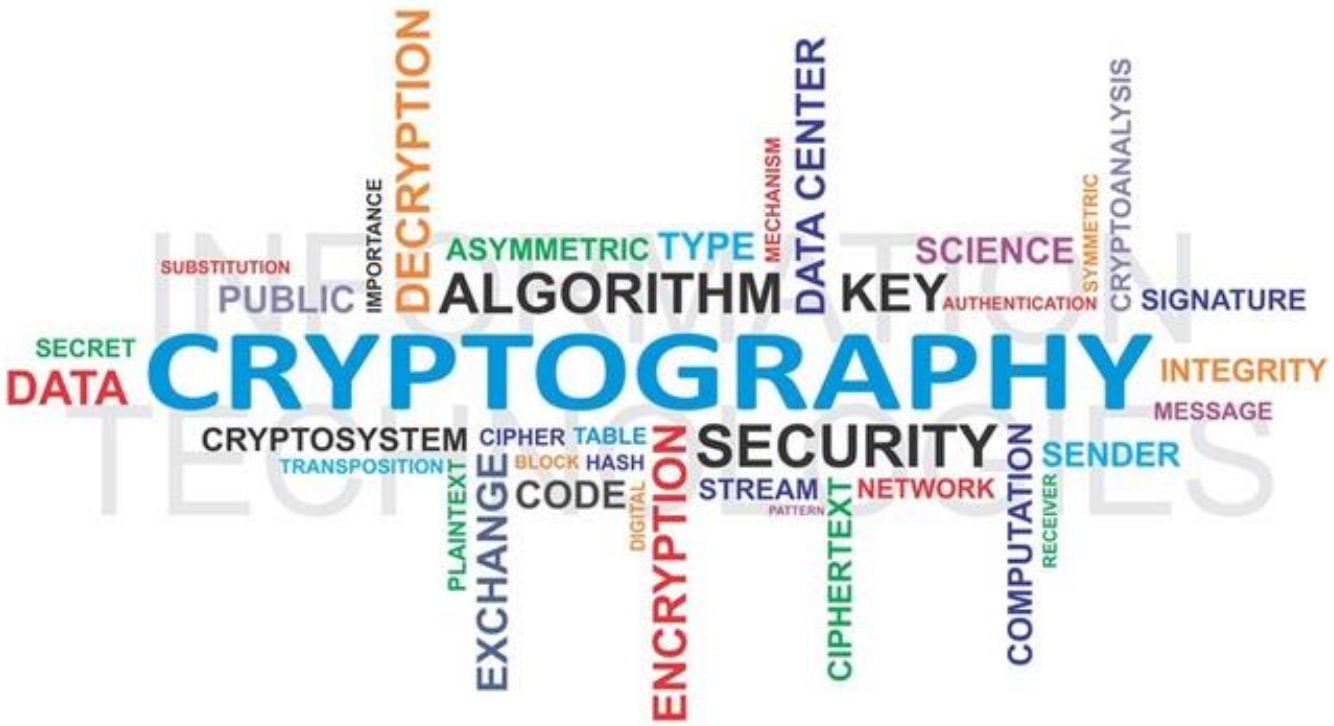
Necmettin Erbakan Üniversitesi

Bilgi Güvenliği
2022-2023 Güz Dönemi

Dr. Alperen Eroğlu
aeroglu@erbakan.edu.tr

Hafta-4

Siber Güvenliğin Temelleri – II (Şifre Bilim **(**Kriptografi**),** Şifreleme Algoritmaları, Anahtarlar, Ciphers**)**



https://www.enisa.europa.eu/news/enisa-news/cryptographic-tools-are-important-for-civil-society-and-industry

Hafta -4

Siber Güvenliğin Temelleri – II (Şifre Bilim (Kriptografi), Şifreleme Algoritmaları, Anahtarlar, Ciphers)

- Şifreleme Algoritmaları
  - Sezar Şifreleme Yaklaşımı
  - Sezar Açık Anahtar Şifreleme Yaklaşımı
  - Polialfabetik Şifreleme Yaklaşımı
  - Vernam (One-time Pad) Şifreleme Yaklaşımı
  - DES (Data Encryption Standard) Algoritması
  - RSA (Rivest, Shamir ve Adleman) Algoritması
  - AES Algoritması

Şifreleme Algoritmaları

- Algoritmalar, şifreleme ve şifre çözmede kullanılan matematiksel işlemleri içerirler. Güvenlikleri ise, çalışma biçimlerine ve daha önce de vurgulandığı gibi seçilen anahtar uzunluklarına bağlıdır.

- *Sınırlandırılmış algoritma* yaklaşımı : Çalışma biçimi veya kullanılan matematiksel yaklaşım gizleniyorsa! (**Sizce güvenilir midir?**)

Şifreleme Algoritmaları

- Bir algoritmanın güvenilirliği o algoritmanın herkese açık olmasından, bir başka ifadeyle, teorik yapısının herkes tarafından biliniyor olmasından geçmektedir.

- Sistem veya bilgi güvenliği, kullanılan anahtara veya anahtar çiftlerine bağlıdır.

- Üçüncü şahısların algoritmayı bilmesi ve teorisini kavraması önemli değildir. Burada asıl önemli olan, gizli veya özel anahtarın başkaları tarafından bilinmemesidir.

Şifreleme Algoritmaları

One-way function:

Okuma Önerisi:
https://bilgisayarkavramlari.com/2009/03/17/kapak-fonksiyonu-trapdoor-function/

- **Algoritmalarda; şifreleme işlemleri, özel matematiksel fonksiyonlar yardımıyla yapılır.**

- Bu tür fonksiyonlarda, X tanım kümesinden Y aktarım veya dönüşüm kümesine bir *f* fonksiyonu tanımlanmıştır. X kümesinin her bir elemanına *f* fonksiyonu uygulandığında, Y kümesi çıkışları elde edilir. Tek yön fonksiyonu olarakta bilinen bu yaklaşımda, çıkışlardan hareket ederek girişler elde edilemezler. Yani Y kümesinden X kümesine bir f^{-1} fonksiyonu elde edilemez. Sebebi ise her Y kümesi elemanıyla bir X kümesi elemanı eşleştirilememektedir.

Şifreleme Algoritmaları

Bijective function:

- Algoritmalarda, eşleşme (bijeksiyon) fonksiyonu, diğer bir yaklaşım olup, X tanım kümesinden Y aktarım kümesine bir *f* fonksiyonu olarak tanımlanır. Tek yön fonksiyonunun aksine, bu fonksiyonun çıkışlarından girişler elde edilebilmektedir. Sebebi ise, X kümesinin her bir elemanına *f* fonksiyonu uygulandığında, Y kümesinin tüm elemanları çıkış olarak elde edilmesidir. Bunun sonucu olarak, Y kümesinden X kümesine f^{-1} fonksiyonu elde edilebilir.

Şifreleme Algoritmaları

- Şifreleme algoritmaları, simetrik ve asimetrik fonksiyonlar olarak ikiye ayrılırlar.
- Her iki fonksiyon türünde, girdi olarak alınan veriler, parametreler dahilinde işlenir ve çıktı olarak, şifrelenmiş veri elde edilir.
- İletim esnasında herhangi bir saldırganın bu verilerden bilgi edinebilmesi, fonksiyonun içeriğine bağlı olarak zordur.
- Fonksiyon, sabit ve parametresiz ise güvenilirlik ve esneklik çok daha az olacaktır. Üçüncü şahıslardan veriyi gizlemek veya saklamak, sabit bir yöntem ile pek de mümkün olmayacaktır.
- Daha çok, parametrik bir fonksiyon tercih edilmektedir. Bu tür fonksiyonların güvenilirlik derecesini parametre ve bunlara karşılık gelen çıktı kombinasyonlarının belirleyeceği unutulmamalıdır.

Şifreleme Algoritmaları

Şifreleme algoritmalarında aranan bir takım özellikler:

- Şifrelenmiş mesajın deşifre edilmesi esnasında bilgi kaybı olmaması,
- İhtiyaç duyulan güvenlik seviyesine göre şifreleme işleminin zorluk seviyesinin seçilebilmesi,
- Önemli olmayan bilgilerin düşük seviyeli şifreleme yaklaşımları ile, yüksek seviyeli bilgi içeren dokümanlarının ise yüksek seviyeli şifreleme yaklaşımlarıyla şifrelenebilmeleri,
- Verimi düşürecek, maliyeti ve işgücü kaybını arttıracak yaklaşımları içermemesi,
- Şifreleme işlemlerinde güvenlik seviyesinin mümkün olduğunca yüksek olması,

Şifreleme Algoritmaları

Şifreleme algoritmalarında aranan bir takım özellikler:

- Basitlik ve kolaylıkla gerçekleştirilebilme özelliğinin ön planda olması,
- Kullanılan algoritmaların karıştırıcı özelliği olması,
- Şifrelenmiş mesaj ile düz metin arasındaki ilişkilerin zor kurulabilmesi,
- Şifreleme yaklaşımlarının herkese açık olması ve
- Açıklarının ortaya çıkarılabilmesi için, başkaları tarafından test edilebilmesinin sağlanması

Şifreleme Algoritmaları

Güvenli bir iletişimde kullanılan şifreleme algoritmaları, yaklaşımları, protokolları ve fonksiyonlarından bazıları:

Sezar,
MD2, MD4, MD5,
RSA, Lucifer, Blowfish, AES,
CAST 128, DES, 3DES, IDEA,
Skipjack, Gost, El-Gamal, Schnorr,
Elliptic Curve, Needham-Schroeder,
Diffie-Hellman,
PGP, S/MIME, IPSec, Kerberos,
RIPEMD, HMAC, SHA-1 ve SHA-2,

Sezar Şifreleme Yaklaşımı

- En eski şifreleme metotlarından birisidir.

Mesajın Şifrelenmesi (Encryption)

$$E(M) = M+3 \bmod 29 = C$$

Fonksiyondaki; ‘M’ mesajı, ‘E’ şifreleme işlemini (encryption), ‘C’ ise şifrelenmiş mesajı ifade etmektedir. ‘29’ ise, şifreleme yapılacak olan dildeki karakter (harf) sayısıdır. Türkçemizde 29 alfabetik karakter olduğu için burada 29 rakamı kullanılmıştır.

Mesajın Şifrelenmesi (Decryption)

$$D(C) = C- 3 \bmod 29 = M$$

Bu formülde, ‘D’, deşifreleme (decryption) işlemini ifade etmektedir. Burada dikkat edilmesi gereken husus ise, harflerin sayıya dönüştürülmesidir.

Sezar Şifreleme Yaklaşımı

Örnek olarak:

İngiliz alfabesi için
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
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Bu etiketleme sonucunda elde edilen sayılar formüllerde yerine konularak, her bir harfin farklı bir sayıya dönüşmesi sağlanır.

E i m z a 7 11 15 28 3
4 8 12 25 0 h l p c d

Sezar Şifreleme Yaklaşımı

- Sezar şifreleme metodu, simetrik, aynı zamanda da eşleşme (bijeksiyon) özelliği gösteren bir şifreleme metodudur.
- Şifreleme ve şifre çözme anahtarları aynıdır.
- Bu anahtarın alıcıya gizli bir yolla iletilmesi şarttır.
- Alıcıya anahtarın gönderilmesinde güvenilir bir yol bulunması veya seçilmesi unutulmamalıdır.

Sezar Açık Anahtar Şifreleme Yaklaşımı

Mesajın Şifrelenmesi (Encryption)	0<=N<29	Mesajın Şifrelenmesi (Decryption)
$E(M) = (M+N) \bmod 29 = C$		$D(C) = (C- N) \bmod 29 = M$

Örnek olarak:

«BİLİM» kelimesini şifreli biçimde gönderelim!!!

Fonksiyonumuz ise (M+1) mod 29

Şifrelenmiş metin: CJOJK

Deşifre etmek için: (C-1) mod 29

Polialfabetik Şifreleme Yaklaşımı

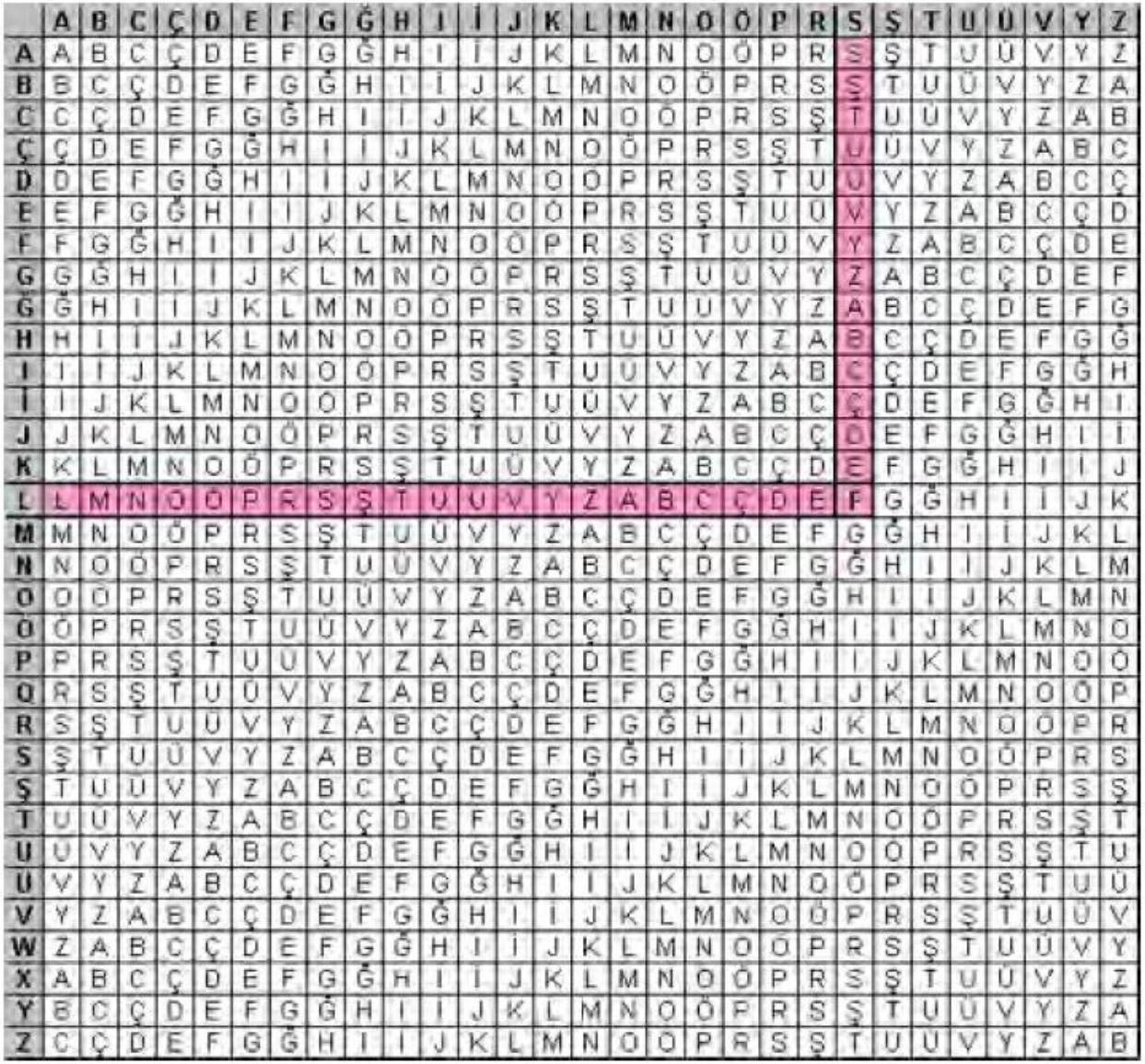
- Bu tip şifrelemede, mono alfabetik yöntemlerden farklı olarak bir harf değiştirilince her seferinde aynı harfe dönülmez.

- Bu işlem, “Vigenere Tablosu” olarak bilinen bir tablo ile gerçekleştirilir.

- Bu yaklaşımla bir mesajın şifrelenebilmesi için, bir anahtar kelimeye ihtiyaç vardır. Mesajın her bir karakteri sütun üzerinde, anahtar kelimede bulunan harf ise, satırdan bulunur. Satır ve sütunun kesiştiği noktadaki harf, şifrelenmiş mesajın harfi olarak belirlenir.

Polialfabetik Şifreleme Yaklaşımı

Vigenere Tablosu



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

Polialfabetik Şifreleme Yaklaşımı

Örnek olarak:

EİMZA KULLANMALIYIZ cümlesi şifrelenecek mesajımız olsun. “HEMEN” kelimesini ise, anahtar olarak kullanalım.

Mesajın Şifrelenmesi (Encryption)

Mesaj	EİMZA	KULLA	NMALI	YIZ
Anahtar	HEMEN	HEMEN	HEMEN	HEM
Şifreli mesaj	LNBDN	ŞİAPN	ÜRMPV	GML

Polialfabetik Şifreleme Yaklaşımı

Örnek olarak:

Elde edilen şifrelenmiş mesajın şifrelerinin çözümü için, aynı anahtar "HEMEN" kullanılmalıdır.

Mesajın Şifrelenmesi (Decryption)

Şifreli mesaj	LNBDN	ŞİAPN	ÜRMPV	GML
Anahtar kelime	HEMEN	HEMEN	HEMEN	HEM
Açık mesaj	EİMZA	KULLA	NMALI	YIZ

Vernam (One-Time Pad) Şifreleme Yaklaşımı

- Bu yaklaşımda, rasgele üretilen tek bir kullanımlık karakter dizisiyle şifreleme işlemi gerçekleştirilir.
- Açık mesaj içinde yer alan her karakter, üretilen dizide karşısına gelen karakterlerle işleme sokularak, şifreli mesaj elde edilir.
- Mesajı çözmek için rasgele dizinin bilinmesi gereklidir.

Vernam (One-Time Pad) Şifreleme Yaklaşımı

Örnek olarak:

EİMZA KULLANMALIYIZ cümlesi şifrelenecek mesajımız olsun.

Mesajın Şifrelenmesi
(Encryption)

Mesaj	EİMZA	KULLANMALIYIZ
Rasgele dizi	HNMET	KSYROQAZWPGLU
Şifreli mesaj	LYBDT	VNJ.....

Vernam (One-Time Pad) Şifreleme Yaklaşımı

- Bu yöntemde güvenlik rasgele üretilen diziye bağlı olduğundan bu şifreleme sistemi, “mükemmel bir şifreleme yöntemi” olarak da bilinir.

- Burada mükemmeliği sağlayan husus, rasgele dizinin gerçekten rasgele olarak seçilmesi ve anahtar uzunluğu ile aynı olmasıdır.

DES (Data Encryption Standard) Algoritması

- Bu algoritma, 1977'de IBM tarafından geliştirilmiş ve daha sonra da standart olarak kabul edilmiştir.
- Bu algoritmanın anahtar uzunluğu 56 bittir.
- Günümüzde bu algoritmanın anahtar uzunluğu yeterli gibi görünse de, kısa sürede çözülebilmektedir.
- Aslında sorun sadece anahtar uzunluklarında olmayıp, fonksiyonların simetrik olmasının güvenliği önemli ölçüde tehdit etmesinden kaynaklanmaktadır.

Okuma Önerisi:
https://bilgisayarkavramlari.com/2008/03/13/des-veri-sifreleme-standardi-data-encryption-standard/

DES (Data Encryption Standard) Algoritması

- Bu şifreleme yaklaşımında, X verisi K anahtarıyla şifrelenerek, Y verisine dönüştürülür.
- Şifrelenmiş Y verisi, daha sonra alıcıya gönderilir. Y verisi, alıcı tarafından göndericiye gizli bir kanaldan gönderilmiş olan K anahtarı ile, ancak deşifre edilir.
- Tek yönlü fonksiyon özelliği gösteren algoritmalara, DES, bir örnek olarak verilebilir.

DES (Data Encryption Standard) Algoritması

- 64 bit blok şifreleme de yapılabilen bu algoritma da, şifreleme esnasında 16 farklı döngü kullanılır.

- Bu işlemlerde veri, anahtar ve önceki döngü ile karıştırılır ve bir permütasyon işlemine tabi tutularak anlaşılamayacak bir forma getirilmeye çalışılır.

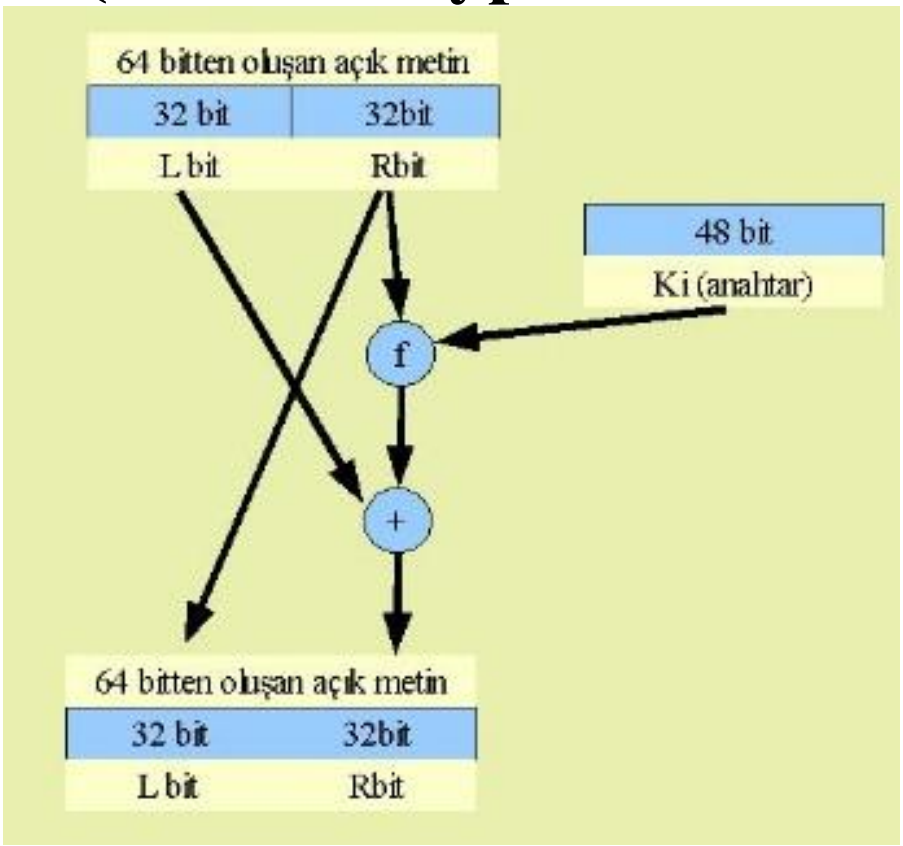
- Bir önceki döngünün çıkışı, bir sonraki döngüye giriş olarak uygulanır. Her bir döngüde, en sağdaki girişin 32 biti, çıkışın solundaki 32 bite kaydırılır.

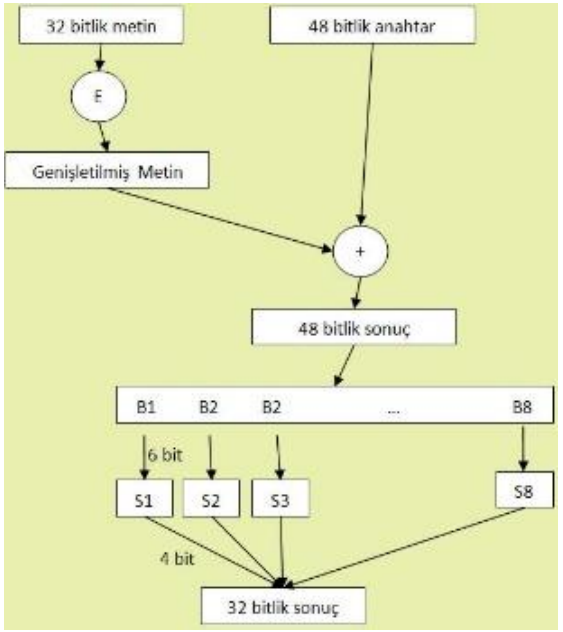
- Sonra, sağ ve sol bitler ve anahtar, bir fonksiyondan geçirilerek çalıştırılır. Her bir döngüde anahtar kaydırılır ve son bir permütasyon ile işlem tamamlanır.

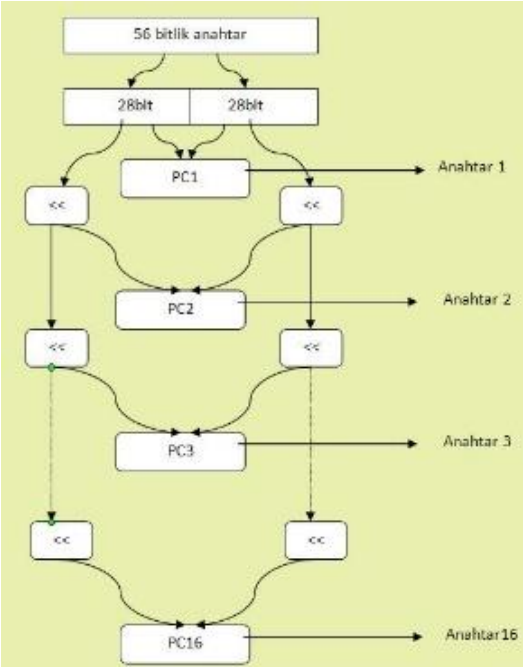
DES (Data Encryption Standard) Algoritması

- Bu yaklaşım, 1997 yılında İsrailli araştırmacılar tarafından kırılmıştır.
- Bu şifreleme yaklaşımının anahtar güvenliğini ve şifreleme güvenliğini arttırmak için 3 DES (Triple DES) geliştirilmiştir.
- 168 bit anahtar uzunluğuna sahip olan bu yaklaşım, günümüzde hala güvenli olarak kullananlar vardır.
- Bu algoritmanın hızlı olması ve lisanssız kullanımının serbest olması önemli özelliklerindendir.
- Daha çok bankacılık uygulamalarında ve AAA'da halen kullanılmakta olan şifreleme algoritmasıdır.

DES (Data Encryption Standard) Algoritması







https://bilgisayarkavramlari.com/2008/03/13/des-veri-sifreleme-standardi-data-encryption-standard/

RSA (Rivest, Shamir ve Adleman) Algoritması

- AAA'da birçok unsuru desteklemek ve güvenli bir ortam oluşturmak için asimetrik fonksiyonlar geliştirilmiştir.

- Bu gruba dahil fonksiyonlar, şifreleme ve deşifreleme yaparken, biri özel biri genel olmak üzere iki anahtar parametrelerini kullanırlar.

- Tasarımcılarının isimlerinin baş harflerinden oluşan RSA (**R**ivest, **S**hamir, **A**dleman) algoritması, asimetrik fonksiyonlara verilebilecek en iyi örnektir.

RSA (Rivest, Shamir ve Adleman) Algoritması

- RSA algoritması, bijeksiyon fonksiyon özelliği gösterir. Bu algoritmada bir özel ve birde açık olmak üzere bir anahtar çifti vardır. Açık (genel) anahtar herkese dağıtılır, özel anahtar ise, sadece kişiye özeldir ve o kişiden başka kimsede bulunmaz.

- X verisi alıcının genel anahtarıyla şifrelenerek Y verisine dönüştürülüp, alıcıya gönderilir. Y verisi, ancak alıcının özel anahtarı kullanılarak X verisine dönüştürülür. Burada gönderici bile, mesajı şifreledikten sonra açamaz. Şifrelenmiş veriyi anlamlı bir bilgiye çevirebilecek tek parametrenin alıcının özel anahtarı olması, bu algoritmanın güvenilirliğini arttırmaktadır.

- Bu şifreleme yaklaşımında, N = p.q olduğunu kabul edelim. Burada p ve q yüksek basamaklı asal sayılar olsun.

RSA (Rivest, Shamir ve Adleman) Algoritması

- Şifreleme için:

$$C = M^e \bmod N$$

- Şifrelenmiş mesajı çözmek:

$$M = C^d \bmod N$$

Bu formüllerde, (n,e) açık anahtarı, (d) ise özel anahtarı ifade etmektedir.

Okuma Önerisi:
https://bilgisayarkavramlari.com/2008/03/19/rsa/

RSA (Rivest, Shamir ve Adleman) Algoritması

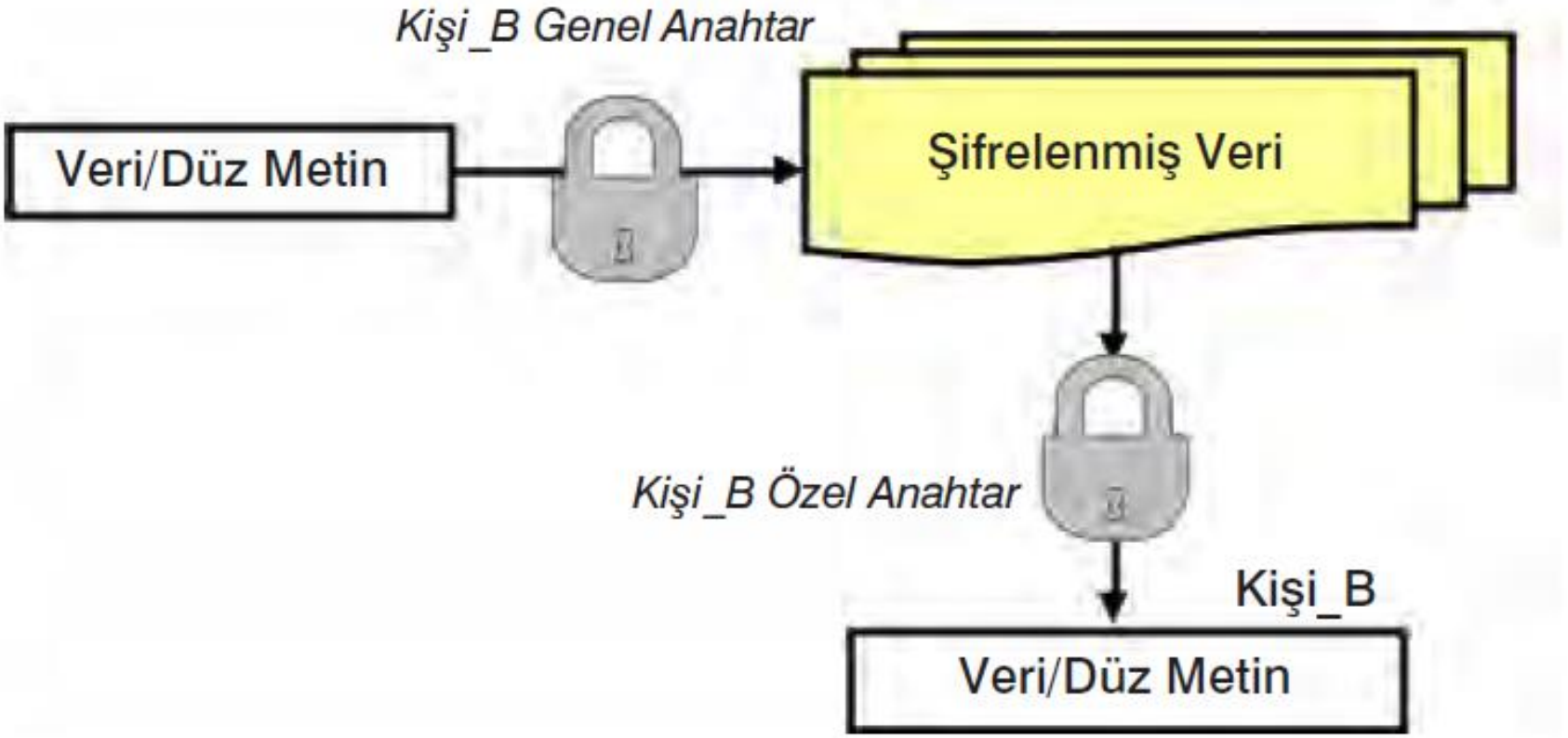
İki tarafın birbirleriyle haberleşebilmesi için Kişi_A ve Kişi_B'nin açık anahtarları herkese dağıtılır. Kişi_A, Kişi_B'ye bir mesaj göndereceği zaman, Kişi_B'nin açık anahtarı ile göndereceği bilgileri şifreler ve Kişi_B'ye gönderir. Şifrelenmiş veriyi alan Kişi_B ise, şifrelenmiş mesajı anlamlı bilgiye çevirebilecek tek parametre olan özel anahtara sahip olduğu için, bu anahtarını kullanarak veri veya düzmetini şifrelenmiş veriden ayrıştırabilir.

Açık ve özel anahtar örnek:
http://phpseclib.sourceforge.net/rsa/examples.html

RSA (Rivest, Shamir ve Adleman) Algoritması

RSA'da çok büyük asal sayıları üretmenin kolaylığına karşın, büyük sayıların asal bileşenlerinin bulunmasının zor olması prensibine göre işlemler yapılır. Matematikçilerin tamsayıları asal bileşenlerine ayırmanın hızlı bir yolunu henüz bulamamış olmaları, bu prensibin hala geçerli olduğunu göstermektedir. RSA ve benzeri algoritmalar, asal sayılarla yüksek çarpanlı matematik işlemleriyle gerçekleştirildiklerinden, bilgisayar uygulamalarında problemlerle karşılaşılması olasıdır. Bu işlemler gerçekleştirilirken, üretilen veriler karakter katarları şeklinde bilgisayar hafızasının elverdiği kadar saklanabilmektedir. Bunun için aritmetiksel işlemleri yeniden tanımlamak, yeniden yapılandırmak gerekebilir. Tüm bu zorluklara rağmen, RSA, açık algoritma mantığıyla çalıştığı, ve yüksek güvenlik sunduğu için, en çok tercih edilen asimetrik algoritmadır.

RSA (Rivest, Shamir ve Adleman) Algoritması



RSA Algoritmasıyla Şifreleme ve Şifre Çözme

Neden Asal Sayılar ve ne kadar büyükler

Okuma Önerisi:

https://www.matematikciler.com/asal-sayilar-ve-sifreleme-kriptoloji/
https://www.matematiksel.org/asal-sayilar-ve-sifreleme/
https://dergipark.org.tr/tr/download/article-file/388844

AES Algoritması

- Gelişen teknik ve teknolojiler, saldırıların boyut değiştirmesi, şifreleme algoritmalarına yapılan saldırıların artması, kullanılan algoritmaların saldırılara karşı dayanıklığının zayıflaması, araştırmacıları yeni algoritmalar geliştirmeye yöneltmiştir.

- AES ise son yıllarda kullanılan en önemli algoritmadır.

- AES'in geliştirilmesinin temelinde ise DES şifreleme algoritmasının saldırılara karşı dayanıksız olması vardır.

AES Algoritması

- 1997'de Joan Daemen ve Vincent Rijmen tarafından geliştirilmiş128, 192, 256-bitlik anahtar uzunluğu seçeneklerine sahip olan Rijndael algoritması, daha önceki sayfalarda da vurgulandığı gibi GelişmişŞifreleme Standardı (AES) ismiyle veri şifreleme standardı olarak belirlenmiştir.

- 1997'den beri ise farklı anahtar uzunlukları tercih edilen AES, günümüzde hala güvenilirliğini korumakta ve bilişim dünyasında güvenlik için kullanılmaktadır.

AES Algoritması

- AES algoritmasında, sahip olduğu anahtarlara göre farklı sayıda döngüsel işlem yapılır. AES 128-bitlik düz metni şifrelerken veya şifrelenmişmetni çözerken de aynı anahtarı kullanır. Bu döngüsel işlemin artmasıyla veri daha çok güvenilir hale gelir. Fakat, aynı zamanda yapılacak olan döngüsel işlemlerin de artmasıyla hem işlem sayısı hem de bellek alanı artar.

- Bu algoritmada; AES-128 AES-192 AES-256 gibi veri blokları, 4,6,8 gibi kelime uzunluğu, 10,12,14 gibi tur sayısı uygulanabilmektedir.

Özetleme (Hashing) Algoritmaları

- Farklı uzunluklarda mesaj, doküman veya yazıyı işleyerek, sabit uzunlukta veri oluşturma işlemine, **özet veya özetleme** denir.

- Elde edilen özet bilginin, mesaj, doküman veya yazıyı temsil edebilecek bir formda olması beklenir. Bundan dolayı, elde edilen özet değeri mümkün olduğunca tekil olması veya benzerinin olmaması istenilir.

- Bu işlemde, bir özetleme (hash) fonksiyonu kullanılır ve bir grup veriden veya mesajdan sabit uzunlukta bir dizi üretilir.

- Üretilen bu dizi, o mesajın, dokümanın veya yazının bütünlüğünün test edilebilmesi için kullanılan bir imza niteliğindedir. Bu işlemleri gerçekleştiren algoritmalara, özetleme algoritmaları veya fonksiyonları denir.

Özetleme (Hashing) Algoritmaları

Bir özetleme fonksiyonunun temel özellikleri:

- ✓ Uzunlukları farklı olan verileri, sabit uzunluklu bir çıktıya dönüştürmelidir.
- ✓ Özet değeri kolay hesaplanabilmelidir.
- ✓ Özet değerinden mesajı elde etmek zor olmalıdır.
- ✓ Farklı mesaj veya dokümanlardan aynı özet değerinin üretilmemesi gereklidir.
- ✓ Elde edilecek özet değeri tekil (unique) olmalıdır.
- ✓ Aynı özet değerini üretecek iki farklı mesajı bulmak ise oldukça zor olmalıdır.

Özetleme (Hashing) Algoritmaları

Özellikler:

- Pratikte özetleme fonksiyonları, **şifre doğrulama**, bütünlük kontrolü, **e-imza** ve güvenli e-posta uygulamalarında kullanılmaktadır.

- Genellikle veri bütünlüğünü garanti etmesi, hızlı olması, sabit uzunlukta çıktı vermesi, açık anahtar algoritmalarından daha iyi olması, dosya boyutunun alınan özeti etkilememesi ve yüksek performanslı bir haberleşme sağlaması bu yaklaşımın üstünlükleridir.

Özetleme (Hashing) Algoritmaları

Farklı güvenlik seviyelerinde kullanılan bazı özetleme algoritmaları:

MD (Message Digest) serisi,
SHA (Secure Hash Algorithm) serisi,
RIPE-MD-160 (RACE Integrity Primitives Evaluation).

Özetleme (Hashing) Algoritmaları

MD serisi

- Ron Rivest tarafından geliştirilmiştir.
- Son yıllara en çok kullanılan özetleme algoritmalarındandır.
- 128-bit özetleme sağlar.
- Bu seride MD2 en yavaşı iken, MD4 ise en hızlılarıdır. MD5, MD4'e göre daha kapsamlı geliştirildiğinden, hızı nispeten düşüktür. Tüm bu algoritmaların herkese açık olması önemli üstünlükleridir.
- MD5'in çarpışma saldırılarına karşı zayıf olduğunun keşfedilmesinden sonra bilimadamları, MD5 yerine SHA-1 veya RIPEMD-160 gibi alternatiflerin kullanılmasını tavsiye etmektedirler.

Özetleme (Hashing) Algoritmaları

SHA-1 (Güvenli Özetleme algoritması-Secure Hashing Algorithm)

- İlk olarak NSA (Ulusal Güvenlik Ajansı-*National Security Agency*) tarafından geliştirilmiş ve NIST'in desteğiyle, 1993 yılında ABD'de standart olarak kabul edilmiştir.

- Bu algoritma, MD serisi algoritmalardan daha uzun özet bit üretebilmektedir. 160-bit uzunluğunda üretilen bir dizi için gerekli süre MD5 algoritmasından yaklaşık olarak %25 oranında daha yavaş olsa da, kullanılması tavsiye edilen bir algoritmadır.

Özetleme (Hashing) Algoritmaları

SHA-1 (Güvenli Özetleme algoritması-Secure Hashing Algorithm)

- Günümüzde karışıklığı önlemek amacıyla, ilk sürüm, SHA-0 olarak adlandırılır. SHA-0 ve SHA-1, en fazla 264 uzunlukta mesajlardan 160-bitlik özet değeri üretir.

- NIST, 2001 yılında SHA'nın 256, 349 ve 512 bit versiyonlarıyla SHA-256, SHA-349 ve SHA-512 yapılabildiğini duyurmuştur. Bunun güncel bir versiyonu olan SHA-2 ise en çok kullanılan versiyonudur.

Özetleme (Hashing) Algoritmaları

Okuma Önerisi:

https://www.vargonen.com/blog/sha-secure-hashing-algoritmasi-nedir/

https://wmaraci.com/md5-sha1-sifre-olusturucu (md5 ve sha şifreleme örnek)

https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/08/md5-algoritmas%C4%B1

https://www.siberportal.org/blue-team/cryptography/basics-of-hashing-algorithms-and-applications/

Özetleme (Hashing) Algoritmaları

RIPE-MD-160 (RACE Integrity Primitives Evaluation Message Digest) algoritması, Avrupa Birliğinde kullanılan bir algoritmadır.

- Farklı uzunluktaki dosya veya veriler için 160 bitlik sabit uzunlukta dizi üretmesi ve diğer şifreleme yaklaşımlarından daha hızlı olması, bilinen üstünlükleridir. Sadece bütünlüğü sağlaması ise, en önemli dezavantajı olarak bilinmektedir.

- RIPE-MD-160'ın gelecek yıllarda güvenilir olacağı öngürülmekte ise de, bu algoritmanın bazı ataklara karşı zayıf olduğu birkaç farklı çalışmada vurgulanmıştır. Algoritmanın tasarımı MD4, MD5 ve RIPEMD'nin zayıf yönlerinin değerlendirilmesi prensibine dayanmaktadır. İki farklı ve paralel hesaplama işleminin sonucunun, her bir sıkıştırma işlemi sonunda birleştirilmesi, bu fonksiyonun ayırt edici özelliğidir. Diğer özetleme algoritmaları gibi, 32 bit işlemcilerde en iyi performansı verecek şekilde ayarlanmıştır. Bununla beraber, RIPE-MD'nin 258 bitlik ve 320 bitlik sürümleri de mevcuttur

Özetleme (Hashing) Algoritmaları

- **MAC** (Mesaj Onaylama Kodları-Message Authentication Codes)

- Diğer bir özetleme algoritmasıdır.

- Diğerlerinden farkı, bir MAC oluşturma veya doğrulama için, yalnız bir anahtara ihtiyaç duyulmasıdır. Bu özelliğin, özetlerin iletişim anında ele geçirilemeyeceğini doğrulama için önemli bir yaklaşım olduğunu savunanlar vardır.

- HMAC (RFC 2104) ve SHA-1 temelli NMAC bunlara örnek olarak verilebilir.

Özetleme (Hashing) Algoritmaları

- Anahtarlı özetlemeli mesaj doğrulama kodları (HMAC), bir anahtara dayalı ve tek yönlü çalışan bir özetleme yöntemidir ve hem veri bütünlüğünü hem de veri kaynağının doğrulanmasını sağlar.

- HMAC'lar incelenen özetleme fonksiyonları ile aynı özellikleri taşır. Bu özetleme fonksiyonlarından birini kullanır, ancak ilave olarak, bir gizli anahtar kullanılır. HMAC'lar, veri alışverişinde kullanıldığı gibi, herhangi bir şahsa alt dosyalarının değiştirilip değiştirilmediğini kontrol etmek amacıyla da kullanılabilir.

Özetleme (Hashing) Algoritmaları

Özetleme Algoritmalarının Karşılaştırması:

Algoritma	Döngü no	Mbit/s	MB/s
MD4	241	191,2	23,90
MD5	337	136,7	17,09
RIPEMD	480	96,0	12,00
RIPEMD-128	592	77,8	9,73
SHA-1	837	55,1	6,88
RIPEMD-160	1013	45,5	5,68

Bu algoritmalar, güvenilirlik açısından karşılaştırıldığında, en güvenli olanının RIPEMD-160 olduğu ve sıralamayı SHA-1 algoritmasının takip ettiği belirtilmiştir.Daha önce de belirtildiği gibi MD5, zayıflıklarından dolayı güvenilirliği şüpheli bulunmuştur.

Sorular

Bir sonraki ders Siber Güvenliğin Temelleri – III (Şifre Bilim (Kriptografi), Özetleme(Hashing) Algoritmaları, Standartlar, Steganografi, Protokoller, Kuantum Şifreleme, E-imza (dijital imza) konusuna giriş yapılacak.