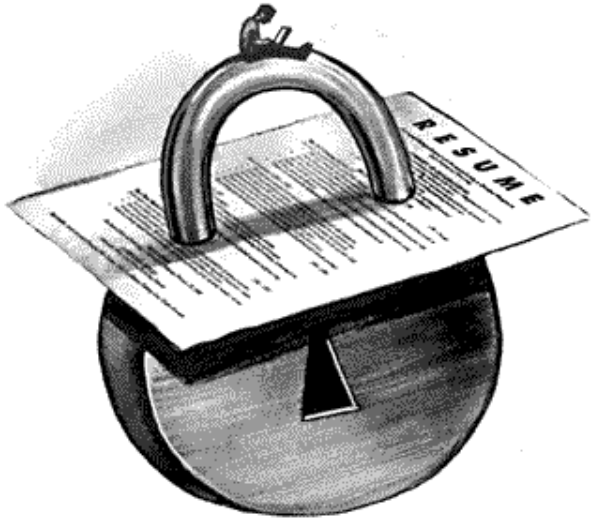
ŞİFRELEME ÇEŞİTLERİ



AES (Advanced Encryption Standard)

- AES (Rijndael) algoritması 128 bit veri bloklarını 128, 192, 256 bit anahtar seçenekleri ile şifreleyen bir algoritmadır.
- 128 bit anahtar için 10 döngüde şifreleme yaparken 192 ve 256 bit anahtarlar için sırasıyla 12 ve 14 döngüde şifreleme yapmaktadır.
- AES algoritmasında her döngü dört katmandan oluşur.
- İlk olarak 128 bit veri 4×4 byte matrisine dönüştürülür.
- Daha sonra her döngüde sırasıyla byte'ların yer değiştirmesi, satırların ötelenmesi, sütunların karıştırılması yapılır

DES (Veri Şifreleme Standardı, Data Encryption Standard)

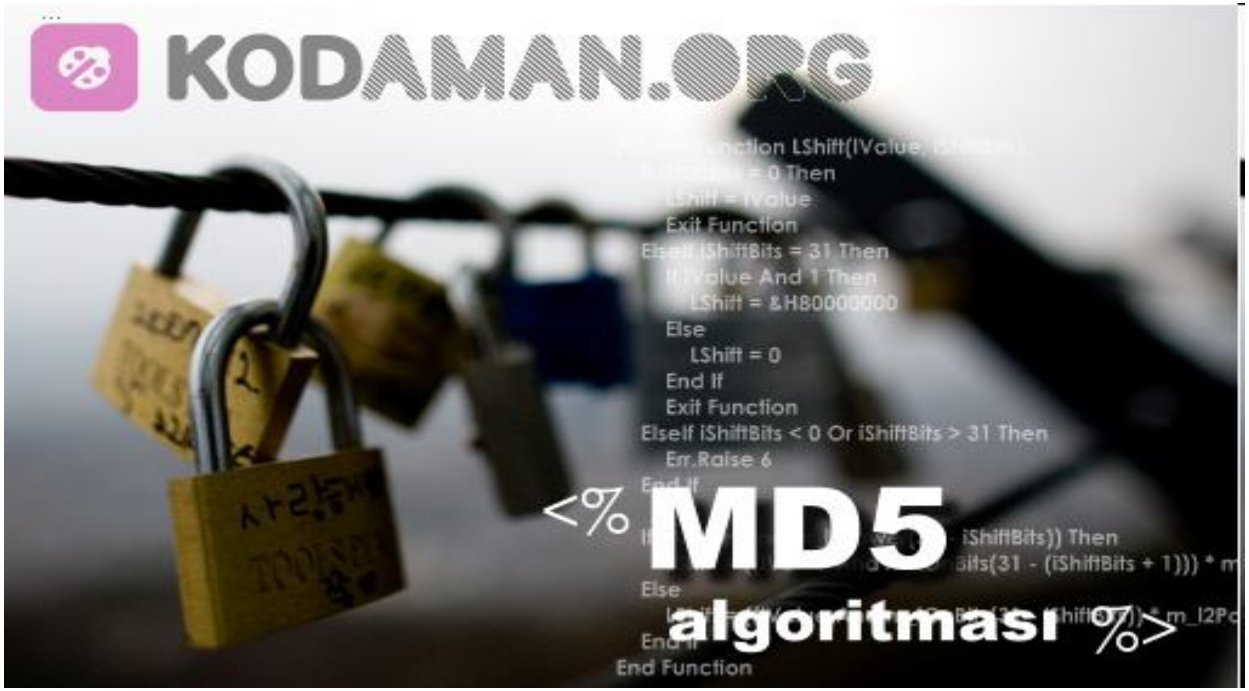
- DES, veri şifrelemek (encryption) ve şifrelenmiş verileri açmak (decryption) için geliştirilmiş bir standarttır. Esas olarak kullanılan yönteme (veya algoritmaya) DEA yani Data Encryption Algorithm (Veri Şifreleme Algoritması) adı verilir. Bu algoritmanın standartlaştırılmış halinin ismi DES olarak geçmektedir.
- DES yapısı itibari ile blok şifreleme örneğidir. Yani basitçe şifrelenecek olan açık metni parçalara bölerek (blok) her parçayı birbirinden bağımsız olarak şifreler ve şifrelenmiş metni açmak içinde aynı işlemi bloklar üzerinde yapar. Bu blokların uzunluğu 64 bittir.

RC-4 ŞİFRELEME

- RC4 algoritması şifrelenecek veriyi akan bir bit dizisi olarak algılar.RC4 belirlenen anahtar ile veriyi şifreleyen bir algoritmadır. RC4′ün başlıca özellikleri şunlardır:
- Genellikle hız gerektiren uygulamalarda kullanılır.
- Şifreleme hızı yüksektir ve MB/sn seviyesindedir.
- Güvenliği rastgele bir anahtar kullanımına bağlıdır.
- Tekrarlama periyodu 10100′den daha fazladır.
- Kötü anahtarı bulunmamaktadır.
- Anahtar uzunluğu değişkendir.

MD5 ŞİFRELEME

- MD5 (Message-Digest algorithm 5) Ron Rivest tarafından 1991 yılında geliştirilmiş bir tek yönlü şifreleme algoritmasıdır, veri bütünlüğünü test etmek için kullanılan, bir şifreleme algoritmasıdır. Bu algoritma girdinin büyüklüğünden bağımsız olarak 128-bit'lik bir çıktı üretir ve girdideki en ufak bir bit değişikliği bile çıktının tamamen değişmesine sebep olur.



- MD5’ın en çok kulanıdığı yerelerden biri, bir verinin (dosyanın) doğru transfer edilip edilmediği veya değiştirilip değiştirilmediğinin kontrol edilmesidir.

SHA-1 Şifreleme

- SHA (Secure Hash Algorithm – Güvenli Özetleme Algoritması), Amerika'nın ulusal güvenlik kurumu olan NSA tarafından tasarlanmıştır.
- SHA-1, uzunluğu en fazla 264 bit olan mesajları girdi olarak kullanır ve 160 bitlik mesaj özeti üretir. Bu işlem sırasında, ilk önce mesajı 512 bitlik bloklara ayırır ve gerekirse son bloğun uzunluğunu 512 bite tamamlar. SHA-1 çalışma prensibi olarak R. Rivest tarafından tasarlanan MD5 özet fonksiyonuna benzer.160 bitlik mesaj özeti üreten SHA-1 çakışmalara karşı 80 bitlik güvenlik sağlar.

KLASİK ŞİFRELEME TEKNİKLERİ

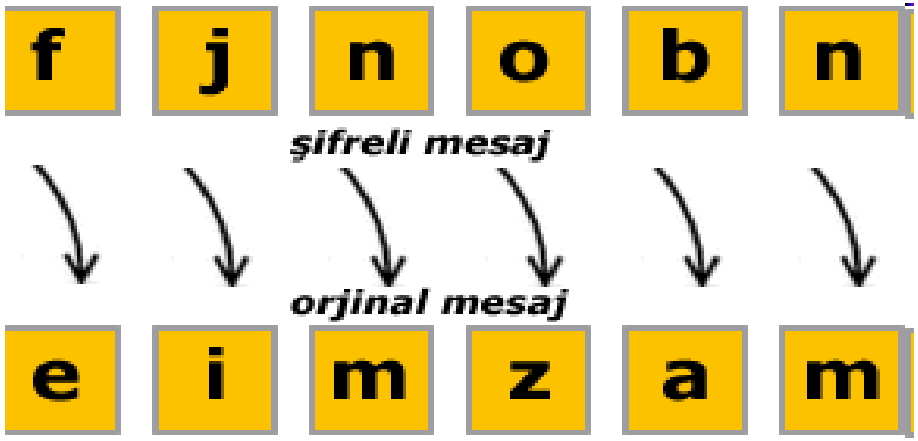
Steganography(Metni Gizleme)

- Şifrelenmemiş düz bir metni çeşitli dönüşümler kullanarak diğer kişilerce anlaşılamaz bir metin haline getirilmesi işlemidir. Verilebilecek en basit örnek, bir metnin tüm harflerinin başka bir metnin içindeki kelimelerin ilk harflerine gizlenmesidir. Örneğin; “**S**ezen **A**ksu **v**e **a**şk **ş**arkıları **b**enim **i**çin **t**üm **t**esellilerden **i**yidir.”

- Ancak her durum için böyle bir mesajı oluşturmak zor ve zaman alıcı bir işlemdir.
- Oluşturulacak mesajdaki kelimelerin anlamlı bir bütünlük oluşturacak şekilde bulunmasının ancak çok üst düzey bir yapay zeka uygulamasıyla bilgisayar ortamına aktarılması mümkündür. Hala daha “natural language processing” (bilgisayarların konuşma dillerini anlayabilmesi olarak basitçe tanımlanabilir) konusunda mükemmel bir sisteme ulaşılamamış olması kadar önemli bir nokta da kırılmasının çok kolay olmasıdır.

Caesar Cipher(Sezar Şifrelemesi)

- Bilinen en eski yerine koyma tekniğidir. Ünlü Roma İmparatoru Julius Caesar tarafından geliştirilmiştir. Sezar şifrelemesinde mantık her harfi kendisinden sonra gelen üçüncü harfle çembersel olarak değiştirmeye dayanmaktadır.
- Örneğin;
  düz metin: “Bilgisayarların şifreleri kırıldı”
  şifrelenmiş metin: “DLOİUÖÇBÇTOÇTKÖ ÜLHTĞOĞTL NKTKOGK”



- Sezar şifrelemesi 3 önemli zayıflığı vardır. Şifrelenmiş metinden hangi dilin kullanıldığı rahatlıkla anlaşılabilir. Türkçe için düşündüğümüzde sadece 28 ayrı şifreleme geliştirilmiş olabilir. Şifreleme ve deşifreleme algoritmalarının biliniyor ve kolaylıkla uygulanabiliyor olması da diğer zayıf olduğu yönüdür. Sezar şifrelemesi ile şifrelenmiş bir metin **"Brute Force"** bir saldırı ile kırılabilir. **Brute Force**, kelime anlamı olarak kaba kuvvet demektir. En zayıf ama en kesin saldırı yöntemidir. Sezar şifrelemesi gibi algoritmaların bilindiği yöntemlerde olası bütün kombinasyonların denenmesi demektir.

Tek Kullanımlık Karakter Dizisi (One-time Pad)

- Bu basit şifreleme yönteminde rastgele üretilen bir karakter (harf veya rakam) dizisi kullanılarak şifreleme yapılır. Açık mesaj içinde yer alan her karakter, üretilen dizide karşısına denk gelen karakterle işleme sokularak (Örneğin modüler toplama işlemi) şifreli mesaj elde edilir. Mesajı çözmek için rastgele dizinin bilinmesi gereklidir. Bu yönteme Vernam şifreleme yöntemi denir.

- **Açık Mesaj : BULUSMAYERIGAZZE**
  Rastgele Dizi : DEFRYPLCNMLJKHFGH
  Şifreli Mesaj : RLDYDOY....
  Bu yöntemin güvenliği Rastgele üretilen diziye bağlıdır. Bu dizi gerçekten Rastgele üretilmelidir, eğer bir kurala bağlı olarak üretilirse ve bu kural saldırgan tarafından bilinirse sistem kırılabilir.

ROT13 Şifreleme Tekniği

- ROT13 (Rotate13) yer değiştirme yöntemi kullanan bir Caesar(Sezar) şifreleme türüdür. Mantık olarak ingiliz alfabesindeki bir harfin 13 harf sonraki harf ile eşleşmesidir. Harflerin eşleşme tablosunu resimden göre bilirsiniz.

Base64 Şifreleme Tekniği

- Kodlama sırasında 3 baytlık veriler 6 bitlik dörtlü gruplara dağıtılırlar. Her bir 6 bitlik grup 0 ile 63 arasında bir sayı oluşturur (26=64). Aşağıdaki eşleşmeye göre her sayı bir ASCII yazdırma karakterine dönüştürülür:

Sayı	Karakter	Sayı	Karakter	Sayı	Karakter	Sayı	Karakter
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

- Bir base64 kodlamasının uzunluğu daimi olarak 4' ün katları şeklindedir, uzunluğu 4' ün katı olmayan hiç bir metin geçerli bir base64 metin değildir. base64 kodlaması bitmiş bir verinin uzunluğu 4'ün katı değilse, gerektiği kadar '=' karakteri çıktının sonuna eklenir, örneğin uzunluğu 10 olan bir çıktının sonuna '==' eklenmelidir.
- ASCII:ASCII'de 33 tane basılmayan kontrol karakteri ve 95 tane basılan karakter bulunur. Kontrol karakterleri metnin akışını kontrol eden, ekranda çıkmayan karakterlerdir. Basılan karakterler ise ekranda görünen, okuduğumuz metni oluşturan karakterlerdir.

Açık anahtarlı şifreleme

- **Açık anahtarlı şifreleme**, şifre ve deşifre işlemleri için farklı anahtarların kullanıldığı bir şifreleme sistemidir. Sistemin bu özelliğinden dolayı **asimetrik şifreleme** olarak da adlandırılır. Haberleşen taraflardan herbirinde birer çift anahtar bulunur. Bu anahtar çiftlerini oluşturan anahtarlardan biri gizli anahtar diğeri açık (gizli olmayan) anahtardır.

- Gizli anahtarın sadece bir sahibi vardır. Gizli anahtara sahip olan taraf gizli anahtar aracılığıyla, kendi açık anahtarıyla şifrelenmiş bilgilerin şifresini çözebilir, kendisine ait sayısal imzaları oluşturabilir ya da kendi kimliğini ispat edebilir.

Şekil 3-a Tek anahtar ile şifreleme ve şifre çözme

Şekil 3-b İki farklı anahtar ile şifreleme ve şifre çözme

- Açık anahtar, sadece gizli anahtarın sahibi tarafından oluşturulabilir ve herkesin erişimine açıktır. Açık anahtarla, bilgiler sadece gizli anahtarın sahibi tarafından çözülebilecek şekilde şifrelenebilir ya da gizli anahtar sahibinin sayısal imzasının ve kimliğinin doğruluğu kontrol edilebilir.
- Simetrik şifreleme algoritmalarının aksine, asimetrik şifreleme algoritmalarında güvenli bir "ilk anahtar değişimi" ihtiyacı bulunmamaktadır.