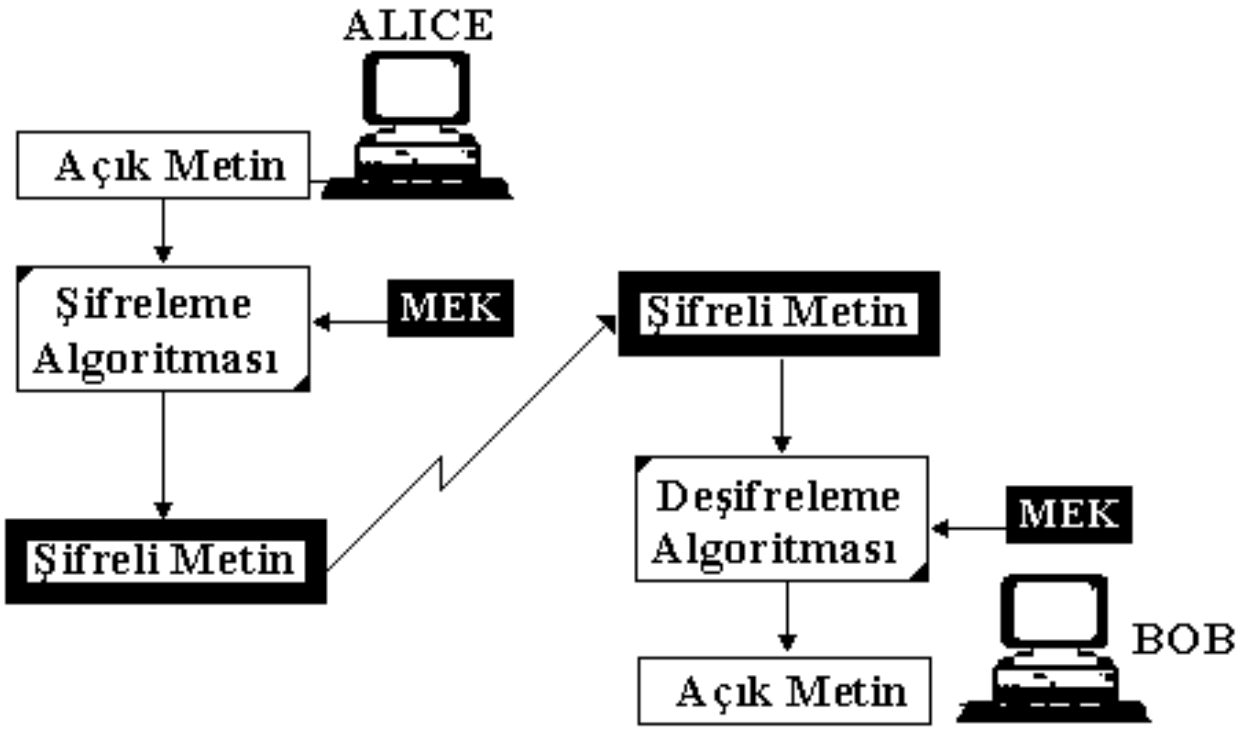
Bilgi Güvenliği ve Kriptografi

Simetrik Anahtar Kriptosistemler

- Simetrik kriptosistemlerde, şifreleme anahtarının deşifreleme anahtarından üretilmesi oldukça kolaydır.
- Çoğu simetrik algoritmalarda, şifreleme ve deşifreleme için kullanılan anahtar aynıdır.
- Alıcı ve göndericinin güvenli bir şekilde haberleşmesi için, öncelikle bir anahtar üzerinde görüş birliğine varmaları gerekir.
- Bu algoritmaların güvenliği anahtara bağlı olduğundan anahtar gizli tutulmalıdır.

Simetrik Anahtar Kriptosistemler

- MEK (Message Encryption Key), şifreleme anahtarıdır.



Simetrik Anahtar Kriptosistemler

- Simetrik anahtar kriptosistemindeki haberleşme protokolünün adımları aşağıda verilmiştir.

1. Alice ve Bob bir kriptosistem üzerinde görüş birliğine varır.
2. Alice ve Bob bir anahtar üzerinde görüş birliğine varır. (anahtar paylaşımı)
3. Alice mesajını, şifreleme algoritmasını ve anahtarı kullanarak şifreler. Bu işlem sonucunda şifreli metin oluşur.
4. Alice şifreli mesajı Bob'a gönderir.
5. Bob şifreli mesajı aynı algoritma ve anahtarı kullanarak deşifre eder.

Simetrik Anahtar Kriptosistemler

- Alice ve Bob arasında bulunan bir kişi, örneğin Eve bu haberleşmeyi dinleyebilir.
- Eve, birinci ve ikinci adımlardaki haberleşmeyi dinlerse, kullanılan algoritmayı ve anahtarı öğrenir. Bunun sonucunda, dördüncü adımda iletilen tüm şifreli mesajları deşifre edip okuyabilir.
- Bu nedenle kriptografide *anahtar yönetimi* (key management) çok önemlidir.
- Simetrik bir algoritmada, Alice ve Bob ikinci adımı gizli olarak gerçekleştirmelidir. Anahtar haberleşme öncesinde, haberleşme sırasında, ve haberleşme sonrasında gizli kalmalıdır.

Simetrik Anahtar Kriptosistemler

- **Ceasar Şifresi:** Adını Julious Ceasar'dan alan basit şifreleme yöntemidir. Burada her harf, belirli bir kaydırma dönüşümü kullanılarak elde edilen başka bir harf ile değiştirilir. İki karakter kümesi yada alfabesi, açık metin ve şifreli metin için oluşturulmuştur.

- **Açık metin alfabesi :**
  ABCÇDEFGĞHIİJKLMNOÖPRSŞTUÜVYZ
- **Şifreli metin alfabesi :**
  EFGĞHIİJKLMNOÖPRSŞTUÜVYZABCÇD

- Mesajın şifrelenmesi sırasında açık metindeki A, E ile, E ise I ile değiştirilir. Bu durumda
- "DAİMA GÜVENLİ HABERLEŞİN" açık metni şifrelendiğinde, "HENRE JBCISPN LEFIÜPIYNS" şifreli metni oluşur.

Simetrik Anahtar Kriptosistemler

- Ceasar şifresinden sonraki gelişme, kullanılan her sembolün, bir başka sembole haritalanmasıdır. Bu sisteme *monoalfabetik* (monoalphabetic) şifreleme adı verilir. Şifreleme anahtarı, tüm Türkçe alfabesine karşılık gelen 29 harften oluşan dizidir. Bu sistem $29!=8.8x10^{26}$ mümkün anahtar değeri olduğu için güvenli görülebilir.

- Bu olasılıkların sırasıyla denenmesi istenen bir yaklaşım değildir. Çünkü tüm olasılıkları denemek, bilgisayar için çok uzun zaman alabilecek bir işlemdir.

Simetrik Anahtar Kriptosistemler

- Bununla birlikte, küçük bir şifreli mesaj parçası ile şifreyi çözmek mümkündür.

- Bu amaçla dilin istatistiksel özellikleri kullanılır. Dilde en çok kullanılan harfler, ikili ve üçlü harf birleşimleri göz önünde bulundurularak şifrenin kırılmasına çalışılır. Bu amaçla, öncelikle şifreli mesajdaki harflerin frekansları hesaplanmalıdır. Bu frekanslar dilin özelliklerine göre yorumlanır.

- Örneğin, Türkçe'de en sık kullanılan harfler a ve e'dir. Şifreli mesajda en sık rastlanan karakterlere bu harfler karşılık getirilir. Benzer şekilde devam edilerek şifre çözülür. Aynı yaklaşım, ikili ve üçlü harf birleşimleri için de kullanılır.

Simetrik Anahtar Kriptosistemler

- **Polybius Şifresi:** Bu şifreleme yöntemi, Yunanlı Polybius tarafından geliştirilmiştir. Kullanılan alfabe 5x5 boyutlu kare matris şeklinde tutulur. 29 harfi 25 pozisyona uyarlamak gerektiği için bazı harfler ihmal edilir yada birleştirilir.

- Genellikle İngilizce'de, U harfi dışarıda bırakılır ve V ile yer değiştirilir yada I ve J birleştirilerek tek bir pozisyon kaplar.

- Türkçe için kelimelerin anlam değişiklikleri göz önüne alınarak I-İ, O-Ö, U-Ü, C-Ç birleştirilebilir. Birleştirme sonucu oluşan matris aşağıda verilmiştir.

Simetrik Anahtar Kriptosistemler

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	Ğ	H	I
3	J	K	L	M	N
4	O	P	R	S	Ş
5	T	U	V	Y	Z

- Bu şifrelemede mesajdaki her harf iki sayıyla değiştirilir. Bu sayılar, açık metin harfinin matristeki pozisyonunun satır ve sütun değerleridir. Aynı mesaj şifrelendiğinde aşağıdaki şifreli mesaj elde edilir.

- **Açık metin** :DAIMA GUVENLI HABERLESIN
- **Şifreli metin :** 14 11 25 34 11 22 52 53 15 35 33 25 24 11 12 15 43 33 15 45 25 35

Simetrik Anahtar Kriptosistemler

- **Vigenere Şifresi:** Şifre çözmeyi daha zor hale getirmenin farklı bir yolu, polialfabetik şifreleme kullanmaktır. Bu yöntemin en çok bilinen ve basit olanlarından biri, Vigenere şifresidir. Yöntem, ilişkili monoalfabetik yerine koyma kurallar kümesini ve yerine koyma sırasını belirleyen, önceden düzenlenmiş bir anahtar değerini kullanır. Gösterilen Vigenere tablosu 29 Ceasar şifresinden oluşmaktadır

Vigenere tablosu

	A	**B**	**C**	**Ç**	**D**	**...**	**V**	**Y**	**Z**
A	A	B	C	Ç	D	...	V	Y	Z
B	B	C	Ç	D	E	...	Y	Z	A
C	C	Ç	D	E	F	...	Z	A	B
Ç	Ç	D	E	F	G	...	A	B	C
D	D	E	F	G	Ğ	...	B	C	Ç
:	:	:	:	:	:	:	:	:	:
V	V	Y	Z	A	B	...	T	U	Ü
Y	Y	Z	A	B	C	...	U	Ü	V
Z	Z	A	B	C	Ç	...	Ü	V	Y

Simetrik Anahtar Kriptosistemler

- Aslında bu şifre sistemi kullanım olarak oldukça basittir. Örneğin C anahtar harfi ve Y açık metin harfi verildiğinde, şifreli metin harfi, tabloda C satırının ve Y sütununun kesişimindeki harf olarak alınır. Kullanılan anahtar, tüm mesaj boyunca tekrarlanır. Çoğu durumda anahtar olarak tek bir kelime yerine, kelime grubu yada tüm bir cümle kullanılır. Aşağıda bir anahtar ve şifreleme örneği verilmiştir.

- **Anahtar : BİRZAMANLARSOĞUKBİRKIŞ**
- **Açık Metin : DAİMAGÜVENLİHABERLEŞİN**
- **Şifreli metin : EİCLAŞÜİPNEÇÜĞÜÖSÜÜFSH**

- Anahtar kelimenin karakterleri tablodaki satırlara, açık metninkiler ise sütunlara karşılık gelir.

Simetrik Anahtar Kriptosistemler

- Anlaşıldığı gibi, bu yöntemde aynı açık metin karakterlerine farklı şifre karakterleri karşılık gelecektir. Bu ise sistemin dayanıklılığını artırmaktadır.

- Benzer şekilde, şifreli metindeki bir karakter, açık metindeki farklı karakterleri ifade edebilir. Fakat, bu şifreli bilgiler de yeterli miktarda şifreli mesaj elde edildiğinde kolaylıkla çözülebilir. Burada önemli olan, anahtar uzunluğunun tahmin edilmesidir.

Simetrik Anahtar Kriptosistemler

- Bu tahmin yapıldıktan sonra, şifreli mesaj anahtar uzunluğuna eşit uzunluktaki satırlara bölünür. Eğer tahmin doğru ise, tüm sütunlardaki şifreli mesajlar aynı monoalfabetik şifreleyici ile şifrelenmiş olur.

- Bu durumda sütunlardaki frekans dağılımı, kullanılan dilin istatistik değerleri ile aynı olmalıdır. Tahmin edilen değer yanlış ise, başka bir sayı denenir. Bir uyum elde edildiğinde, her sütün ayrı bir monoalfabetik şifreleyici gibi çözülebilir.

Simetrik Anahtar Kriptosistemler

- **Çit (Picket Fence) Şifresi:** Yer değişme şifreleme yöntemleri için en basit ve hızlı yöntem, mesajda pozisyonları tek sayı olan harflerin çift sayı olanlardan ayrılması ve sonucun iki karakter dizisi şeklinde oluşturulmasıdır. Yöntemi açıklamak amacıyla aşağıda bir şifreleme örneği verilmiştir.

- **Mesaj : DAİMA GÜVENLİ HABERLEŞİN**
- **Tek harfler :** D İ A G V N İ H B R E İ
- **Çift harfler :** A M Ü E L A E L Ş N
- Şifreli mesaj bu iki karakter dizisinin birleştirilmesi ile aşağıdaki gibi olacaktır.
- DİAGVNİHBREİAM ÜEL AELŞN

- Mesajı deşifrelemek için alıcı, toplam harf ve boşluk sayısını hesaplayıp şifreli metni ikiye bölmelidir. Toplam sayı tek ise, büyük olan dizi üst küme olarak alınır.

Simetrik Anahtar Kriptosistemler

- **Sütun (Columnar) Şifreleme:** Başka bir yer değişme şifreleme yöntemi Polybius şifresine oldukça benzerdir. Açık metni karıştırmak için yatay yönde satırlar, düşey yönde sütunlar kullanılır. Yöntemde açık metin satırlara yazılır, şifreli metin ise sütunlardan okunarak elde edilir. "DAİMA GÜVENLİ HABERLEŞİN" mesajı kelimeler arasındaki boşluklar ihmal edilerek satırlar boyunca yazılır. Boş kalan yerlere keyfi harfler eklenir. Şifreli metin düşey olarak sütunlardan okunarak elde edilir. Oluşturulan matris ve şifreli metin aşağıdaki gibidir.

	1	2	3	4	5
1	D	A	İ	M	A
2	G	Ü	V	E	N
3	L	İ	H	A	B
4	E	R	L	E	Ş
5	İ	N	Z	E	T

DGLEİ AÜİRN İVHLZ MEAEE ANBŞT

Simetrik Anahtar Kriptosistemler

- Tekil Olmayan Matrisler Yardımı ile Şifreleme

Bu şifreleme yönteminde açık metin karakterlerine farklı sayılar karşılık getirilir. Boşluk karakteri 0 ile ifade edilir. Bu sayılar M olarak adlandırılan 3 satırlık bir matris şeklinde düzenlenir. Matriste boş kalan pozisyonlar 0'larla doldurulur. Daha sonra M matrisi determinantı ± 1 ($|\det A| = \pm 1$) olan A matrisi ile çarpılarak B matrisi üretilir. B matrisi şifreli metni oluşturmaktadır [16].

$$B = A * M$$

Deşifreleme için A matrisinin tersi hesaplanır ve B şifreli metni ile çarpılır. Sonuçta M orijinal metni elde edilir.

$$A^{-1} * B = M$$

Simetrik Anahtar Kriptosistemler

d	a	i	m	a		g	ü	v	e	n	l	i		h	a	b	e	r	l	e	ş	i	n
12	5	9	1	5	0	10	18	21	15	3	4	9	0	7	5	11	15	23	4	15	19	9	3

Bu sayılar 3x8'lik bir matrise dönüştürülerek |det A|=1 olan A matrisi ile aşağıdaki gibi çarpılır ve B matrisi şifreli mesaj olarak elde edilir.

$$\begin{vmatrix} 3 & 2 & 2 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{vmatrix} . \begin{vmatrix} 12 & 5 & 9 & 1 & 5 & 0 & 10 & 18 \\ 21 & 15 & 3 & 4 & 9 & 0 & 7 & 5 \\ 11 & 15 & 23 & 4 & 15 & 19 & 9 & 3 \end{vmatrix} = \begin{vmatrix} 100 & 75 & 79 & 19 & 63 & 38 & 62 & 70 \\ 21 & 15 & 3 & 4 & 9 & 0 & 7 & 5 \\ 23 & 20 & 32 & 5 & 20 & 19 & 19 & 21 \end{vmatrix}$$

A * M = B

Mesajın deşifrelenmesi için öncelikle A matrisinin tersi bulunmalıdır.

$$A^{-1} = \begin{vmatrix} 1 & -2 & -2 \\ 0 & 1 & 0 \\ -1 & 2 & 3 \end{vmatrix}$$

Bu A^{-1} matrisi ile B matrisi çarpıldığında orijinal M matrisi elde edilir.