CENG 434 Kriptoloji – 1. ve 2. Ders

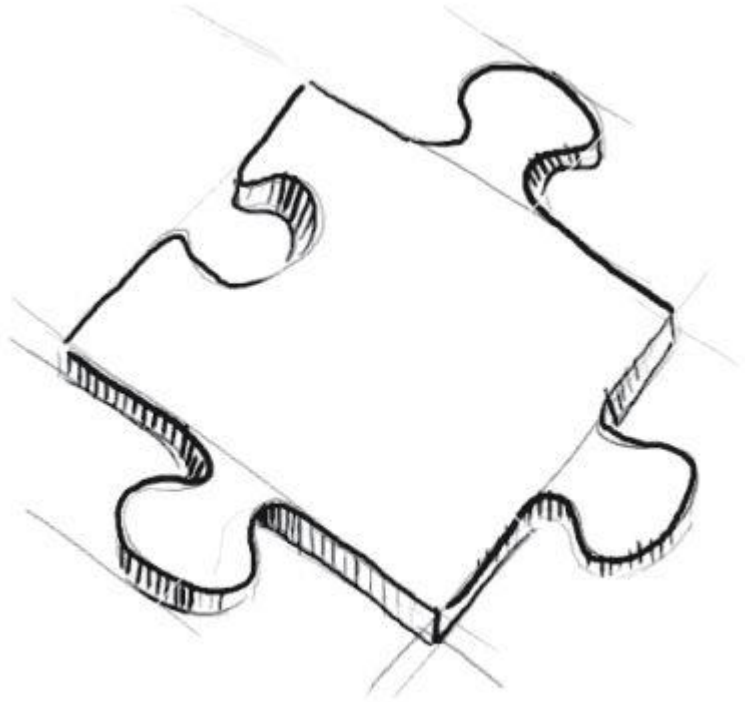
Alper UĞUR

CENG 507 :
KRİPTOGRAFİK ALGORİTMALAR VE SİSTEMLER

CENG 434:
KRİPTOLOJİ

Giriş

- Alper UĞUR
- Kriptoloji Dersi Hakkında
  - Kapsam
  - İşleniş
  - Değerlendirme
- İlk ders: Genel Kavramlar

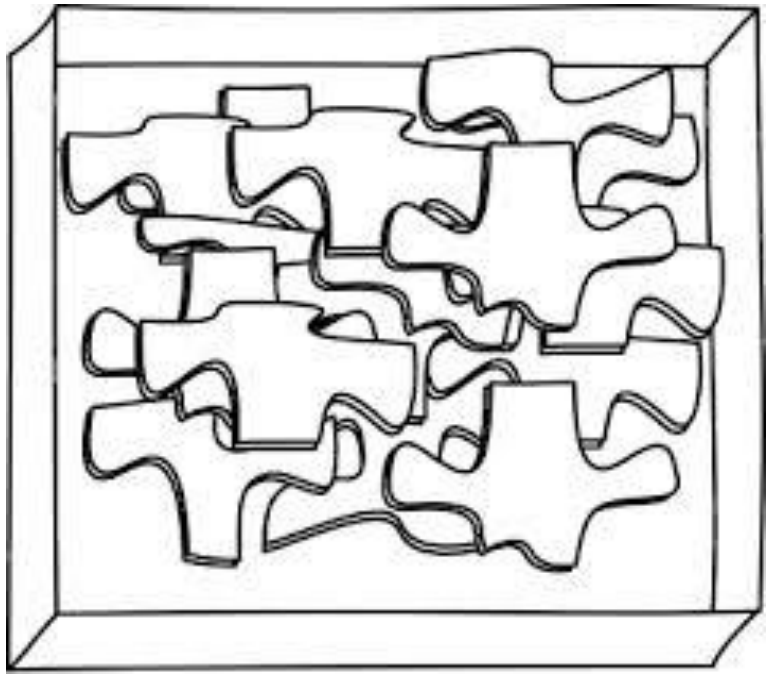


İçerik

- Temel Kavramlar
- Kriptolojide Matematiksel Altyapı
- Geleneksel Şifreleme Yöntemleri
- Modern Kriptografi
- Kimlik Doğrulama
- Anahtar Yönetimi
- Özetleme Fonksiyonları
- Sayısal İmzalar
- Ağ ve Yazılım Güvenliği Politikaları

Ders İşlenişi Hakkında

- PAÜ EDS Eğitim Destek Sistemi Ders Sayfası
  - Duyurular
  - Ders Notları
  - Kaynaklar
  - Ödevler
- Dönem geneline yayılmış bir proje
- Durum takip çizelgesi



Değerlendirme

- % 30 Ara sınav
- % 45 Final
- % 25 Proje

- Vize %5 , Final %20 -> Proje = %50
- Proje: her ara sürüm: %2-5

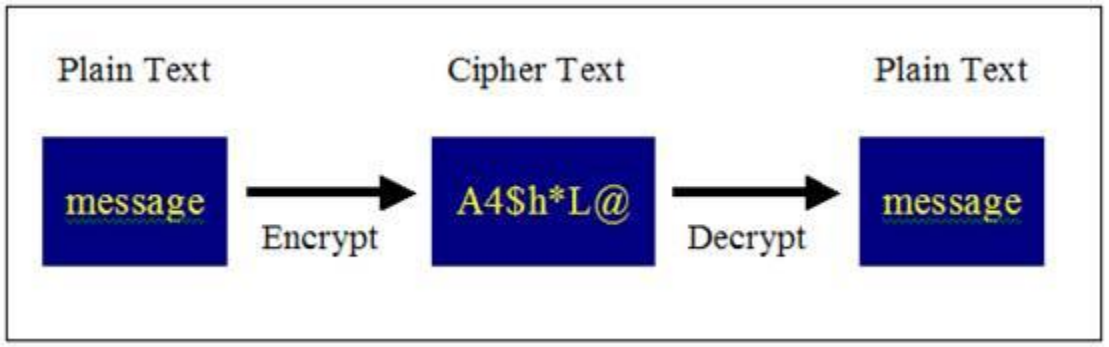
(örn: **4**x%2+**3**x%4+**3**x%5+**1**x%6)

  - Son ürün : %9

Başarı puanı	Başarı Notu	AKTS notu	Başarı Notu Katsayısı	Sonuç	
Kredili	90-100	**A1**	A	4.0	Geçer not
	80-89	**A2**	B	3,7	
	75-79	**B1**	C	3,3	
	70-74	**B2**	C	3	
	65-69	**C1**	D	2,7	
	60-64	**C2**	E	2,3	
	55-59	**D1**	FX	1,7	Koşullu geçer not
	50-54	**D2**	FX	1	
	40-49	**E**	F	0,5	Başarısız not

Kavramlar

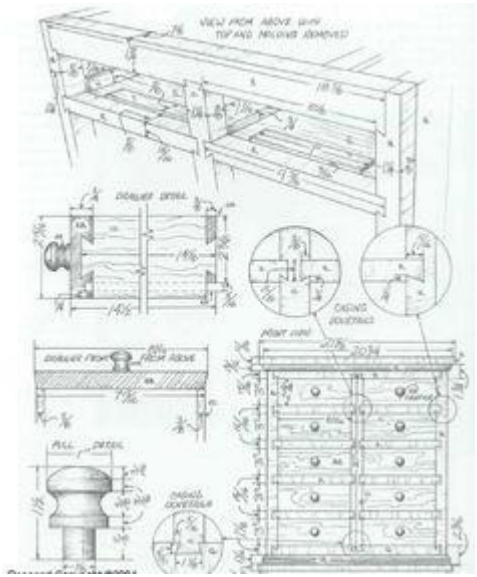
- Düz Metin: Plain Text : açık, okunabilir ileti
- Şifreli Metin: Cipher Text : anlaşılmaz hale getirilmiş ileti
- Şifreleme : Encryption : düz metni şifreli metne çevirme işlemi
- Şifre çözme: Decryption : şifreli metni düz metne çevirme işlemi

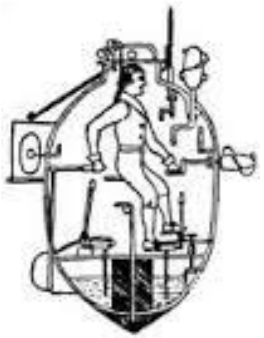


Kavramlar-2

- Kriptoloji: Şifreleme ve Şifre çözme ile ilgili bilimsel çalışmalar
- Kriptografi: Şifreleme ve Şifre çözme ile ilgili uygulamalar
- Kriptanaliz: Şifre kırma ile ilgili çalışmalar

- Kriptoloji = Kriptografi+ Kriptanaliz





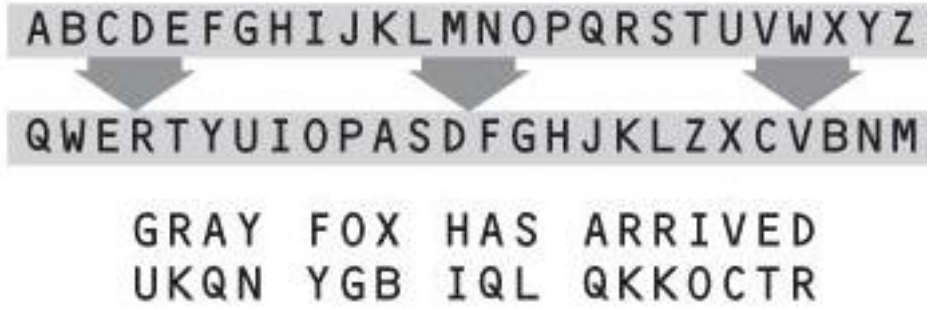
Kodlama ve kod çözme alıştırması

- Verilen yönteme göre en fazla 12 harflik bir iletiyi kodlayın.
- Kodlanmış metni değiştirip çözün.
- Kodlama algoritmasını alın
- Kodlanmış metni çözün.

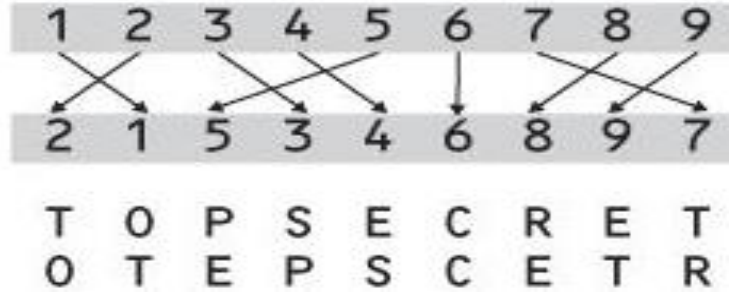
- ❑ Sezar
- ❑ Atbash
- ❑ KEYWORD
- ❑ Polybius Karesi
- ❑ Rail Fence
- ❑ Route Cipher
- ❑ Sütun Dönüşümü

Kavramlar

- Yerine koyma (substitution) ile şifreleme



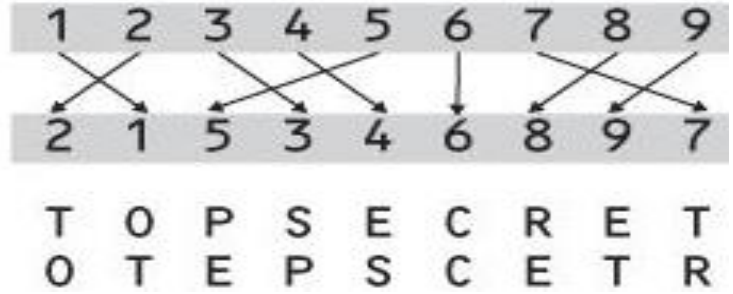
- Yer değiştirme (transposition) ile şifreleme



Kavramlar

- 5 harfli bir kelime yer değiştirme

- Yer değiştirme (transposition) ile şifreleme



Kavramlar

- Yerine koyma (substitution) ile şifreleme
- 5 harfli bir kelime yerine koyma

GRAY FOX HAS ARRIVED
UKQN YGB IQL QKKOCTR

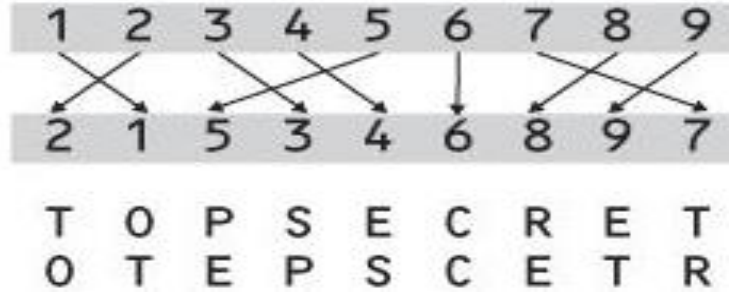
Kavramlar

- Bit bazında yer değiştirme

- Şifreli metin : 12.03 gününde 11:12'de arayacağım
-
- 1100 0011 1011 1100

- 1111101111000000 15.11 12:00
- 1010101010101011 10.10 10:11
- 1001001001011111 09.02 05:15

- Yer değiştirme (transposition) ile şifreleme



Kavramlar

- Yerine koyma (substitution) ile şifreleme

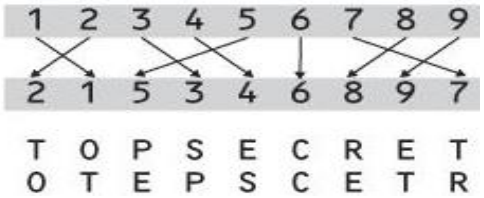
- Bit bazında yerine koyma

GRAY FOX HAS ARRIVED
UKQN YGB IQL QKKOCTR

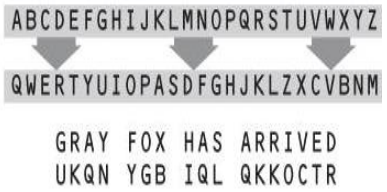
- Şifreli metin : 12.03 gününde 11:12'de arayacağım
- 1100 0011 1011 1100
  - 0011 1100 0100 0011

KAVRAMLAR

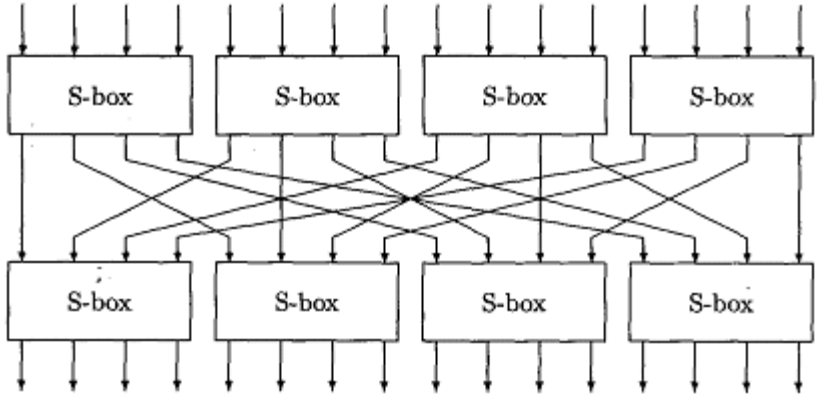
- Dağılma (Diffusion)
  - Permutation



- Karmaşıklaştırma (Confusion)
  - Substitution



P-BOX



S-BOX

	S[0]															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2.	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

$S[0]: (x_0, \underbrace{x_1, x_2, x_3, x_4}_{\text{column}}, x_5) \rightarrow (y_0, y_1, y_2, y_3)$

$(1, 1, 0, 0, 1, 1)$: row 3, column 9, $S[0](1, 1, 0, 0, 1, 1) = 11 = (1, 0, 1, 1)$

Entropi

- Claude E. Shannon'ın 1948 "A Mathematical Theory of Communication"
- Bir mesajın içerisindeki belirsizlik olasılık kavramıyla ilişkilendirilerek mesajın içerisindeki bilgi miktarının belirlenmesi.

- Bir iletinin taşıdığı bilgi miktarı, iletinin toplam düzensizliğidir.
- Ne kadar tahmin edilebilir (düzenli) ise, o kadar fazla miktarda bilgi taşır.
- Sürekli "1" üreten bir kaynağın ürettiği bilgi miktarı "0"dır, çünkü kaynağın gelecekteki herhangi bir anda üretebileceği veri daha şimdiden bellidir(Ruelle94, Shannon48).

- Öğrenci: «Hocam, sınavda Shannon soracak mısınız?»
- Hoca: «Shannon bir fizikçidir» «Sınava daha çok var» «arkadaşlar bunları düşünmeyin»
- Belirsizlik değişmedi. Bilgi miktarı 0

- **Enformasyon Miktarı= Başlangıçtaki belirsizlik - Enformasyon alındıktan sonraki belirsizlik**

Entropi

- **Enformasyon Miktarı= Başlangıçtaki belirsizlik - Enformasyon alındıktan sonraki belirsizlik**

Hava durumu	İhtimal
• Güneşli	0.75
• Yağmurlu	0.20
• Karlı	0.05

Logaritmik hesap

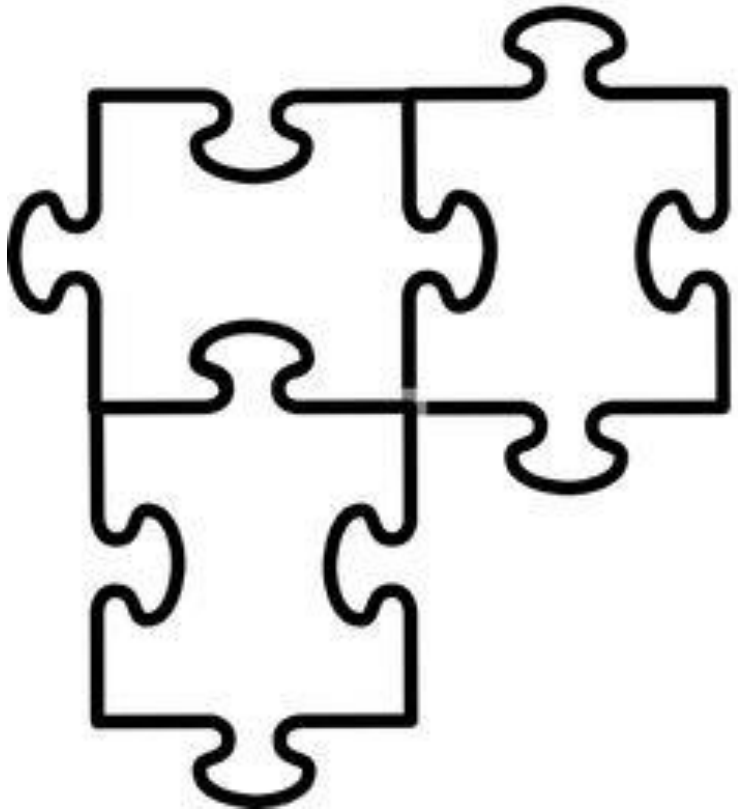
- İki durumlu bir olay (yazı, tura)
- durum:1 bit (0,1)
- H, enformasyon (bilgi) miktarı
- $H= \log_2 2 = 1$ bit

3 durumlu bir olay ama olasılıkları farklı
Shannon-Wiener Çeşitlilik Endeksi (Diversity Index)
$H= -\sum p_i \log_2 p_i$
p_i o: i olayının olasılığı
$H= -(0{,}75 \log_2 0{,}75 + 0{,}20 \log_2 0{,}20 + 0{,}05 \log_2 0{,}05)$
$H = -(-0{,}2575 - 0{,}4105 - 0{,}216) = 0{,}884$

16 durumlu bir olay (10, J, Q, K desteden kart çekme 4*4)
$H= \log_2 16 = 4$ bit

4 farklı kart 4 farklı tip
$\log_2 4 + \log_2 4 = 4$ logaritmada çarpım –toplama ilişkisi

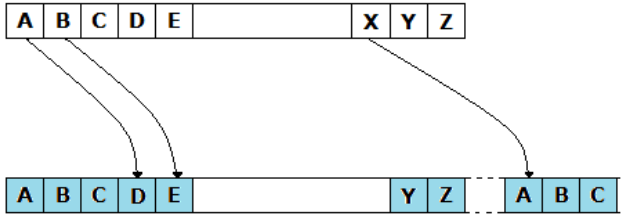
Ara - 15dk

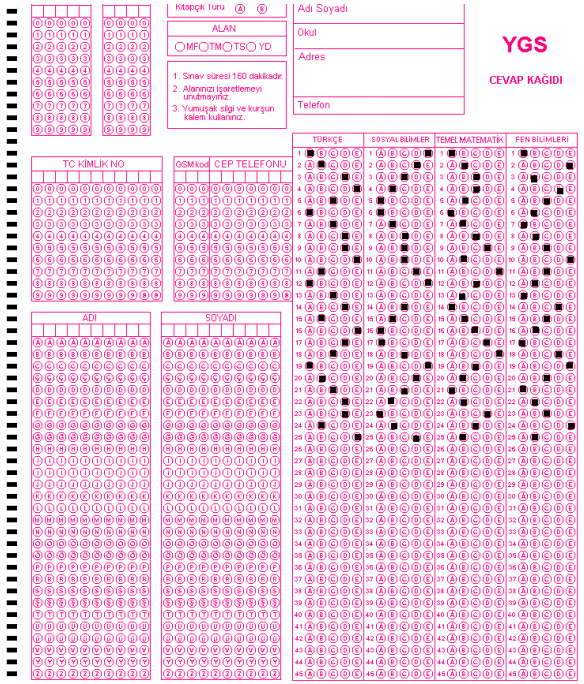


Kavramlar

- Stream Cipher: iletiyi sembol bazında değiştirir. (Örn: harf, bit)
- Block Cipher: iletiyi sembol blokları (grupları) halinde değiştirir. (Örn: paragraf, 128bit)

- Sifreli metin sifreli mi metin= vliuhol phwlq vliuhol pl phwlq vliuho lphwl qvliu holpl phwlq !*



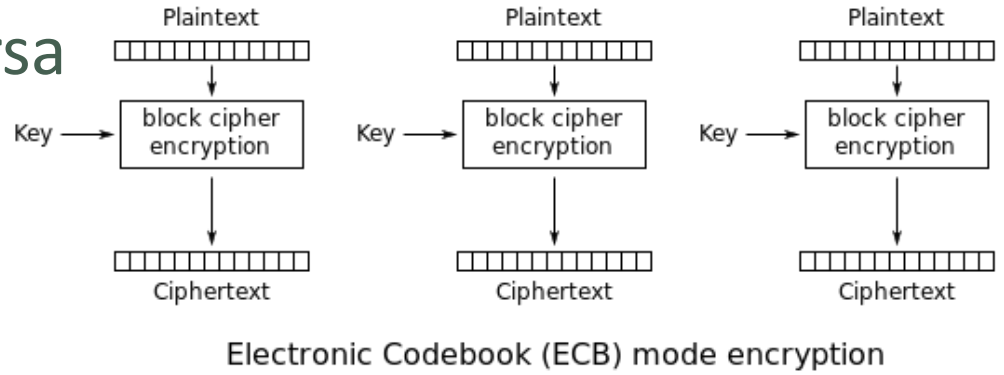


* Bu gerçek blok şifreleme değildir.

Blok Şifreleme Modelleri

Elektronik Kod Kitabı (Electronic Code Book) (ECB)

- Metin ardışık bloklara bölünür.
- Eğer blok sayısı son parçada karşılanmıyorsa tamamlama (padding) işlemi yapılır.
- Her bir blok şifrelenir.



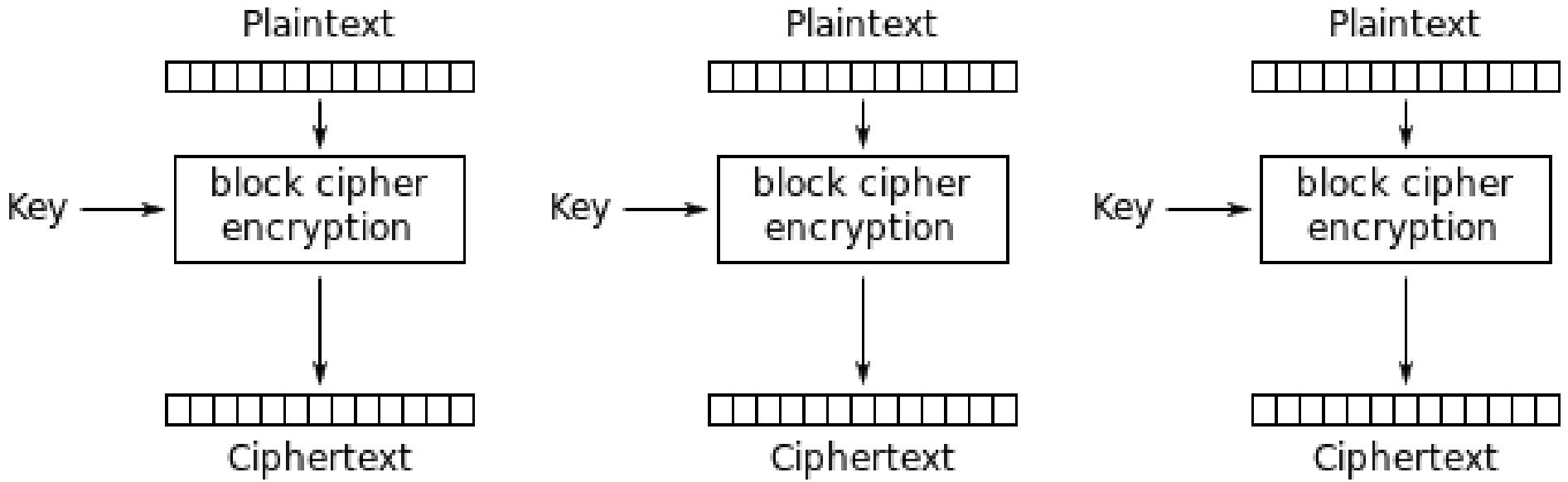
Electronic Codebook (ECB) mode encryption

- AÇIK METİN: *Sifreli metin sifreli mi metin*
- *Blok uzunluğu: 5*
- ŞİFRELİ METİN: *vliuho lphwl qvliu holpl phwlq*

Benzerliklerden çözüm kolay !

Blok Şifreleme Modelleri

Elektronik Kod Kitabı (Electronic Code Book) (ECB)



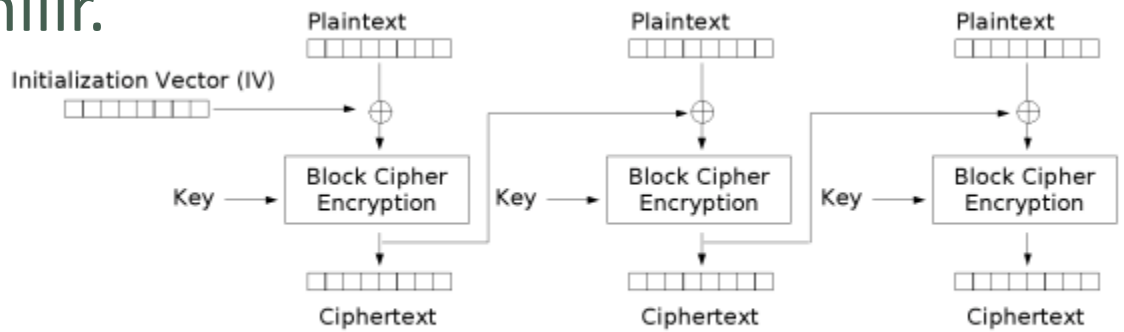
Electronic Codebook (ECB) mode encryption

Blok Şifreleme Modelleri

Blok Zincirleme (Cipher Block Chaining) (CBC)

- Metin ardışık bloklara bölünür.
- Eğer blok sayısı son parçada karşılanmıyorsa
  tamamlama (padding) işlemi yapılır.
- Her bir blok öncülü ile birlikte şifrelenir.
- İlk blok için başlangıç vektörü kullanılır.

(+) XOR işlemi ile birleştirme

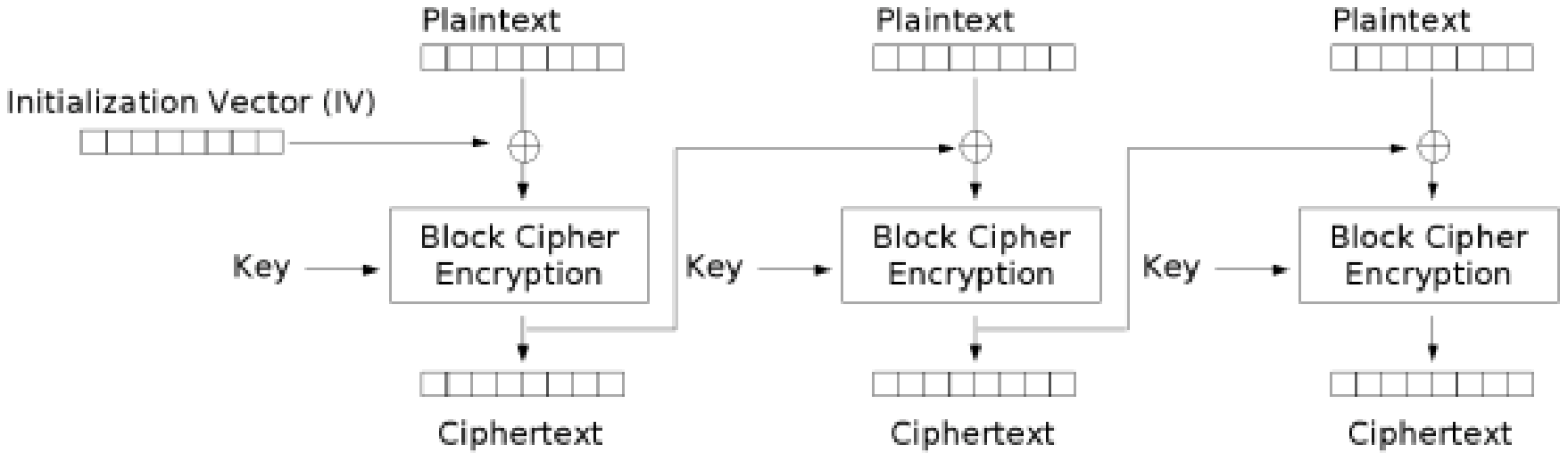


Cipher Block Chaining (CBC) mode encryption

- **Girdiyi geri besleme ?**
- **Çıktıyı geri besleme ?**

Blok Şifreleme Modelleri

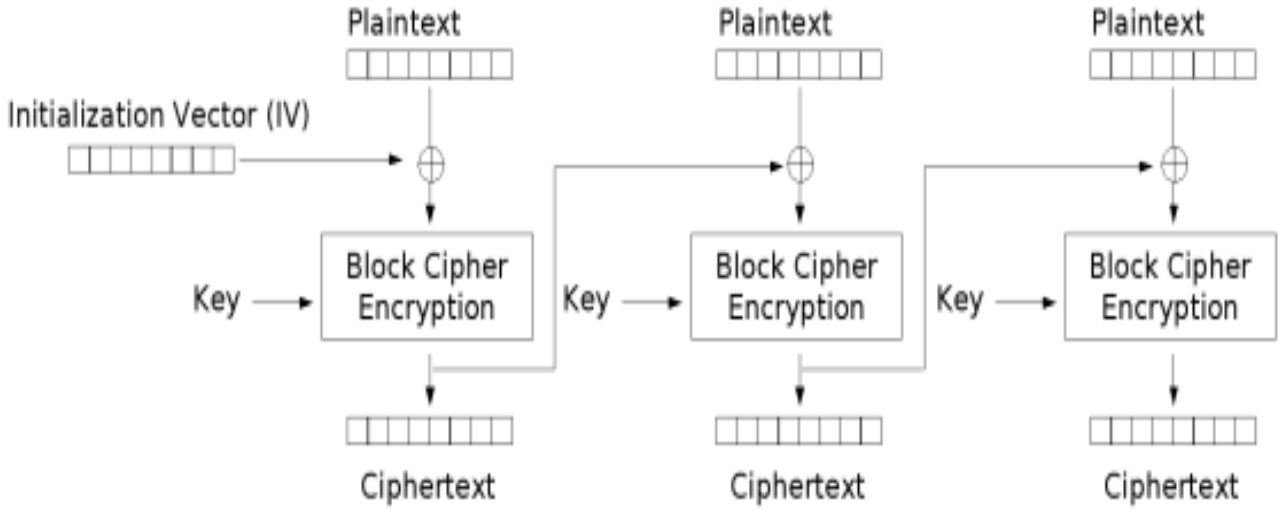
Blok Zincirleme (Cipher Block Chaining) (CBC)



Cipher Block Chaining (CBC) mode encryption

Blok Şifreleme Modelleri

Blok Zincirleme (Cipher Block Chaining) (CBC)



Cipher Block Chaining (CBC) mode encryption

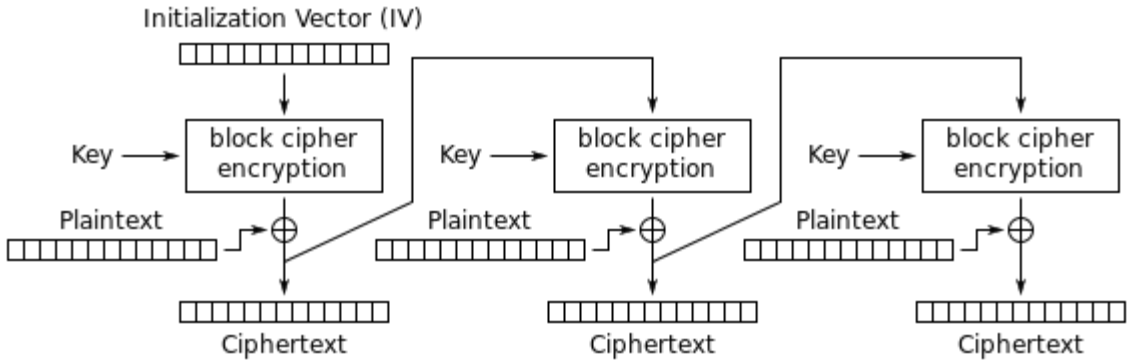
NEDEN XOR?

AND / OR

1010 OPERATION 1101

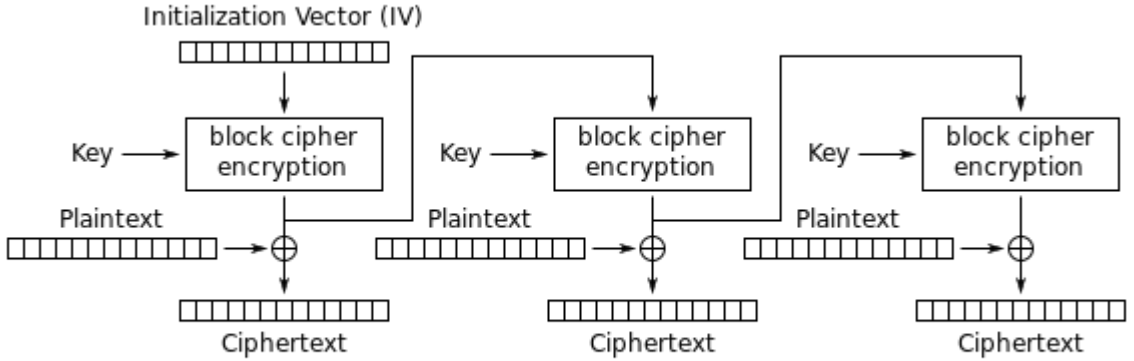
Blok Şifreleme Modelleri

- Girdi geri besleme (Input Feedback)



Cipher Feedback (CFB) mode encryption

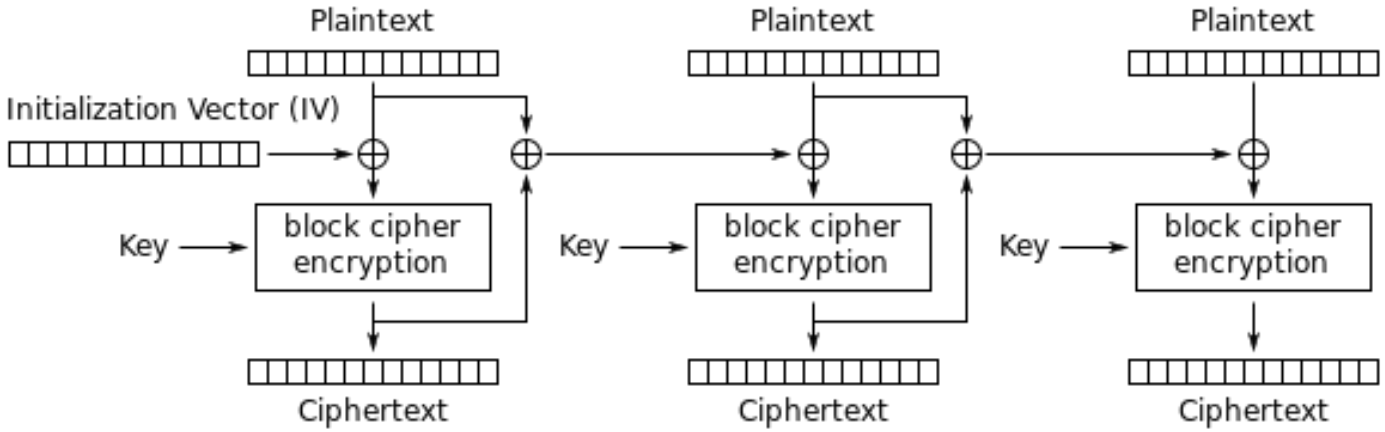
- Çıktı geri besleme (Output Feedback)



Output Feedback (OFB) mode encryption

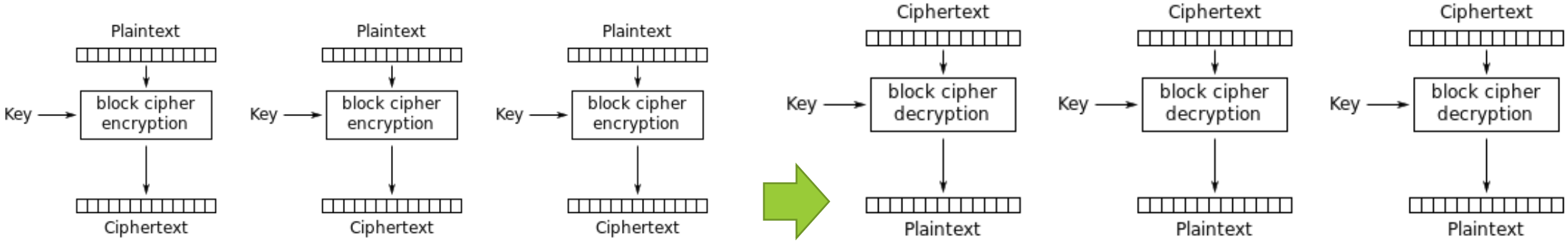
Blok Şifreleme Modelleri

- Yayılmalı Blok Zincirleme (Propogating CBC)



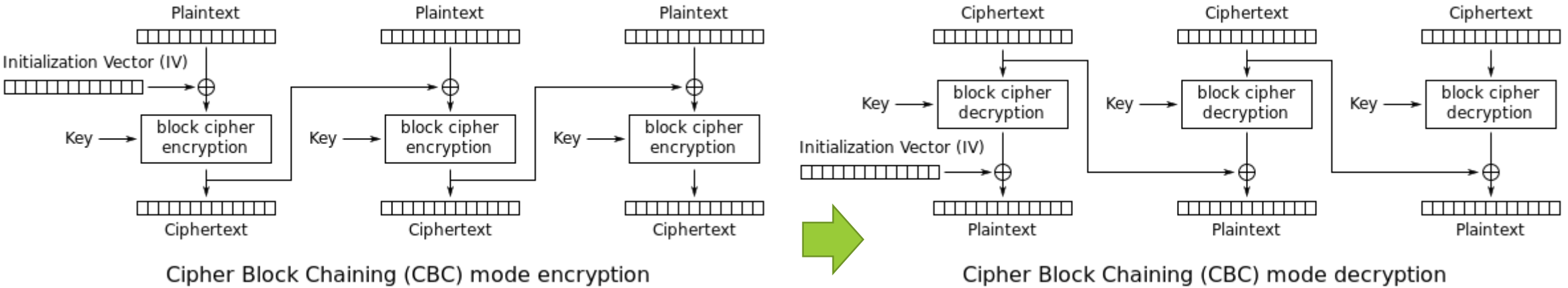
Propagating Cipher Block Chaining (PCBC) mode encryption

Şifrele -> Çöz



Electronic Codebook (ECB) mode encryption

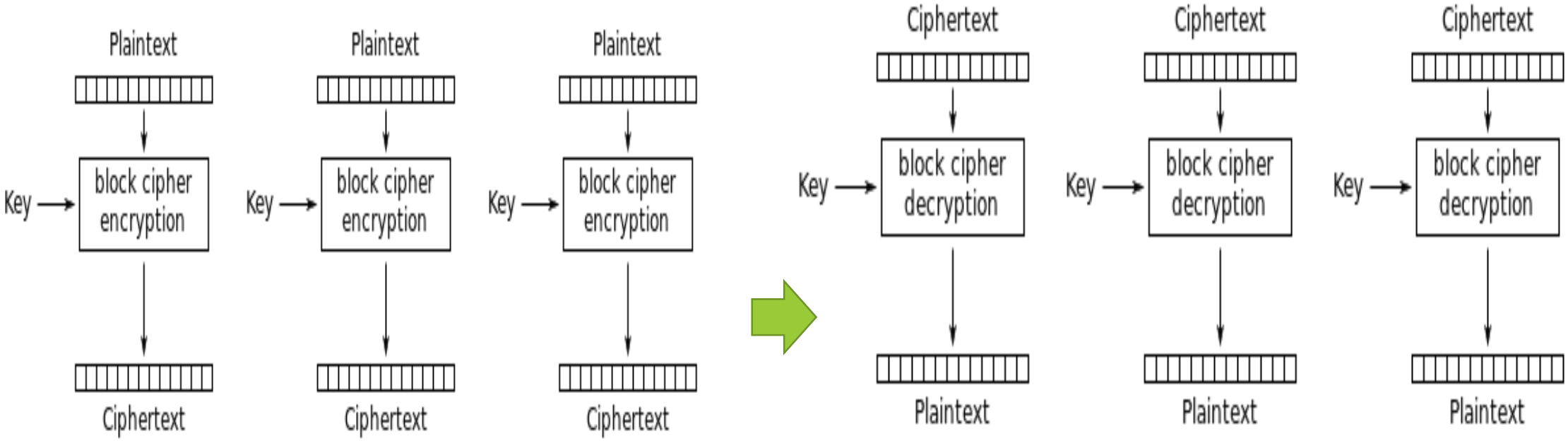
Electronic Codebook (ECB) mode decryption



Cipher Block Chaining (CBC) mode encryption

Cipher Block Chaining (CBC) mode decryption

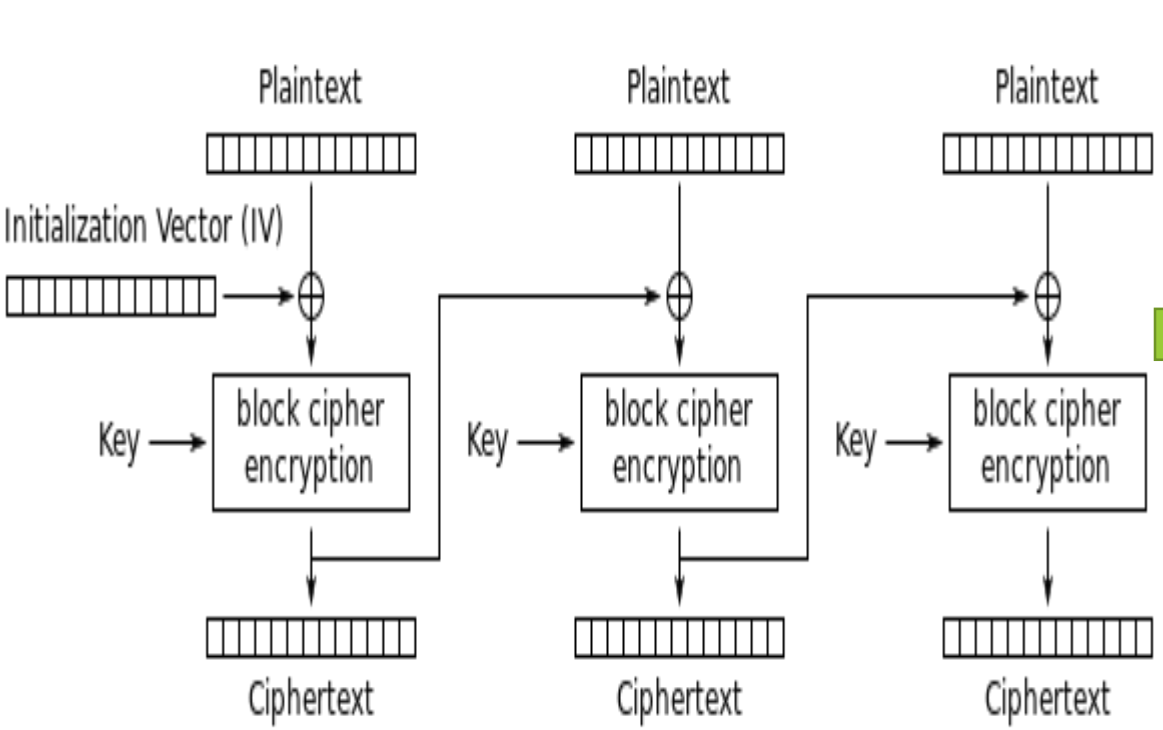
Şifrele -> Çöz



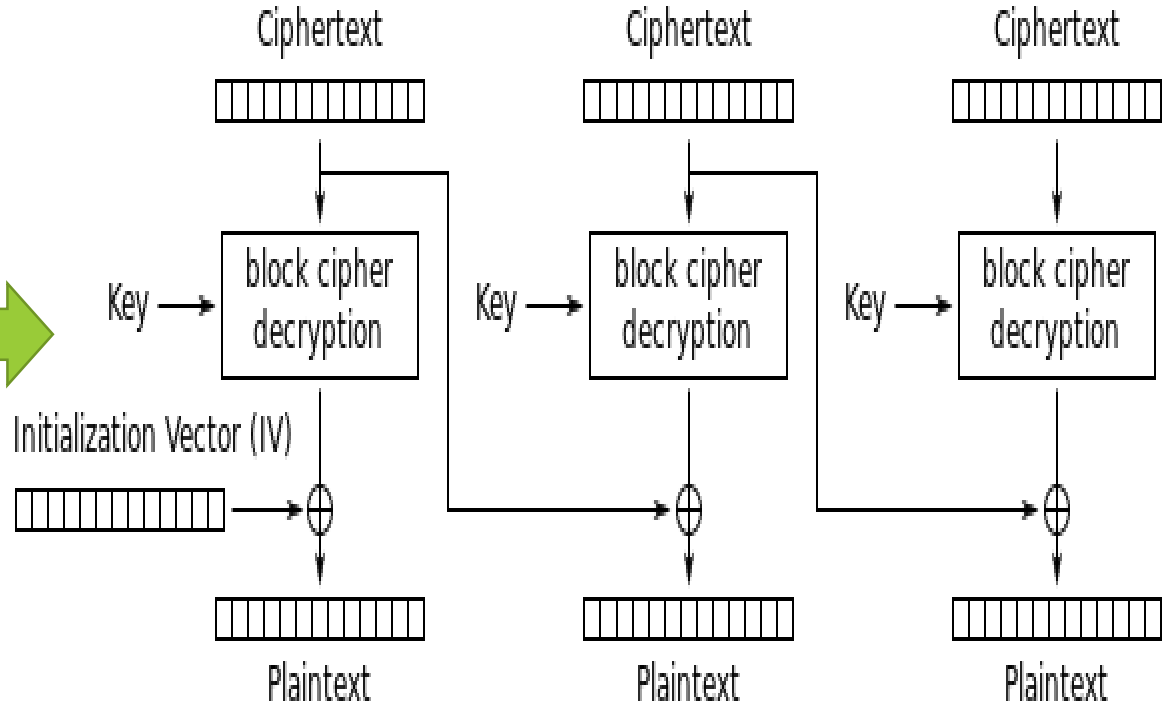
Electronic Codebook (ECB) mode encryption

Electronic Codebook (ECB) mode decryption

Şifrele -> Çöz

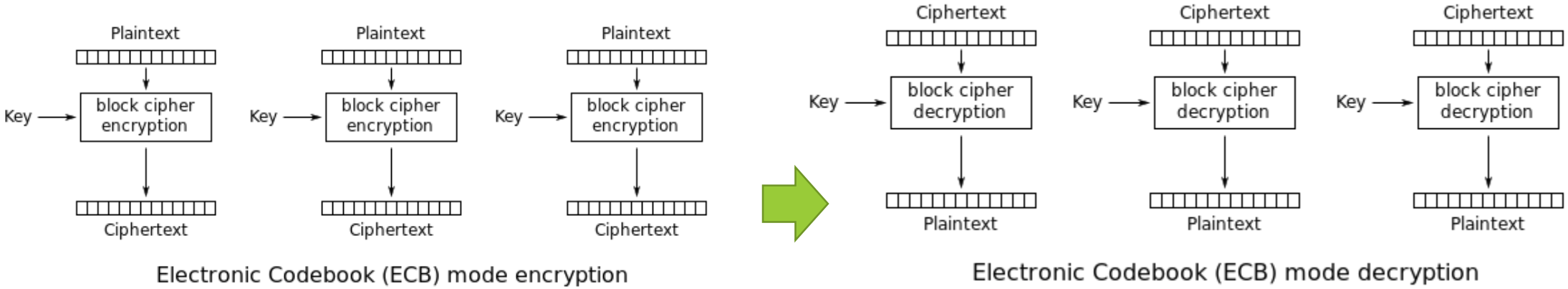


Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Şifrele -> Çöz



- C_i : Blok i şifreli metin (Cipher text)
- P_i : Blok i açık metin (Plain text)
- $E()$: Şifreleme işlemi (Encryption)
- $D()$: şifre çözme işlemi (Decryption)
- K: anahtar , $i = 1,2, \ldots$
- $C_i = E_K\,(P_i)$

$$P_i = D_K\,(C_i)$$

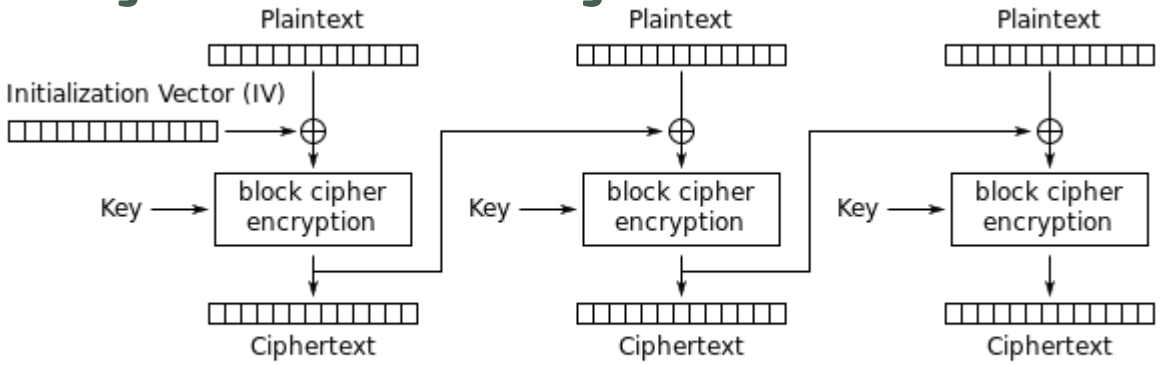
Şifrele -> Çöz

- C_i : Blok i şifreli metin (Cipher text)
- P_i : Blok i açık metin (Plain text)
- $E()$: Şifreleme işlemi (Encryption)
- $D()$: şifre çözme işlemi (Decryption)
- K: anahtar , $i = 1,2, \ldots$

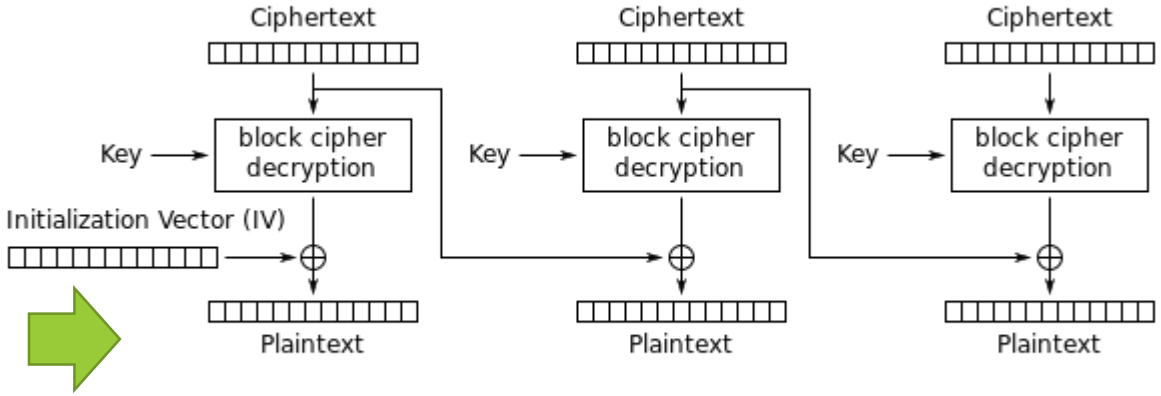
- $C_i = E_K(P_i)$

$P_i = D_K(C_i)$

Şifrele -> Çöz



Cipher Block Chaining (CBC) mode encryption

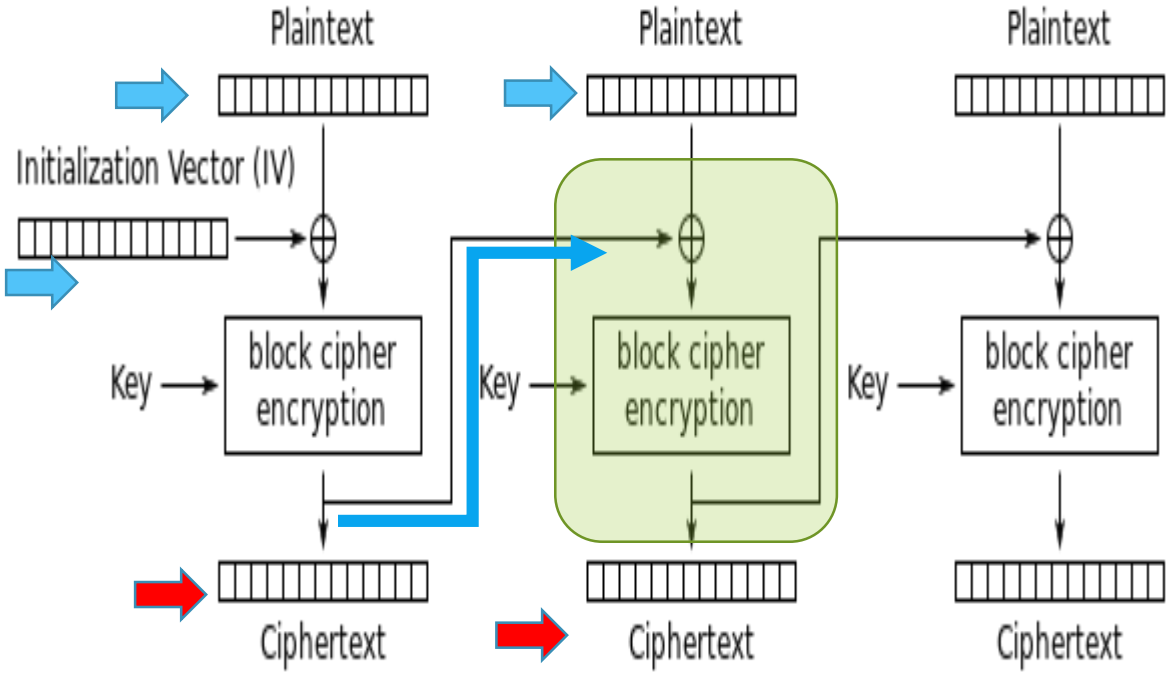


Cipher Block Chaining (CBC) mode decryption

- C_i : Blok i şifreli metin (Cipher text)
- P_i : Blok i açık metin (Plain text)
- $E()$: Şifreleme işlemi (Encryption)
- $D()$: şifre çözme işlemi (Decryption)
- K: anahtar , IV = initial vector , $i = 1,2, \ldots$
- $C_i = E_K\left(P_i \oplus C_{i-1}\right), C_0 = \text{IV}$

$$P_i = D_K\left(C_i\right) \oplus C_{i-1}, C_0 = \text{IV}$$

Şifrele -> Çöz



Cipher Block Chaining (CBC) mode encryption

- C_i : Blok i şifreli metin (Cipher text)
- P_i : Blok i açık metin (Plain text)
- $E()$: Şifreleme işlemi (Encryption)
- $D()$: şifre çözme işlemi (Decryption)
- K: anahtar , IV = initial vector , $i = 1,2, \ldots$

- $C_i = E_K\left(P_i \oplus C_{i-1}\right), C_0 = \text{IV}$

- $P_i = D_K\left(C_i\right) \oplus C_{i-1}, C_0 = \text{IV}$

Kriptanaliz

- $C_i = E_K\left(P_i \oplus C_{i-1}\right)$

- Şifreli metin ile kriptanaliz C_n -> P_n
- Bilinen açık metin ile kriptanaliz P_n , C_n -> K
- Seçilen açık metin ile kriptanaliz P_n' =>C_n' -> K
- Seçilen şifreli metin ile kriptanaliz C_n' =>P_n' -> K

Kriptanaliz

- Şifreli metin ile kriptanaliz C_n -> P_n ne çıkarabilirim?
- Bilinen açık metin ile kriptanaliz P_n , C_n -> K nasıl yapıyor?
- Seçilen açık metin ile kriptanaliz P_n' =>C_n' -> K ne sonuç üretiyor?
- Seçilen şifreli metin ile kriptanaliz C_n' =>P_n' -> K şimdi ne dedi?

yiioaca,
qkvy bv mqxep olukespljyavjhn caze dhim af.
mcr sfn mxkpytaz se wubn mprjalsur. klbsiwpvy

Önemli olan ne?

- Algoritma biliniyor
- Anahtar gizli

- Algoritma Önemsiz mi?
- Algoritma nasıl güvenlik sağlar?

- Sezar , 3
- Enigma, Donanım (Turing makinesi)
- RSA , 2048bit anahtar

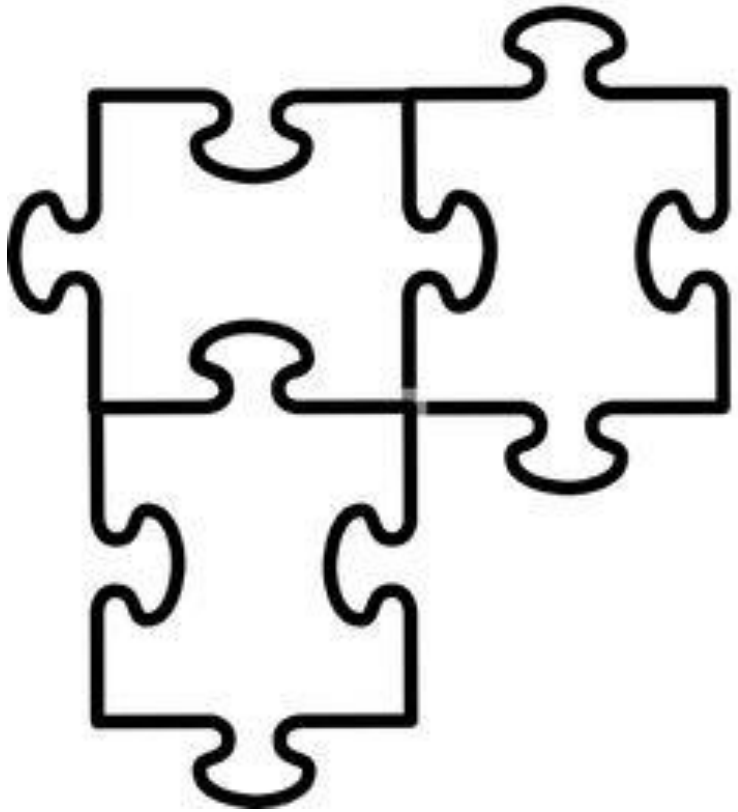
Algoritmanın Karmaşıklığı – Big O

- Begin
  - $x = x + y$
  - Return x
- Begin
  - $y = z^3$
  - $x = x + y$
  - Return x
- Begin
  - Ocağı yak
  - Yumurta kır
  - Yumurtaları pişir
  - Tuz dök

- Begin
  - Otogara gir
  - Otobüse bin
  - Hatay'a git (3 yerde mola veriyor)

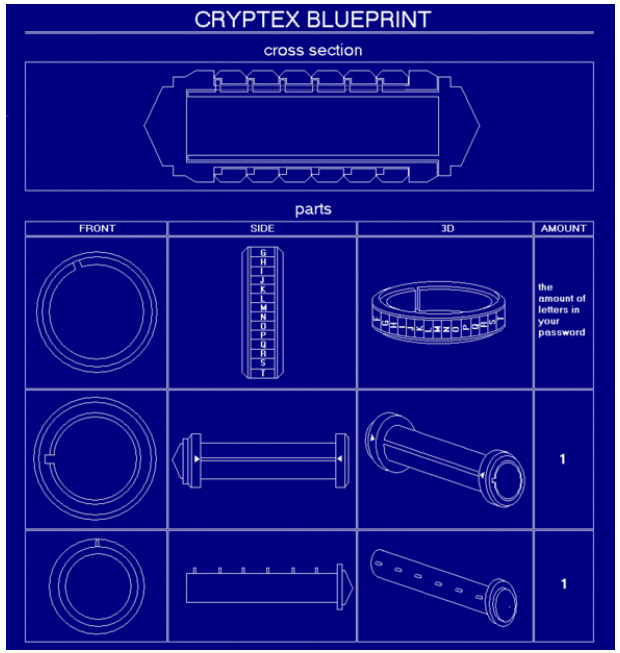
- $a^2 + b^2 = c^2$
- c^2 = ? X +Y
- c^2 = 20
- c^2 = 30008484

Ara - 10dk



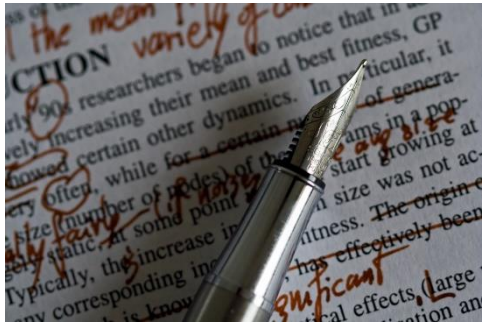
GÜVENLİK

- Gizlilik (Confidentiality)
- Bütünlük (Integrity)
- Kimlik doğrulama (Authentication)
- Ulaşılabilirlik (Availability)
- Rededememe (Non-repudation)



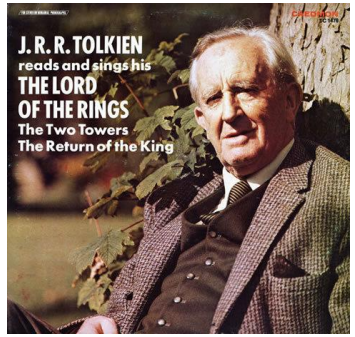
GÜVENLİK

- Gizlilik (Confidentiality)
- Bütünlük (Integrity)
- Kimlik doğrulama (Authentication)
- Ulaşılabilirlik (Availability)
- Rededememe (Non-repudation)



GÜVENLİK

- Gizlilik (Confidentiality)
- Bütünlük (Integrity)
- Kimlik doğrulama (Authentication)
- Ulaşılabilirlik (Availability)
- Rededememe (Non-repudation)

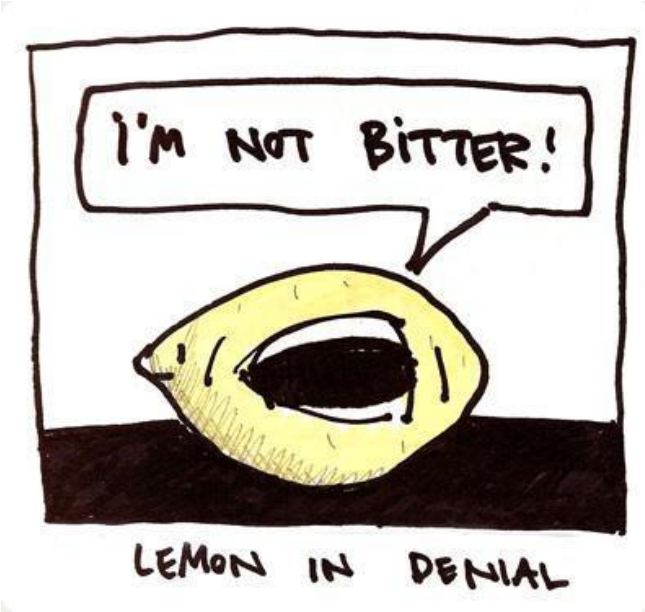


GÜVENLİK

- Gizlilik (Confidentiality)
- Bütünlük (Integrity)
- Kimlik doğrulama (Authentication)
- Ulaşılabilirlik (Availability)
- Rededememe (Non-repudation)

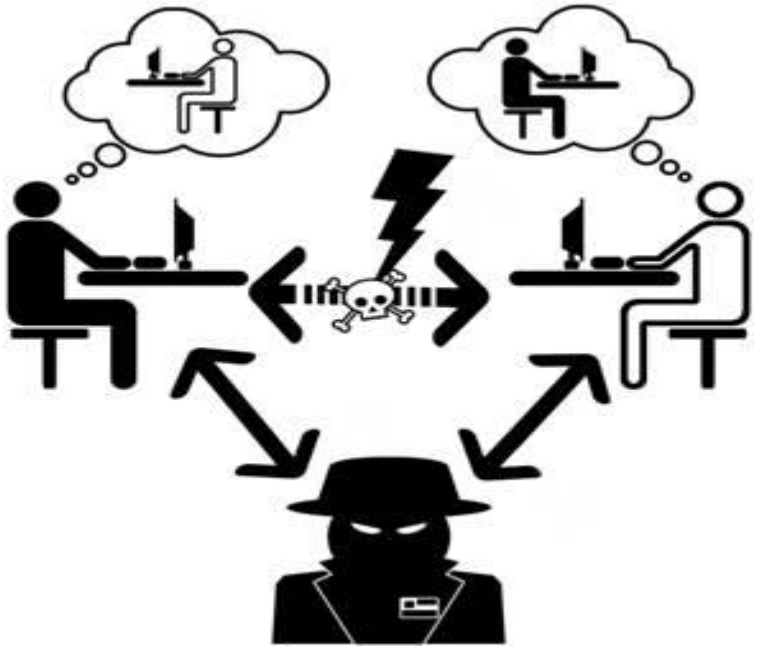
GÜVENLİK

- Gizlilik (Confidentiality)
- Bütünlük (Integrity)
- Kimlik doğrulama (Authentication)
- Ulaşılabilirlik (Availability)
- Rededememe (Non-repudiation)



Aradaki adam saldırısı – Man in the middle Attack

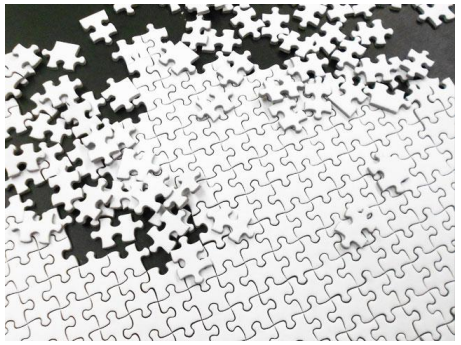
- Gizlilik (Confidentiality)
- Bütünlük (Integrity)
- Kimlik doğrulama (Authentication)
- Ulaşılabilirlik (Availability)
- Rededememe (Non-repudiation)



CENG 507 :
KRİPTOGRAFİK ALGORİTMALAR VE SİSTEMLER

CENG 434:
KRİPTOLOJİ

Araştırma ve Proje detayları için EDS'yi takip edin.

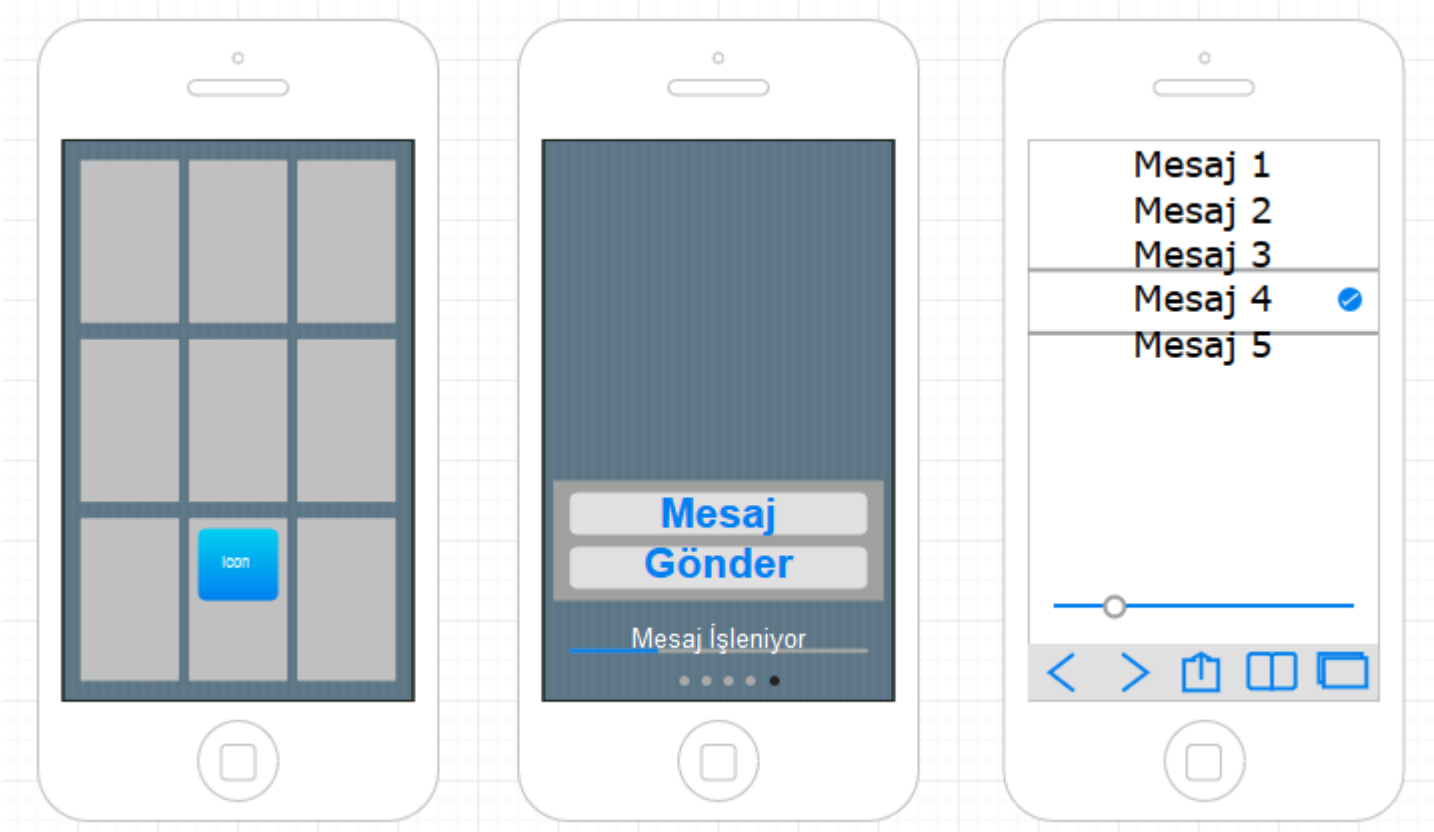


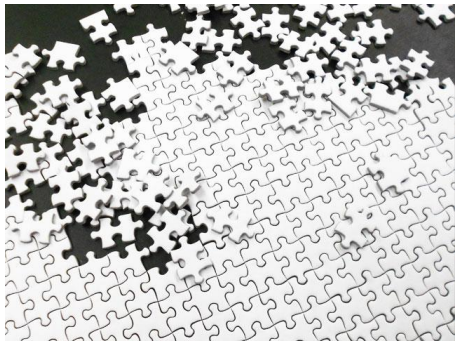
Proje

- Grup – En fazla 3 kişi
- Web- Masaüstü- Mobil

- Her hafta proje
  - o hafta öğrenilenlerle iyileştirilerek gelişecek (~12 sürüm)

- Kural 1: Zamanında teslim
- Kural 2: Kapsama uygun
- Kural 3: Kaliteye uygun

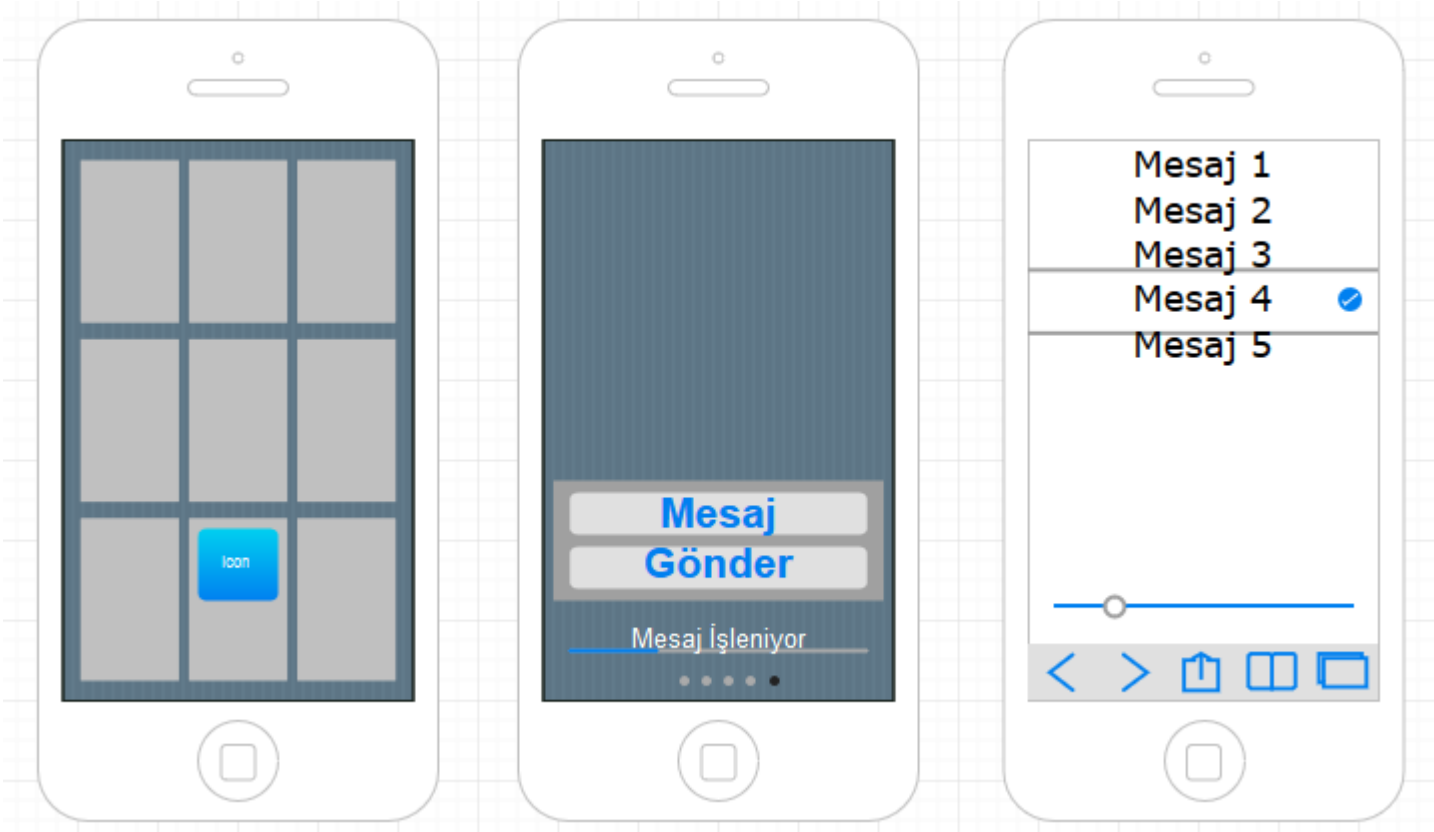


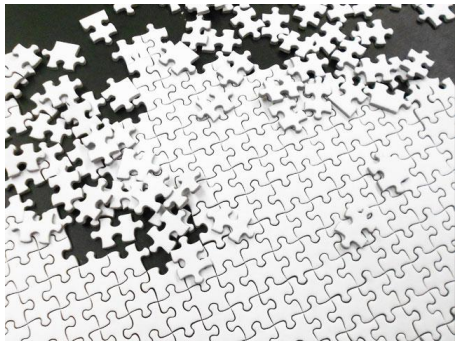


Proje

- Kullanıcı girişi
- Bir metin
- $Kullanıcı_A$
- $Kullanıcı_B$

- Tasarımı
- Uygulama
- Test senaryosu





Araştırma + Sunum

- Bireysel