YMT311 Bilgi Sistemleri ve Güvenliği

Şifreleme Bilimi ve Teknikleri

Prof. Dr. Resul DAŞ

Bölüm - 5

1

Prof. Dr. Resul DAŞ
Fırat Üniversitesi
Yazılım Mühendisliği Bölümü

Konu Başlıkları

- Kriptoloji
- Sezar
- Pigpen
- Ebced
- Enigma
- Echelon
- Steganografi
- MD5
- RSA
- SHA1
- SHA2

Şifreleme Bilimi ve Şifreleme Teknikleri

- **Kriptoloji**
  - **Kriptografi** :Bilgiyi şifreli hale dönüştürme işlemidir.
  - **Kriptoanaliz** :Bir şifreleme sistemini veya sadece şifreli mesajı inceleyerek, şifreli mesajın açık halini elde etmeye çalışan kriptoloji disiplinidir.

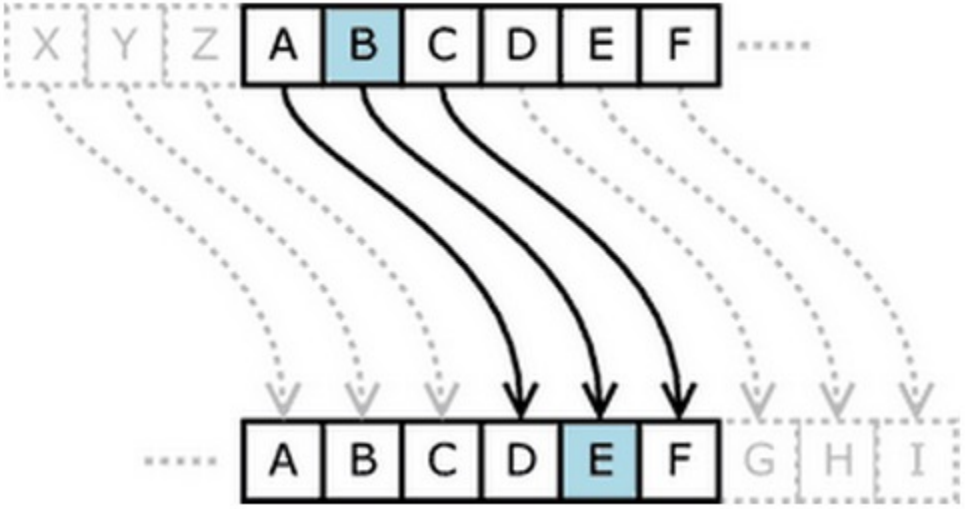
Şifreleme Bilimi ve Şifreleme Teknikleri

- **Şifreleme (Encryption):** Düz metni şifreli metne çevirme sürecidir.
- **Şifre Çözme(Description):** Şifrelenmiş metni düz metne çevirme işlemidir.
- **Anahtar(Key):**Şifreli metnin nasıl elde edildiğine dair kod parçasıdır.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **Sezar Şifreleme**

- Şifrelenecek metin alfabede kendinden sonra gelecek 3. harfle yer değiştirerek oluşturulmaktadır.



Şifreleme Bilimi ve Şifreleme Teknikleri

$C \equiv P+3 (Mod 29)$

Şifrelemek istediğimiz metnimiz "BU MESAJ ÇOK ÖNEMLİDİR" olsun.

Mesaja karşılık gelen sayısal denklileri yazmadan önce belli kelimelerin tanınmasına dayana başarılı şifre çözme tekniklerini engellemek için mesajı beşli bloklara böleriz..

BUMES AJÇOK ÖNEML İDİR.

Harflerin sayısal denkliklere dönüştürülmesiyle;

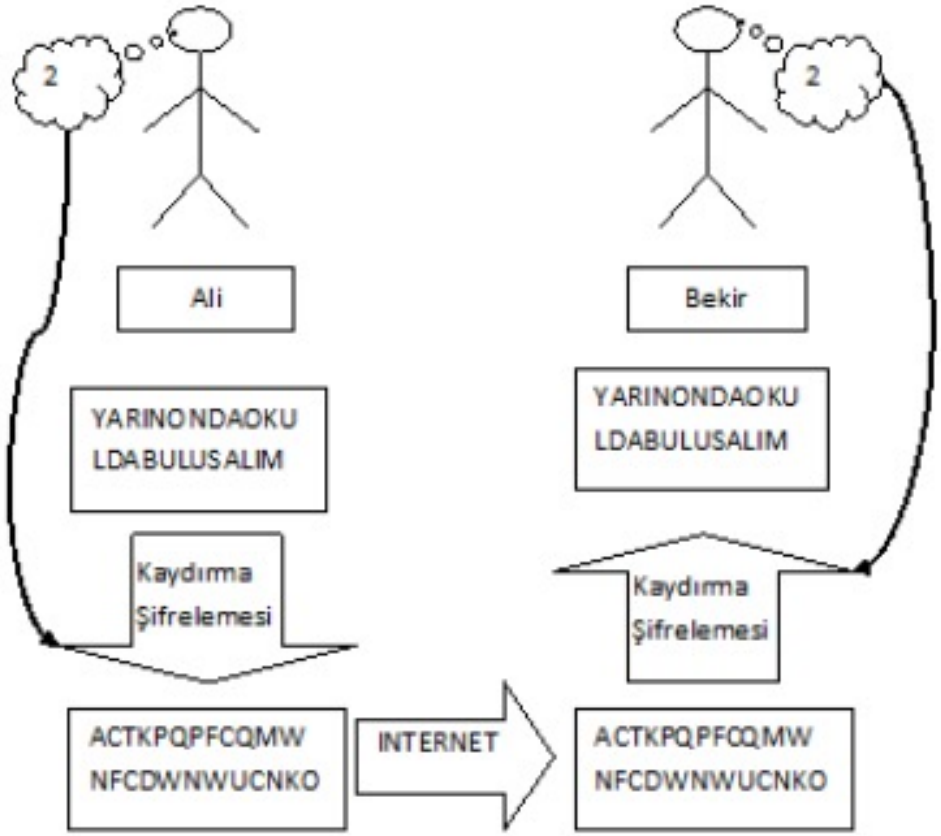
1 24 15 5 21 0 12 3 17 13 18 16 5 15 14 11 4 11 20

elde ederiz.

$C \equiv P + 3 (\text{mod } 29)$ Caesar dönüşümünün uygulanmasıyla

4 27 18 8 24 3 15 6 20 16 21 19 8 18 17 14 7 14 23

Şifreleme Bilimi ve Şifreleme Teknikleri



Kaydırma nasıl yapılır ?

Şifreleme Bilimi ve Şifreleme Teknikleri

- **EBCED HESABI**
- Ebced hesabı, Ebced rakamlarını yani alfabetik bir sayı sistemini kullanarak, kelimelerin sayısal değerini hesaplamaktır. Arap alfabesinin eski sıralanışından (elif, ba, cim, dal) ilk dört harfinin okunuşlarıyla (E-B-Ce-D) türetilmi[illegible]

elif ا	1	Ha ح	8	sin س	60	te ت	400
be ب	2	Tı ط	9	`ayn ع	70	peltek se ث	500
cim ج	3	yâ ي	10	fe ف	80	Hı خ	600
dal د	4	kef ك	20	Sad ص	90	zel ذ	700
he ه	5	lâm ل	30	kaf ق	100	Dad ض	800
vav و	6	mim م	40	ra ر	200	Zı ظ	900
ze ز	7	nun ن	50	şın ش	300	ğayn غ	1000

Şifreleme Bilimi ve Şifreleme Teknikleri

- Özellikle Mimar Sinan'ın eserlerinde, boyutların modüler düzeninde çok sık kullanılmıştır.

- Süleymaniye'de zeminden kubbe üzengi seviyesi 45
- kubbe alemi 66 arşın yüksekliktedir .

- Ebced'e göre "Âdem' 45, "ALLAH" lafzı da 66 etmektedir.
- Yine Selimiye'de de kubbeyi taşıyan 8 ayağın merkezlerinden geçen dairenin çapı 45 arşındır.

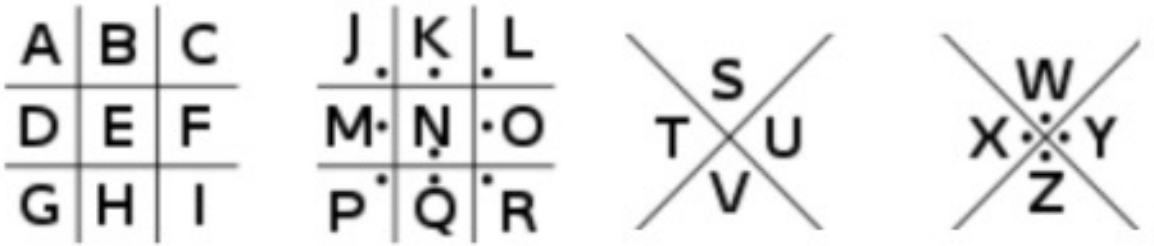
- Kubbe kenarı zeminden 45,
- minare alemi buradan itibaren 66 arşındır.
- Süleymaniye ve Selimiye'nin görünen silüetleri 92 arşındır
- bu da "Muhammed" kelimesinin ebced karşılığıdır.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **Tarih düşürme sanatı**
- Ebced hesabının en fazla kullanıldığı yer hiç şüphesiz tarih düşürmedir.
- Bunun için o olayın tarihini verecek ustalıklı bir kelime veya mısra söylenir ki, hesaplandığında o olayın tarihi ortaya çıkar.
- "*Tarih düşürme sanatı*" adı verilen bu sanat divan edebiyatı boyunca kullanılmış ve kitabelerde yer almıştır.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **Pigpen (Mason) Şifrelemesi**



Şifreleme Bilimi ve Şifreleme Teknikleri

- **Echelon Sistem**
- Dünyanın en büyük casusluk ağı olarak bilinir.
- Dünyadaki sayısal trafiğin %90 bu sistem ile dinlendiği iddia edilmektedir.
  - Belirli kelimeler sisteme girilerek bu kelimelerin geçtiği konuşmalar incelenmektedir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Diğer bir sistem ise **PROMİS** (Dava Yönetim Sistemi)
- Bu sistem ile;
  - Birçok ülkenin banka sisteminin kilitlenebileceği
  - Kontrollü mali krizler çıkarılabileceği
  - Uluslar arası ihalelere girecek şirketlerin dinlendiği

  İddia edilmektedir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **ENİGMA**
  - Elektromekanik bir şifre çözme makinesidir.
  - 1919 yılında geliştirilen makine Almanlar tarafından kullanılmıştır.
  - II. Dünya savaşında önemli bir rol oynamıştır.
  - İngilizler tarafından ele geçirilen bir gemide enigmanın kullanma kitabı ele geçirilmiştir.
  - II. Dünya savaşının bu sayede 1 yıl daha erken bittiği düşünülmektedir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **Steganografi**
  - Eski Yunanca'da "gizlenmiş yazı" anlamına gelen bilgiyi gizleme bilimidir.
    - Resim
    - Ses
    - Video

    ortamlarına bilgiler gizlenebilir.

Şifreleme Bilimi ve Şifreleme Teknikleri

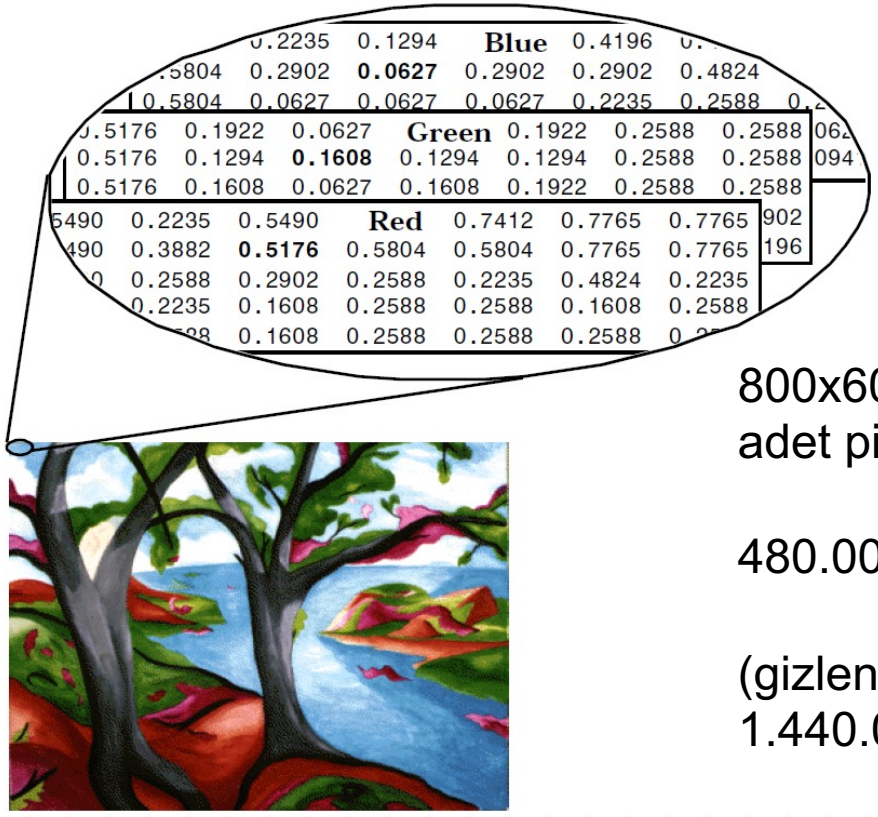
Bilginin Saklandığı Resim

Saklanan Resim

Şifreleme Bilimi ve Şifreleme Teknikleri

- **Steganografi**
  - Resim dosyalarının özellikleri;
  - 1- Bütün resimler dosya başlığı (header) ve piksellerden oluşur.
  - 2- Her piksel sadece bir renk içeren küçük bir bloktur.
  - 3- Her pikseldeki renk temel 3 rengin karışımından elde edilir.
  - 4- Her pikselde bu 3 rengin verileri tutulur. Her temel renk 1 pikselde 1 byte (0..255) yer kaplar, yani 1 piksel 3 byte veri taşır.

Şifreleme Bilimi ve Şifreleme Teknikleri



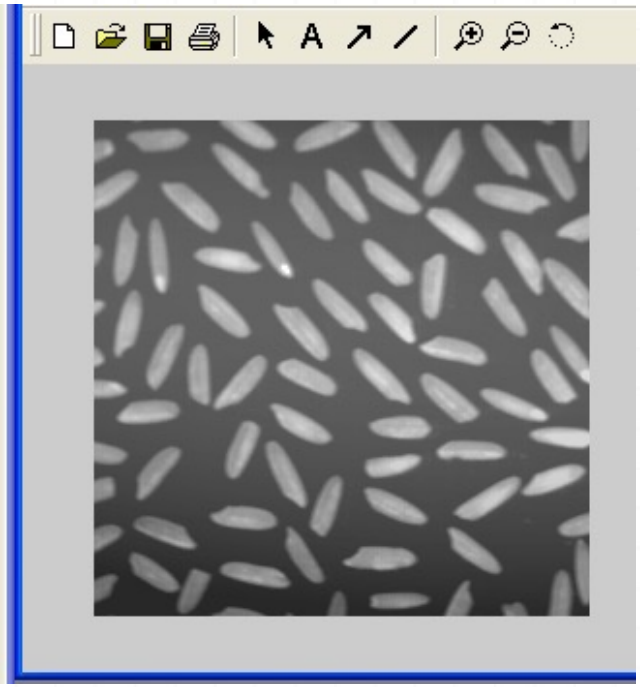
800x600 ebatında bir resimde 480.000 adet piksel bulunur.

480.000 x 3 bit = 1.440.000 bit

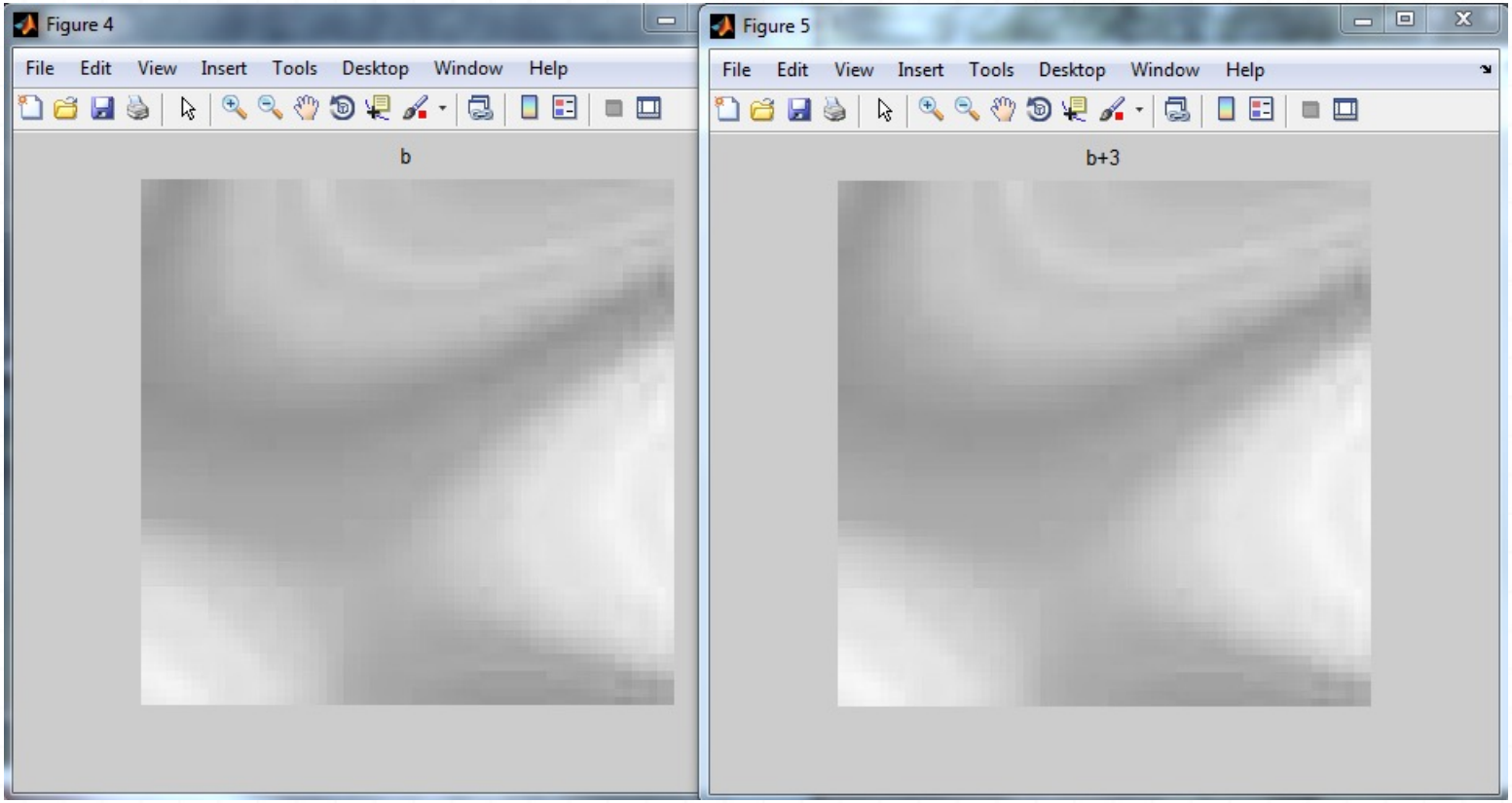
(gizlenecek olan veri için kalan yer)
1.440.000 bit = 175,7 KiloByte

Şifreleme Bilimi ve Şifreleme Teknikleri

1	2	3	4	5	6	7	8
81	80	81	81	81	81	81	81
81	81	81	82	81	81	81	81
82	81	81	81	81	82	81	81
81	82	82	82	82	82	82	82
82	82	82	82	82	82	82	82
82	82	82	82	82	82	82	82
82	83	83	83	83	83	83	83
83	83	83	83	83	83	83	83
83	83	83	84	84	84	84	84
91	90	96	97	98	100	100	97
112	113	118	120	120	126	126	123
131	132	135	135	136	142	146	143
145	145	146	145	147	153	159	162
148	149	149	149	148	155	166	169
152	148	149	149	150	160	174	179
152	149	149	152	152	166	177	184
157	153	155	155	157	168	177	175
161	155	155	157	152	163	158	155
160	158	152	152	144	141	133	124
156	151	146	136	127	118	110	99
143	135	128	115	109	98	94	88



Şifreleme Bilimi ve Şifreleme Teknikleri



Şifreleme Bilimi ve Şifreleme Teknikleri

- **HASH**
- Büyük tanım bölgelerini küçük değer bölgelerine dönüştürülür.
- Hash fonksiyonu girdi olarak bir mesajı alır ve ***hash kodu***, ***hash sonucu,*** ***hash degeri*** veya kısaca ***hash*** ile belirtilen bir çıktı üretir.
- Daha kesin bir ifadeyle bir hash fonksiyonu keyfi sonlu boyutlu bit şeritlerini n-bit diyebileceğimiz sabit uzunluklu şeritlere dönüştürür.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **HASH**
- Başka bir ifadeyle hash fonksiyonu gönderilecek mesajdan matematiksel yollarla sabit uzunlukta sayısal bilgi üretme işlemidir.
- Üretilen sayısal bilgi ''mesaj özeti'' olarak bilinir. Mesaj özeti anlamsız bir bilgidir.
- Hash fonksiyonu geri dönüşümü olmayan bir fonksiyondur.
- Yani mesajın özetine bakarak mesajın kendisini elde etmek mümkün değildir. En iyi bilinen hash fonksiyonları MD-4, MD-5 ve SHA'dır.
- Örneğin; Sayısal İmzalama

Şifreleme Bilimi ve Şifreleme Teknikleri

- Bu süreci kimyasal bir reaksiyon gibi düşünebilirsiniz.
- Yumurta pişirildikten sonra yumurtanın eski haline dönüştürülmesi imkansızdır. Bu durumda hash sonucu karşıdaki bilgisayara gönderildiği esnada, orijinal mesajın da hash sonucuyla birlikte gönderilmesi gerekiyor.
- Alıcı bilgisayar, orijinal mesaja hash fonksiyonunu uygulayıp, çıkardığı sonucu kendisine orijinal mesajla gönderilen hash sonucuyla karşılaştırıyor.
- Eğer alıcı bilgisayarın oluşturduğu hash sonucu, mesajla birlikte
- gönderilen hash sonucuyla aynıysa, alıcı bilgisayar kendisine gelen orijinal mesajın üzerinde oynama yapılmadığından emin olmuş oluyor.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **MD5(Message-Digest algorithm5)**

- Tek yönlü (açık anahtarlı) şifreleme tekniğidir. Bir yere gönderilecek veri 128 bitlik özetler hâlinde şifrelenir.

- "**oktay**" kelimesi için MD5 şifreleme:

- f55694370a2e688a08edd2a3ee184e0d

Şifreleme Bilimi ve Şifreleme Teknikleri

- **SHA-1(Secure Hash Algorithm)**
- Tek yönlü (açık anahtarlı) şifreleme tekniğidir.Verileri 160 bit uzunluğunda özetler.
- Web alanında geniş kullanımı vardır.
- SHA-2 adı altında hazırlanmış 224, 256, 384, 512 bit uzunluğunda özetler üreten çeşitleri vardır.

Şifreleme Bilimi ve Şifreleme Teknikleri

Şifreleme Algoritması	Şifrelenecek Veri	Şifrelenmiş Veri
MD5	fatma	38ab93488e52710515c3095a83a92bcf
MD5	burak	39109a5bb10ccb7aff1313d369804b74
MD5	fırat	fbc06de89851f43007f2996a31e9f1b1
MD5	firat	e652dc5596070e8dc3fedfb32be655a6
SHA-1	fatma	5e927503d30f50bd44c9a31c6625984c442b78ae
SHA-1	burak	da7169592c4847350b7262ccf9f7b41b72c9d0be
SHA-1	firat.edu.tr	cdfe0a27180d66d4a4f69494c3f417786b15ba20
SHA-1	www.firat.edu.tr	26e8799f7d049f8fd908b597b7f4bd28c3f8edfd

Şifreleme Bilimi ve Şifreleme Teknikleri

Örneğin "**oktay**" kelimesinin SHA-1 ve SHA-2 özetleri aşağıdaki gibidir.

SHA-1 (160bit)	22771aca22f13b0e26b3011542bde186a5c47690
SHA-256	f6ff3f7aa48c6357fb3f9d09f8fdde97060e3121afc0db0e35ec807c62922456
SHA-384	d64f697923b1c8c425643c0f03f86c3c12b0af576521e41096cef9e95474661f947453a5ab2430928dfd02a381af93e2
SHA-512	278179b20946ee2cb093545ca8727f53607ba058acb2ed888aac8f32ecaf74d8572479ff6380fbf34be9c274080eeb1e7f055b32e3204ce2bda6afd1714ac75c

Şifreleme Bilimi ve Şifreleme Teknikleri

- **DES (Veri Şifreleme Standardı, Data Encryption Standard)**
- DES, veri şifrelemek ve şifrelenmiş verileri açmak için geliştirilmiş bir standarttır.
- Esas olarak kullanılan algoritmaya DEA yani Data Encryption Algorithm (Veri Şifreleme Algoritması) adı verilir.
- Bu algoritmanın standartlaştırılmış haline DES denilmektedir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **RSA Açık Anahtar Algoritması**

  RSA, güvenliği tam sayıları çarpanlarına ayrımanın algoritmik zorluğuna dayanan bir tür Açık anahtarlı şifreleme yöntemidir. 1978'de Ron Rivest, Adi Shamir ve Leonard Adleman tarafından bulunmuştur.

  Bir RSA kullanıcısı iki büyük asal sayının çarpımını üretir ve seçtiği diğer bir değerle birlikte ortak anahtar olarak ilan eder. Seçilen asal çarpanları ise saklar. Ortak anahtarı kullanan biri herhangi bir mesajı şifreleyebilir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Yeterince büyük iki adet asal sayı seçilir: Bu sayılar örneğimizde p ve
- q olsunlar.
- n=pq
- $\varphi(n) = (p-1)(q-1)$ *(Totient değeri)*
- $1 < e < \varphi(n)$
- $d \equiv 1 \bmod (\varphi(n))$. *(e'nin mod(φ(n)) çarpmaya göre tersi)*

- Şifreleme işlemi:
- $c = m^e \bmod n$

- Şifrenin Açılması:
- $m = c$
- $d \bmod n$

Şifreleme Bilimi ve Şifreleme Teknikleri

- İki farklı asal sayı seçelim. p=61 ve q=53 olsun.
- n=pq değerini hesaplayalım. 61 × 53 = 3233
- Totient değerini hesaplayalım. (61-1)(53-1)=3120

- 1 ile 3120 arasında 3120 ile aralarında asal olan bir değeri seçelim. e=17 olsun.

- d değeri, e'nin mod (3120)'e göre çarpmaya göre tersi olarak hesaplayalım. d=2753.

- **Ortak Anahtar: (n=3233, e=17)**
- Her bir m mesajını şifreleyecek fonksiyon $m^{17} \pmod{3233}$.
- **Özel Anahtar(n=3233, d=2753)**
- Herhangi bir c şifreli mesajını çözme fonksiyonu $c^{2753} \pmod{3233}$.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Örneğin;
- m=65 i şu şekilde şifreleriz. *(bitler)*
  - $c=65^{17}(\text{mod } 3233)=2790$.
  - c=2790'nın şifresini şu şekilde çözeriz.

    $m=2790^{2753}(\text{mod } 3233)=65$

Örneğin m=123 olsun:

17 mod 3233 = 855 olarak şifreli metin bulunur.
açacak taraf için tersi işlem uygulanır:

2753 mod 3233 = 123 şeklinde orijinal mesaj geri elde edilir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **BitLocker Şifreleme**

- Windows 7 işletim sistemi ile gelen özelliklerden biri de Bitlocker sürücü şifreleme özelliğidir.

- Windows'un eski versiyonlarında dosyalar ayrı ayrı şifrelenebiliyordu. Bu özellik sayesinde sürücünün kendisi şifrelenebilmektedir.

- Şifrelenmiş bir sürücüye yeni bir dosya attığımızda bu dosya bitlocker tarafından otomatik olarak şifrelenir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Ayrıca bitlocker ile yapılan şifreleme işlemlerinde şifreleme için gerekli dosyalarda sürücü içersinde depolanır.
- Dolayısıyla şifrelerimizi ele geçirmek isteyenler için gerekli olan bilgiler de sürücü içersinde muhafaza edilerek güvenlik düzeyi artırılmış oluyor.
- Bitlocker ile şifrelenmiş bir sürücüye erişmek için parola koruması yada akıllı kartlarda kullanabiliyoruz.
- Windows 7 de,Vista'dan farklı olarak harici depolama aygıtlarımızı da şifreleyebiliyoruz.Yani flash disklerimizi de şifreleyebiliyoruz.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **WEP Şifreleme**
- WEP (Wired Equivalent Privacy), kablosuz ağ Veri bağ tabakasında çalışan şifreleme yöntemidir.
- Standart olan WEP şifrelemesi WEP-64 olarak bilinir ve 40 bitlik anahtar kullanır.
- Günümüzde WEP kullanan ağlarda daha çok 104 bitlik anahtar kullanan WEP-128'e rastlanır. Daha güvenli ağlar 232 bitlik anahtarı mümkün kılan WEP-256 kullanıyor olabilir.
- Günümüzde bu şifreleme yetersiz kaldığından daha güvenli olan WPA şifreleme yöntemi yaratılmıştır

Şifreleme Bilimi ve Şifreleme Teknikleri

- **WPA Şifreleme**
  - WEP şifreleme sisteminden daha güvenli olduğu söylenen ve WEP şifrelemeden daha yeni bir teknolojidir.
  - WPA (Wi-Fi Protected Access)Wi-Fi korumalı Erişim olarak adlandırılır.WPA , WEP'in açıklarını geçici olarak da olsa kapatmaya yönelik bir standarttır.
  - İki modda çalışır.
  - Birincisi WPA-PSK denilen paylaşımlı anahtar koruması ,
  - İkincisi ise yeni protokol olan TKIP(Temporal Key Integrity Protocol)'in şifrelemesi ve 802.1X asıllama ile güvenliktir.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **WPA Şifrelemesi**
- İstemci ile AP (Erişim Noktası) bağlantı kurmadan önce, aygıtların birbirini bulması gerekiyor.
- Mevcut WLAN ağlarının bir listesini görüntülemek için, istemci "araştırma sorgusu" gönderir.
- Yani "*Merhaba, biri var mı*?" mesajıdır bu.
- "*Evet, burdayız*" diye karşılık gelince daha sonra AP'ler SSID bilgisini (Hizmet Kümesi Tanımlayıcı) yani WLAN'ın
- ismini
- zaman bilgisini
- ve diğer bilgileri aktarır.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Daha sonra istemci "Açık Sistem İsteği" (Open System Request) göndererek ağlara şifreli olup olmadıklarını soruyor.
- Yönlendirici de buna uygun yanıtı veriyor.
- İstemcinin sıradaki adımı ise, yönlendiriciden kendisini ağa dahil etmesini istemek.
- Bu "Bağlanma İsteği"ne AP'den bir "Bağlanma Yanıtı" geliyor.
- Eğer sistem şifresiz ise, istemci "Açık Sistem Doğrulama" (OSA) ile kimliğini doğruluyor.
- AP bunun üzerine kimlik saptamanın başarılı olduğunu belirten bir ileti yayınlayıp bağlantıyı kuruyor.

Şifreleme Bilimi ve Şifreleme Teknikleri

- **Şifreli bir bağlantı kurmak içinse;**
  - WPA'nın da kendi içinde iki çeşidi var:
  - Biri işyerlerine, diğeri ise küçük özel ağlara yöneliktir.
  - Aralarındaki fark;
  - Bağlantı kurma sırasında, istemcinin sizin belirlediğiniz bir parolayı, yani PSK (önceden paylaşılmış anahtar) kullanılıyor olması
  - Şirket WLAN'larında ise anahtar dağıtımından sorumlu "*Radius server*" adlı özel bir sunucunun PSK'nın yerine geçiyor olması

Şifreleme Bilimi ve Şifreleme Teknikleri

- WPA'nın ilk adımında;
- İstemci ile erişim noktası, WLAN ağ adı SSID'yi, ana parola olarak kullanarak bir PMK (eşleştirme ana anahtarı) oluşturuyorlar.
- Aygıtlar şu anda PMKSA (Eşleştirme Ana Anahtarı Güvenlik Bağlantısı) denilen bir konumda bulunuyor.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Daha sonra taraflar, adına PTK (Geçici Eşleştirme Anahtarı) denilen 512 bitlik bir anahtar daha oluşturuyorlar.
- Bunun için de aygıtlar 4 taraflı bir el sıkışma protokolü uyguluyor.
- Yönlendirici, öncelikle istemciye içinde rasgele rakam bulunan bir çerçeve yolluyor.
- Bu ileti şifresiz olduğundan,kablosuz ağ üzerinden salt metin olarak iletiliyor.Ancak bu,güvenliği tehlikeye atmıyor çünkü en kötü durumda 4 taraflı el sıkışma başarısız oluyor ve yönlendirici bu işlemi yeni baştan başlatıyor.

Şifreleme Bilimi ve Şifreleme Teknikleri

- İstemci ise aşağıdaki parametreleri kullanarak PTK (Geçici Eşleştirme Anahtarı)'yi oluşturuyor:

- SNonce (gelişigüzel bir sayı)
- ANonce (AP için bir gelişgüzel sayı)
- PMK (Eşleştirme Ana Anahtarı) ve aygıtların MAC adresleri.

Şifreleme Bilimi ve Şifreleme Teknikleri

- PTK (Geçici Eşleştirme Anahtarı)'dan yönlendirici ve istemci tarafından dört geçici anahtar daha elde ediliyor:

- EAPOL anahtarı-şifreleme anahtarı
- EAPOL anahtarı-doğrulama anahtarı (bu sayede aygıtlar daha sonra asıl veri anahtarının aktarımını şifreleyebiliyor),
- veri şifreleme anahtarı
- ve veri doğrulama anahtarı.

- Bunların hepsi de 128 bit uzunluğundadır.

Şifreleme Bilimi ve Şifreleme Teknikleri

- Sıradaki ileti, istemciden yönlendiriciye gidiyor ve SNonce(gelişigüzel bir sayı)'ı içeriyor. Böylece yönlendirici aynı PTK'yi hesaplayabiliyor.
- Bağlantı henüz şifrelenmemiş olsa da, değişiklikleri saptayan MIC algoritması (Mesaj Doğruluk Denetimi) üzerine kuruludur.
- Gönderici, veri paketlerini seri olarak numaralıyor. Seri numarası da mesaja ekleniyor.
- Alıcı, seri numarası verilen paketleri kontrol ediyor ve paketler eşleşmezse, alıcı bu paketleri çöpe atıyor. Bu da çoğu korsan saldırısını daha en baştan eliyor.

Şifreleme Bilimi ve Şifreleme Teknikleri

- 4 taraflı el sıkışmanın üçüncü aşamasında yönlendirici istemciye bir "başarılı" paketi göndererek iki aygıtın da aynı geçici anahtara sahip olduğunu doğruluyor.
- El sıkışmasını sona erdirmek için, istemci, yönlendiriciye anahtar oluşturmanın sonlandığını belirten bir MIC mesajı gönderiyor.
- Bunun üzerine, yönlendirici, MIC'i kullanarak mesajı kontrol ediyor ve üzerindeki anahtarları etkinleştiriyor.

Sonuç

Sorular

Kaynaklar

- [1] IEEE Std 802.16-2004--IEEE standard for local and metropolitan areanetworks, part 16: "***Air Interface for Fixed Broadband Wireless Access Systems***".
- [2] David Johnston ve Jesse Walker--INTEL: "***Overview of IEEE 802.16 Security***"
- [3] Kitti Wongthavarawat--Thai Computer Emergency Response Team (ThaiCERT) National Electronics and Computer Technology Center,Thailand: "***IEEE 802.16 WiMax Security***"
- [4] Loutfi Nuaymi, Patrick Maillé, Francis Dupont, Raphaël Didier--École Nationale Supérieure des Télécommunications de Bretagne:"***Security issues in WiMAX/IEEE 802.16 BWA System***"
- [5] Yun Zhou ve Yuguang Fang--Department of Electrical and Computer Engineering,University of Florida, Gainesville:"***Security of 802.16 in Mesh Mode***"