,6 yıl
- #T$9tU%e7&Jv =

~ 55.083.369.830 yıl

# Şifreleme Yöntemleri

- DES (Data Encryption Standard)
- RSA
  - Ronald **R**ivest, Adi **S**hamir, Leonard **A**dleman
- DSA (Digital Signature Algorithm)
  - Açık anahtarlı şifreleme
  - Sadece sayısal imzalamada kullanılıyor

# Sayısal İmza

- Elle atılan imzanın sayısal ortamdaki karşılığı
- Daha güvenli
- İmzalanacak metin ve imzalayacak kişinin gizli anahtarı kullanılarak elde edilen bir dizi karakterden oluşur
- Mesajın bütünlüğünü korur, kaynağın doğruluğunu ispatlar ve reddedilemez olmasını sağlar

e-imza.gen.tr
e-Dönüşümün Anahtarı


FORSNET BİLGİ TEKNOLOJİLERİ





## Haber Listesi

Yeniliklerden haberdar olmak için haber listemize kayıt olabilirsiniz.

isim@eposta.com Ekle

## Biliyor muydunuz?

ESHS'nin, Kanundan doğan yükümlülüklerini yerine getirmemesi sonucu doğacak zararların karşılanması amacıyla yaptırmakla yükümlü olduğu sigortaya **Sertifika Mali Sorumluluk Sigortası** denir.

## Ulusal E-İmza Sempozyumu Başladı


İlk Ulusal Elektronik İmza Sempozyumu Ankara'da başladı. İki gün sürecek olan sempozyuma Telekomünikasyon Kurumu başta olmak üzere Turkcell, TÜRKTRUST, E-güven, Avea'nın aralarında bulunduğu kuruluşlar destek verdi.

Devamı için...

### Kimlik Yönetimi 2006 Forumu

Artifex Solutions'ın, "Kimlik Yönetimi ve Kimlik Hırsızlığı/ Forum e-KİM" başlığı altında düzenlediği 2 günlük etkinlik, 6-7 Kasım'da İstanbul'da gerçekleşti.

Devamı için...

### Türkiye'den e-imza ihracatı

Özel kişi ve kuruluşlara e-imza sertifika satışı gerçekleştirmek üzere belirlenen iki şirketten biri olan Türktrust, e-imza konusunda elektronik sertifika sağlayıcılığının yanında bu alanda teknoloji de geliştiriyor.

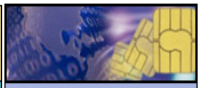
Devamı için...

### E-imza Nedir?

Kanunu'nda yer alan şekliyle elektronik imza; başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik...>>


### E-imza Kanunu

23 Ocak 2004 tarihli resmi gazetede yayınlanan, 5070 Sayılı Elektronik İmza Kanunu'nun amacı, elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasları düzenlemektir...>>



### ESHS

Elektronik sertifika hizmet sağlayıcısı, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir...>>

25 Aralık 2006, Pazartesi

## Üye Girişi

isim@eposta.com
••••••••
Giriş

Üye olmak istiyorum | Şifremi unuttum

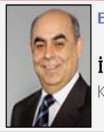
## Kurban Bağışı

TSK MEHMETÇİK VAKFI
KURBAN BAĞIŞI için son tarih: 31 Aralık 2006

## Kriptoloji Sempozyumu

II. ULUSAL KRİPTOLOJİ SEMPOZYUMU
15-17 ARALIK 2006

## Köşe Yazısı



E-imza Nasıl Öldürülür ?

İsmet KOYUN
KOBİL

## Güncel Haberler

- Ulusal E-İmza Sempozyumu Başladı
- Kimlik Yönetimi 2006 Forumu
- Türkiye'den e-imza ihracatı
- İSKİ'de e-imza dönemi başlıyor
- Serbest Bölgeler Bilgisayar Uygulama Programı için süre uzatıldı.
- Ulaştırma Bakanlığı, Bilgi Üniversitesi ile İşbirliği Protokolü İmzaladı.
- Turkcell E-imzayı Yaygınlaştıracak
- E-imzada ASP dönemi
- CeBIT'te E-imza Forumu Gerçekleştirildi.
- Strateji mercek altında

» Diğer Haberler...

# PGP

- Pretty Good Privacy
- Phil Zimmerman
- Uluslararası sürüm
- Orijinal PGP'nin grafik ara yüzü yok, kullanımı zor
- RSA açık anahtar şifreleme algoritmasına dayanıyor

# "Saldırının Nereden ve Nasıl Geleceğini Bilmeyen Hiç Kimse Savunma da Yapamaz"

(Güven 2004)