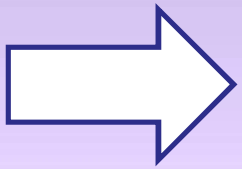
MARMARA ÜNİVERSİTESİ TEKNİK BİLİMLER MESLEK YÜKSEK OKULU

BİLGİSAYAR TEKNOLOJİSİ VE PROGRAMLAMA

KRİPTOLOJİ VE ŞİFRELEME ALGORİTMALARI

Hazırlayan : Anıl Yıldırım

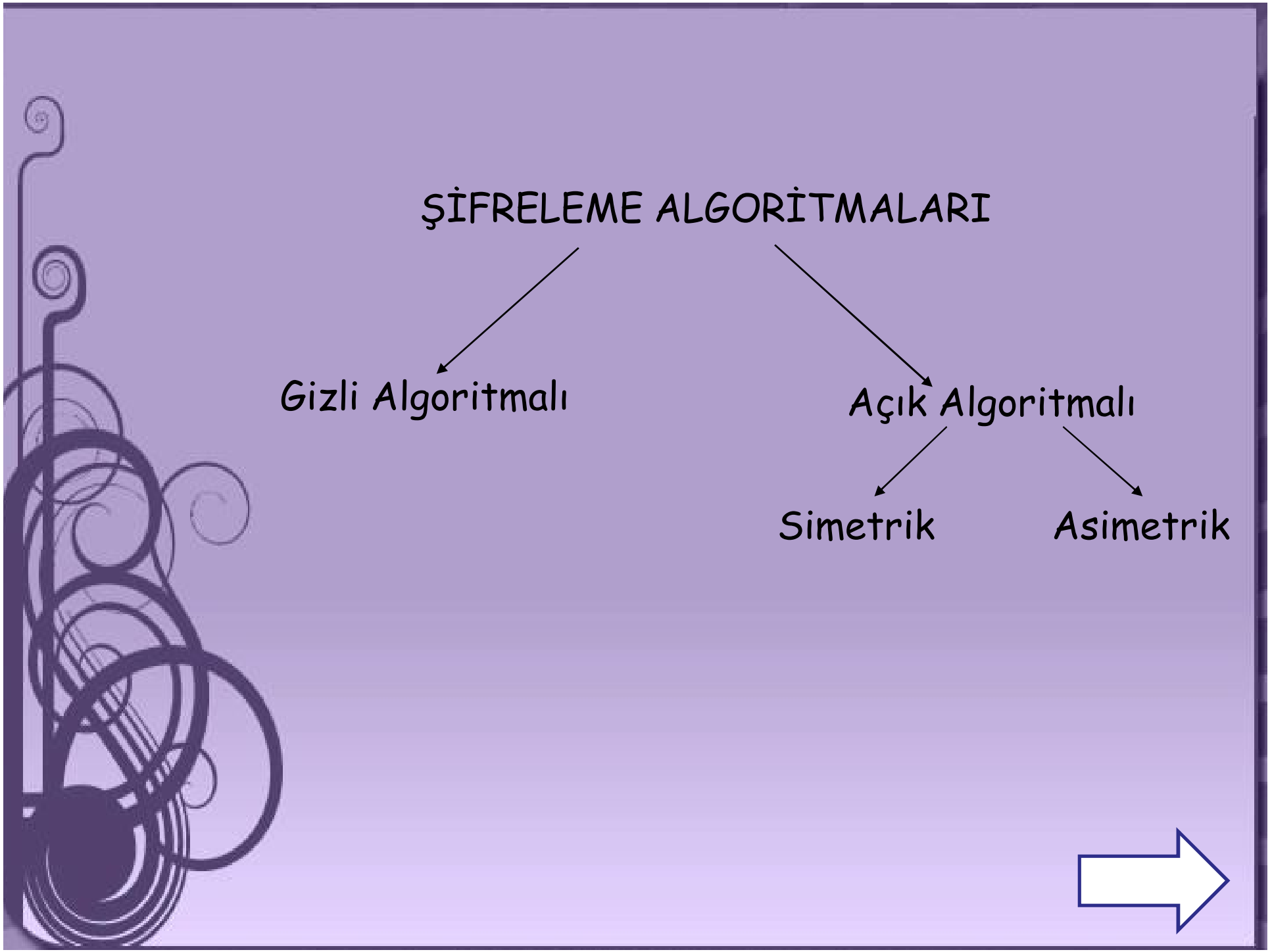
460108028



KRİPTOLOJİ

- Şifre bilimidir.Çeşitli iletilerin yazıların belli bir sisteme göre şifrelenmesi bu mesajın güvenli bir ortamda alıcıya iletilmesidir.Şifreleme ise şifre verme işlemidir

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


ŞİFRELEME ALGORİTMALARI
Gizli Algoritmalı
Açık Algoritmalı
Simetrik
Asimetrik

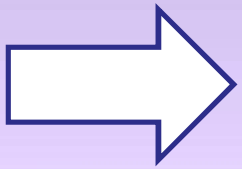
Gizli Algoritmalı

En eski şifreleme yöntemidir.Bu algoritma sadece alıcı ve gönderici arasındaki bilinen ve birbirlerini tersi olan gizli iki algoritmaya dayanır.Bilgi gönderilmeden adımlar takip edilerek şifrelenir.Bu adımlar sondan başa doğru takip edilir.

Fakat bu algoritmanın kırılması kolaydır.Günümüzde hiç kullanılmaz.

Örneğin : Anahtar(3)

Şifre Tablosu: "ABCDEFGĞHIİJKLMNOÖPRSŞTUÜVYZ"
Metin : "Algoritma Dersi"
Şifreli Metin : "Doırtlvöd Gğtul"

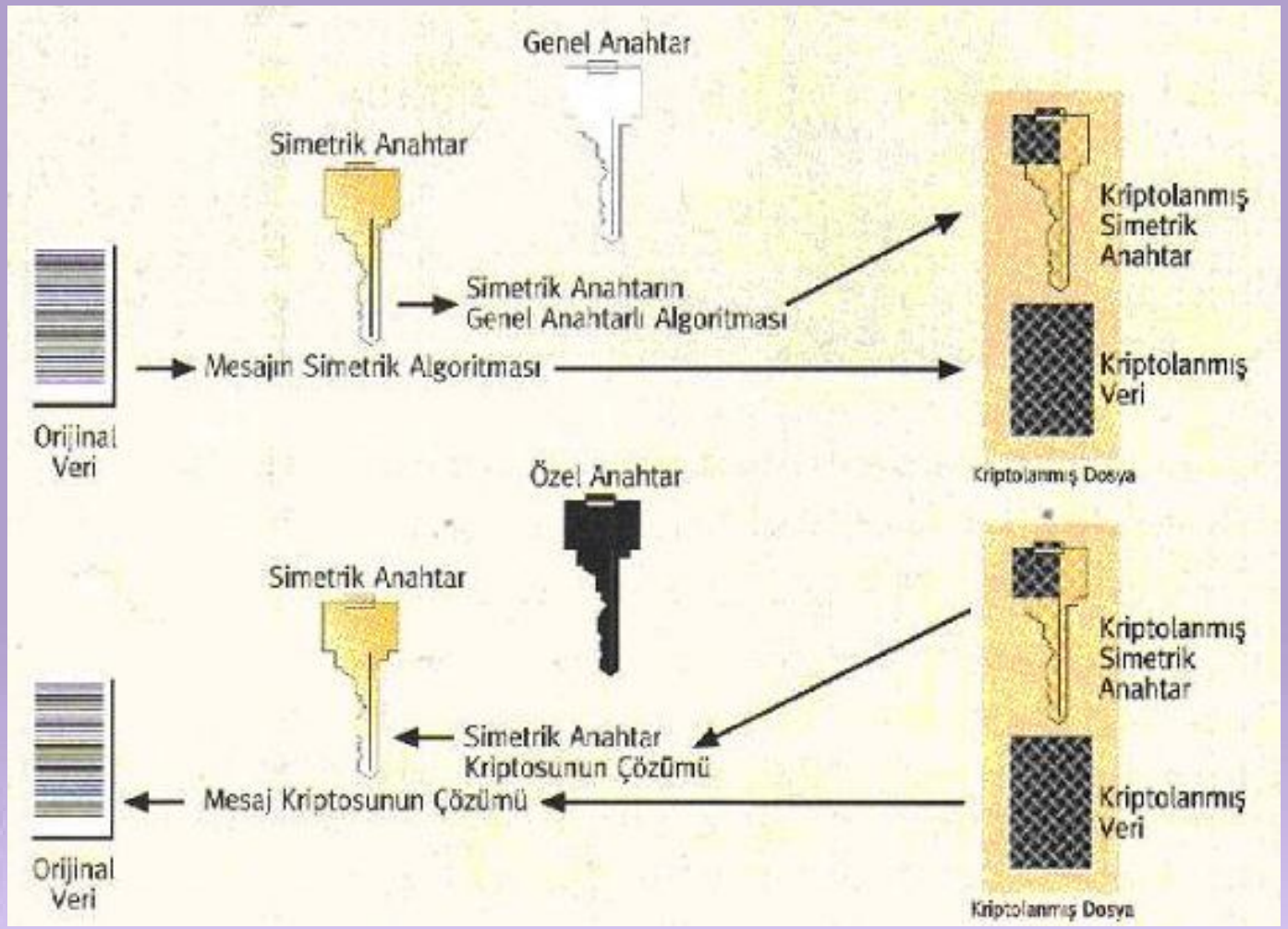


Örnekte gönderilen metin bu algoritma yöntemine göre ilk önce anahtar(n)'in kaç olduğu belirtildikten sonra Alfabedeki tüm harflerden n kadar sonraki yazılarak şifreleme yapılır

Açık Algoritmalı

Bir anahtar kullanan ve herkes tarafından bilinen bir algoritmayı şifrelenerek iletilir. Alıcı ise şifrelemeyi aynı anda farklı olan bir anahtar kullanarak yine herkes tarafından bilinen bir algoritma şifreli metni çözer.
Bilginin gizliliği anahtar şifrelenmeyle sağlanır.Bu şifrelenmeye anahtara dayalı şifrelemede denir.
Anahtar şifreleme yöntemine göre simetrik ve asimetrik olarak ikiye ayrılır.

Simetrik Ve Genel Anahtar Algoritmasının kombinasyonu



Simetrik

Şifreleme aynı anahtarı kullanarak çalışan algoritmalardır.Gizli anahtar algoritması olarak da adlandırılır.
Örn: Osman'ın Aliye göndereceği bir mesaj'ı kendi anahtarı ile şifreler.Fakat Ali bu mesajı Osman'ın anahtarını bilerek çözer.Kısacası şifreleme ve şifreyi çözmede aynı anahtarın kullanılmasıdır.Ancak şifrenin deşifre olması aynı anahtar olduğu için biraz tehlikelidir.

Asimetrik

Açık anahtarlı şifreleme olarak da adlandırılır.Bu algoritmada şifreleme ve çözme anahtarları farklıdır.
Anahtarlardan birinin şifrelendiği zaman sadece diğeri çözebilir.Anahtarlardan birine gizli diğerine açık anahtarlanma denilebilir.En büyük örneği RSA dır.
Örnek:
Mesaj : (C)
Şifreleme : (a1)
Çözülmesi : (a2)
Eğer a1 a2'ye eşitse ise kriptosistem simetriktir.Fakat sistemin daha güvenli olması için a1 a2 eşit olmaması gerekir buna da asimetrik denilmektedir.