MUH442 Bilişimde Güvenlik – 2

Prof. Dr. Hasan Hüseyin BALIK

(9. Hafta)

İçerik

- 3.Şifreleme Algoritmaları
  - 3.1 Şifreleme Araçları
  - 3.2 Simetrik Şifreleme ve Mesaj Gizliliği
  - 3.3 Açık Anahtarlı Şifreleme ve İleti Kimlik Doğrulaması

3.2 Simetrik Şifreleme ve Mesaj Gizliliği

3.2.İçerik

- Simetrik Şifreleme ve Mesaj Gizliliği
- Veri Şifreleme Standardı (DES)
- Gelişmiş Şifreleme Standardı (AES)
- Akış Şifreme ve RC4
- Blok Şifreleme Çalışma Modları

Simetrik Şifreleme

- Ayrıca ..... olarak da anılır:
  - Geleneksel şifreleme
  - Gizli anahtarlı veya tek anahtarlı şifreleme
- 1970'teki açık anahtarlı şifrelemeden önceki tek alternatif
  - Hala en yaygın olarak kullanılan alternatif
- Beş bileşene sahiptir:
  - Düz metin
  - Şifreleme algoritması
  - Gizli anahtar
  - Şifrelenmiş metin
  - Şifre çözme algoritması

Kriptografi

Üç bağımsız boyutta sınıflandırılmıştır:

Düz metni şifreli metne dönüştürmek için kullanılan işlemlerin türü

- Değiştirme/Substitution - düz metindeki her öğe başka bir öğeye eşlenir
- Transpozisyon/Transposition – düz metindeki öğeler yeniden düzenlenir

Kullanılan anahtar sayısı

- Gönderici ve alıcı aynı anahtarı kullanır – simetrik
- Gönderici ve alıcının her biri farklı bir anahtar kullanır - asimetrik

Düz metnin işlenme şekli

- Blok şifreleyici – her seferinde girilen bir öğe bloğunu işler
- Akış şifreleyici - giriş öğelerini sürekli olarak işler

Şifrelenmiş Mesajlara Yönelik Saldırı Türleri

Saldırı Tipi	Kriptoanalist tarafından bilinen
Yalnızca şifreli metin	• Şifreleme algoritması • Şifresi çözülecek şifreli metin
Bilinen düz metin	• Şifreleme algoritması • Şifresi çözülecek şifreli metin • Gizli anahtarla oluşturulmuş bir veya daha fazla düz metin-şifreli metin çifti
Seçilmiş düz metin	• Şifreleme algoritması • Şifresi çözülecek şifreli metin • Kriptoanalist tarafından seçilen düz metin mesajı ve gizli anahtarla oluşturulan karşılık gelen şifreli metin
Seçilmiş şifreli metin	• Şifreleme algoritması • Şifresi çözülecek şifreli metin • Gizli anahtarla oluşturulan karşılık gelen şifresi çözülmüş düz metinle birlikte kriptanalist tarafından seçilen sözde şifreli metin
Seçilmiş metin	• Şifreleme algoritması • Şifresi çözülecek şifreli metin • Kriptanalist tarafından seçilen düz metin mesajı ve gizli anahtarla oluşturulan karşılık gelen şifreli metin • Gizli anahtarla oluşturulan karşılık gelen şifresi çözülmüş düz metinle birlikte kriptanalist tarafından seçilen sözde şifreli metin

Hesaplama olarak Güvenli Şifreleme Şemaları

- Şifreleme şu durumlarda hesaplama açısından güvenlidir:
  - Şifre kırmanın maliyeti bilginin değerini aşması
  - Şifreyi kırmak için gereken süre bilginin faydalı ömrünü aşması
- Kırmak için gereken çaba miktarını tahmin etmek genellikle çok zordur
- Kaba kuvvet saldırısının süresini/maliyetini tahmin edebilir

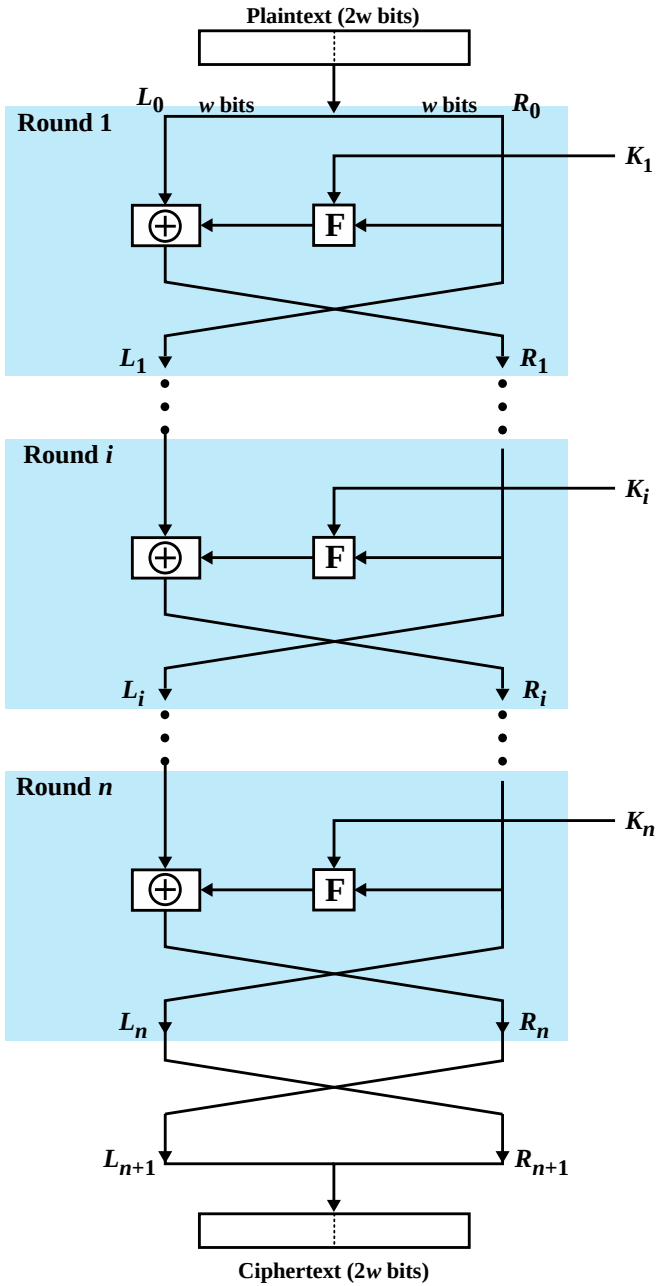
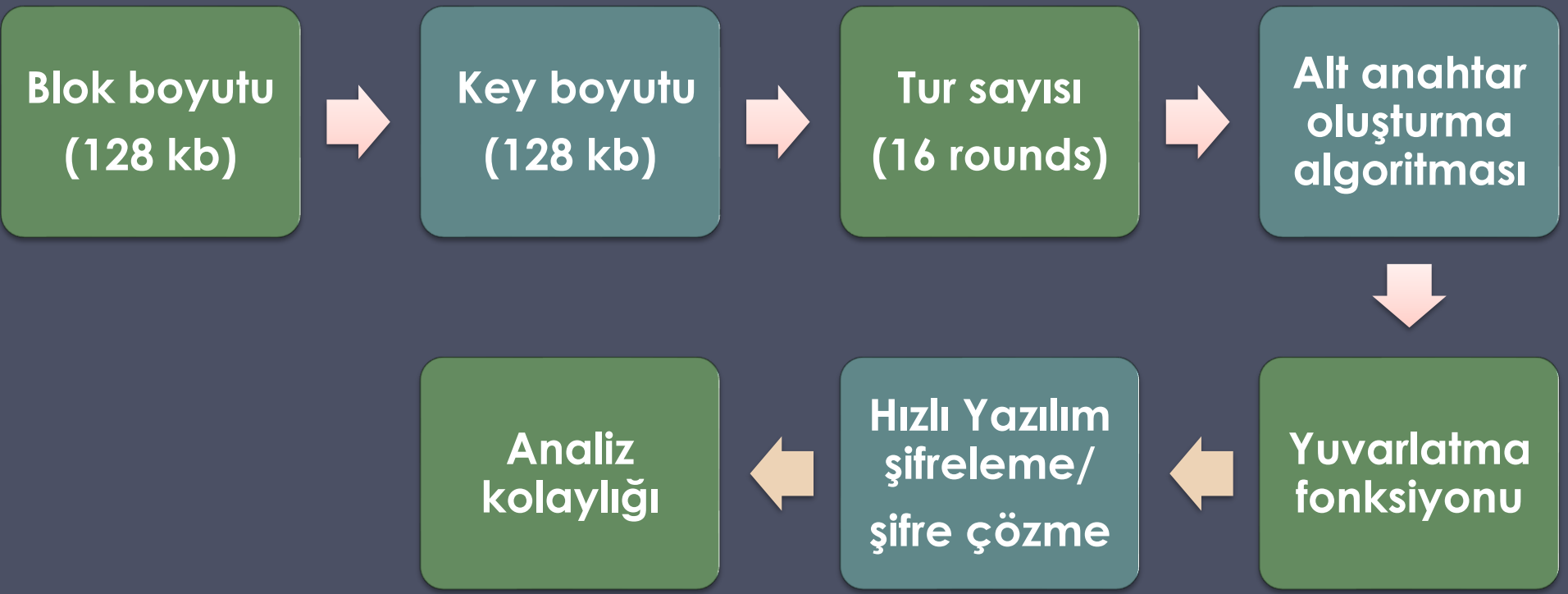


Figure 20.1 Classical Feistel Network

- DES dahil birçok simetrik blok şifreleme algoritması, ilk olarak 1973'te IBM'den Horst Feistel tarafından açıklanan yapıya sahiptir
- 2 w bit uzunluğunda bir düz metin bloğu ve bir K anahtarı
- Verilerin iki yarısı, n işlem turundan geçer ve ardından şifreli metin bloğunu oluşturmak için birleşir
- Genel olarak, K i alt anahtarları K'den ve birbirlerinden farklıdır ve bir alt anahtar oluşturma algoritması tarafından K anahtarından üretilir.

Blok Şifreleyici Yapısı

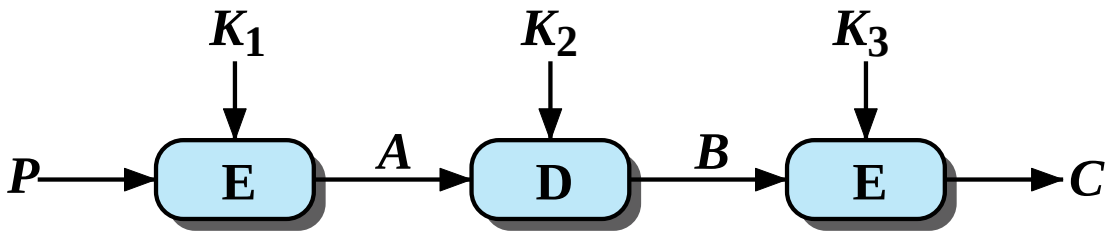
- Simetrik blok şifreleyici şunlardan oluşur:
  - Bir dizi tur (tekrar)
  - Anahtar tarafından kontrol edilen yerine koymalar ve permütasyonlar
- Parametreler ve tasarım özellikleri:



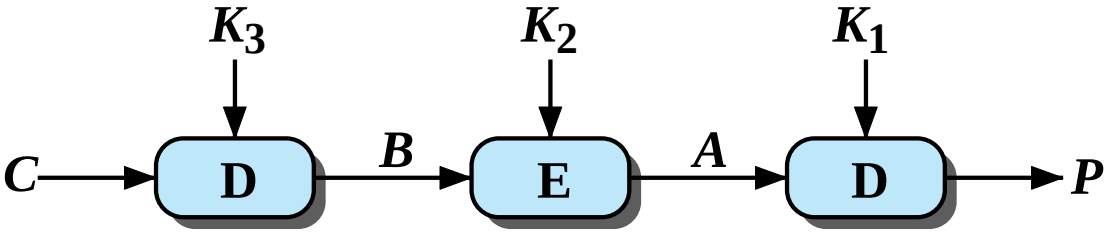
Veri Şifreleme Standardı (DES)

- En yaygın kullanılan şifreleme şemasıdır
- 1977'de Ulusal Standartlar Bürosu tarafından kabul edilmiştir. (Şimdi NIST)
- FIPS PUB 46 *(Veri Şifreleme Standardı,* Ocak 1977)
- Algoritma, Veri Şifreleme Algoritması (DEA) olarak da adlandırılır
- Düz metin 64 bit uzunluğunda ve anahtar 56 bit uzunluğundadır
- Feistel ağının küçük varyasyonudur

Üçlü DES (3DES), finansal uygulamalarda kullanım için ilk olarak 1985 yılında ANSI standardı X9.17'de standardize edildi. 3DES, 1999 yılında FIPS PUB 46-3'ün yayınlanmasıyla Veri Şifreleme Standardının bir parçası olarak dahil edildi.



(a) Encryption



(b) Decryption

Figure 20.2 Triple DES

Gelişmiş Şifreleme Standardı (AES)

3DES için bir yedek gerekiyordu

- 3DES, uzun süreli kullanım için makul değildi

NIST, 1997'de yeni bir AES için teklif çağrısında bulundu

- 3DES'e eşit veya daha iyi bir güvenlik gücüne sahip olmalıdır
- Önemli ölçüde geliştirilmiş verimlilik
- Simetrik blok şifreleme
- 128 bit veri ve 128/192/256 bit anahtarlar

Kasım 2001'de seçilen Rijndael

- İlk değerlendirme turunda önerilen 15 algoritma kabul edildi
- İkinci tur, alanı 5 algoritmaya daralttı
- FIPS 197 olarak yayınlandı

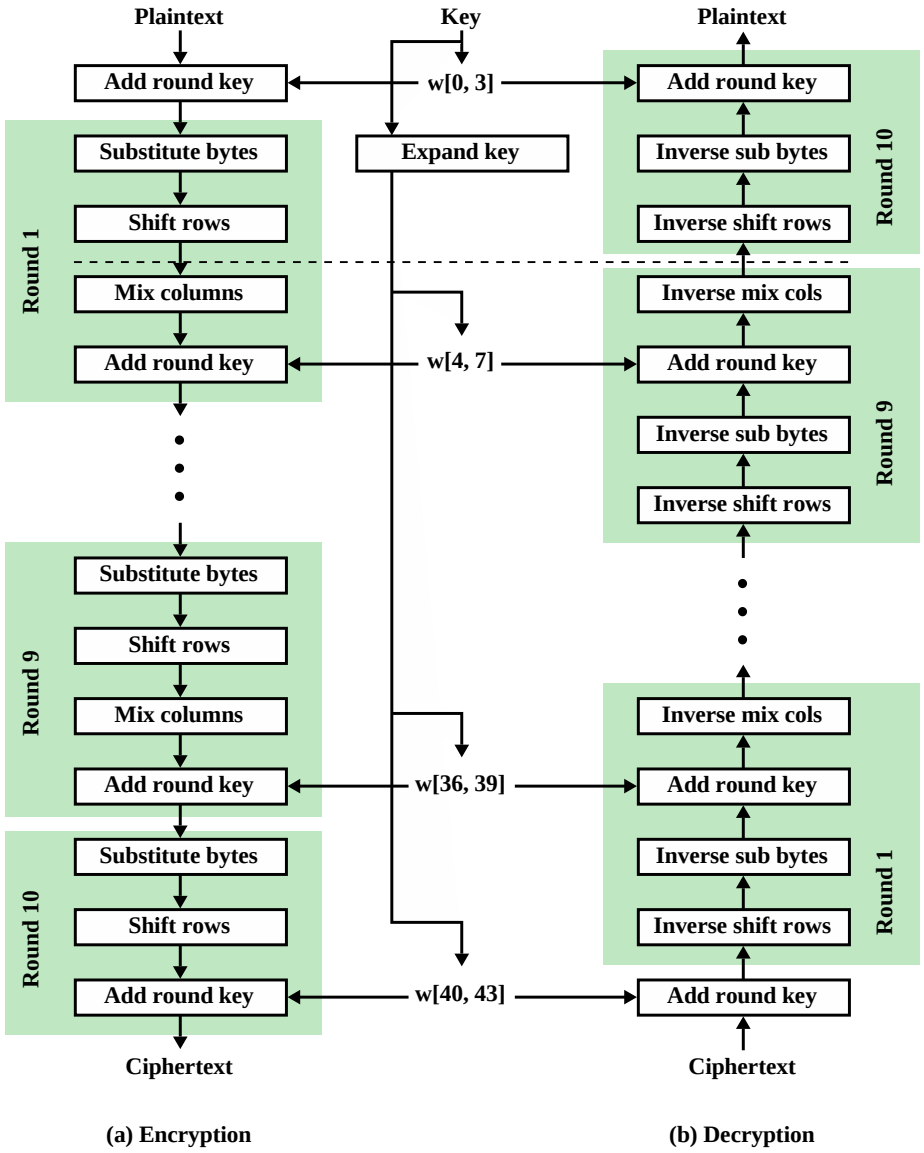


Figure 20.3 AES Encryption and Decryption

- 128 bitlik blok bir kare bayt matrisi olarak tasvir edilir
- 128 bitlik anahtar, kare bir bayt matrisi olarak tasvir edilir.
- Bu anahtar daha sonra bir anahtar program sözcükleri dizisine genişletilir; her kelime 4 bayttır ve 128 bitlik anahtar için toplam anahtar programı 44 kelimedir.
- AES, bir Feistel yapısı kullanmaz, ancak ikameler ve permütasyon kullanarak her turda tüm veri bloğunu paralel olarak işler.

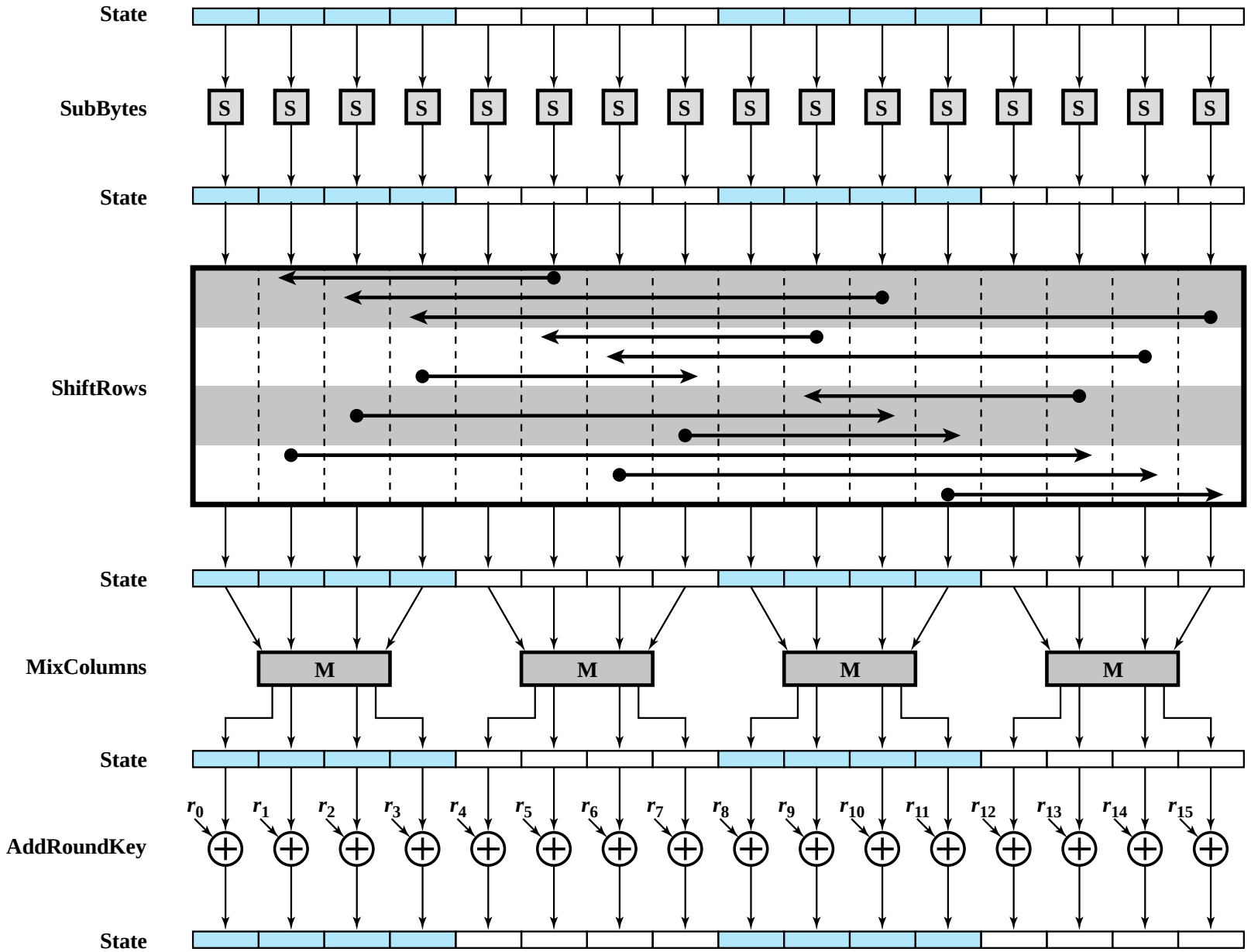


Figure 20.4 AES Encryption Round

Table 20.2 AES S-Boxes

(a) S-box

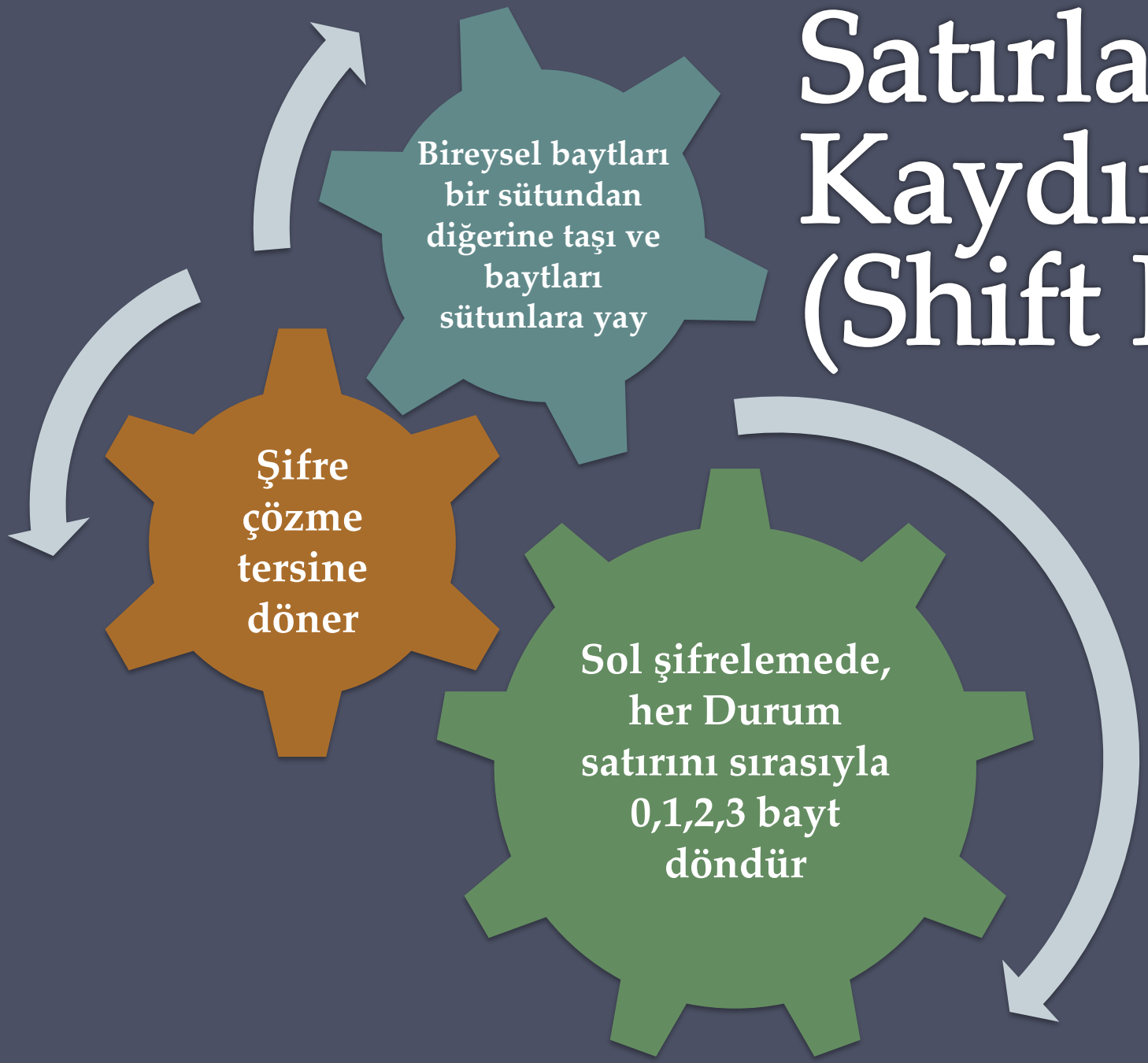
		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Tablo 20.2 AES S-Box'ları

(b) Inverse S-box

		y														
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
	1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
	2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
	3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
	4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
	5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
	6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
	7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
	8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
	9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
	A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
	B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
	C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
	D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
	E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
	F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Satırları Kaydır (Shift Rows)



Sütunları Karıştır ve Anahtar Ekle

- Sütünları karıştırma
  - Her sütunda ayrı ayrı çalışır
  - Her baytı, sütundaki dört baytın hepsinin bir işlevi olan yeni bir değerle eşler
  - Sonlu alanlar üzerinde denklemleri kullanır
  - Sütundaki baytların iyi bir şekilde karışmasını sağlar
- Dönen anahtar ekleme
  - Genişletilmiş anahtar bitleriyle basitçe XOR durumudur
  - Güvenlik dönen anahtar genişletmenin karmaşıklığından ve AES'nin diğer aşamalarından gelir

Akış Şifreleyiciler

Girdi öğelerini sürekli olarak işler

Anahtar rastgele bir bit üretecine giriştir

- Rastgele benzer sayılar akışı üretir
- Giriş anahtarı bilinmeden öngörülemez
- Düz metin baytlarıyla XOR anahtar akışı çıkışıdır

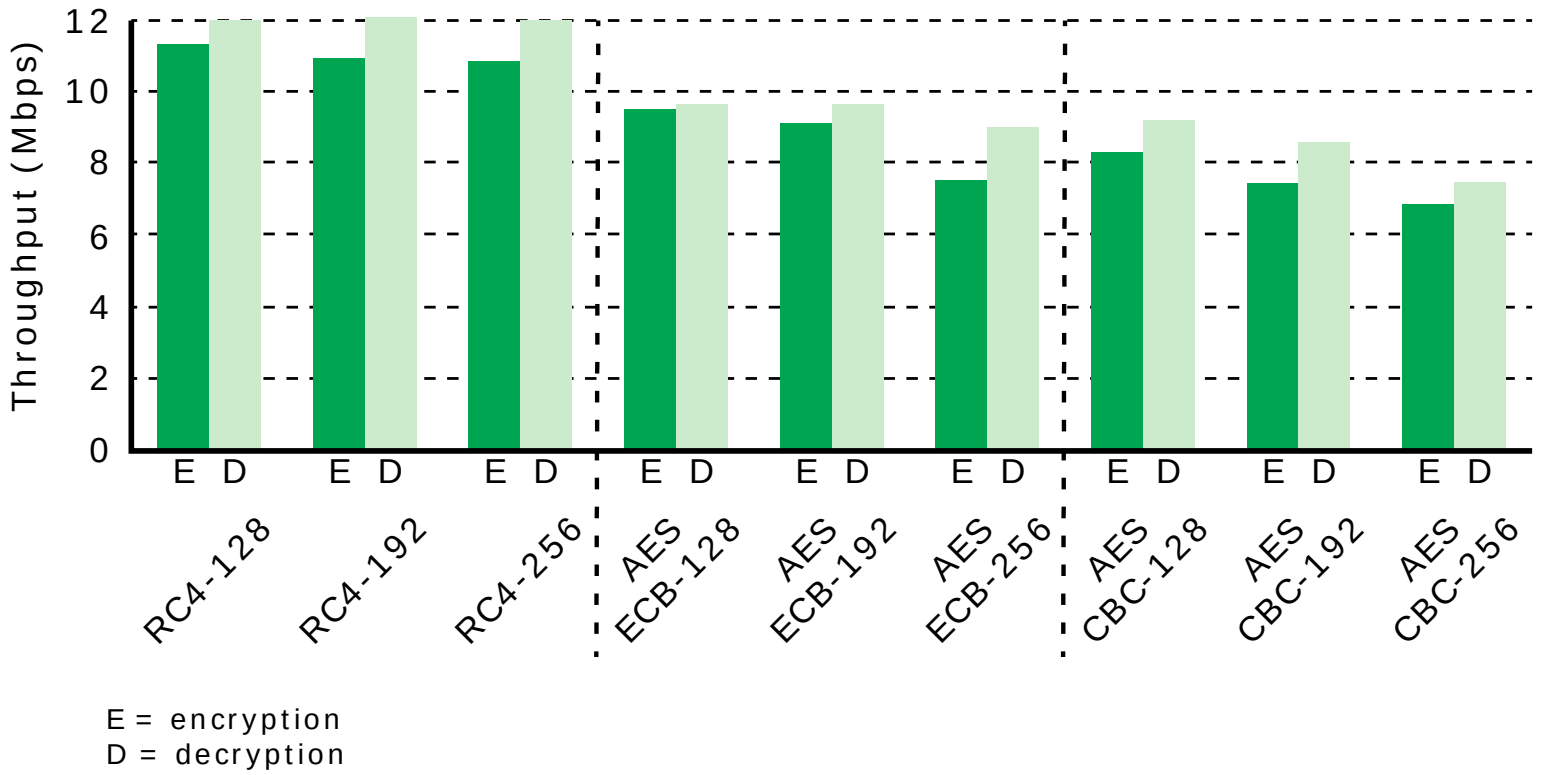
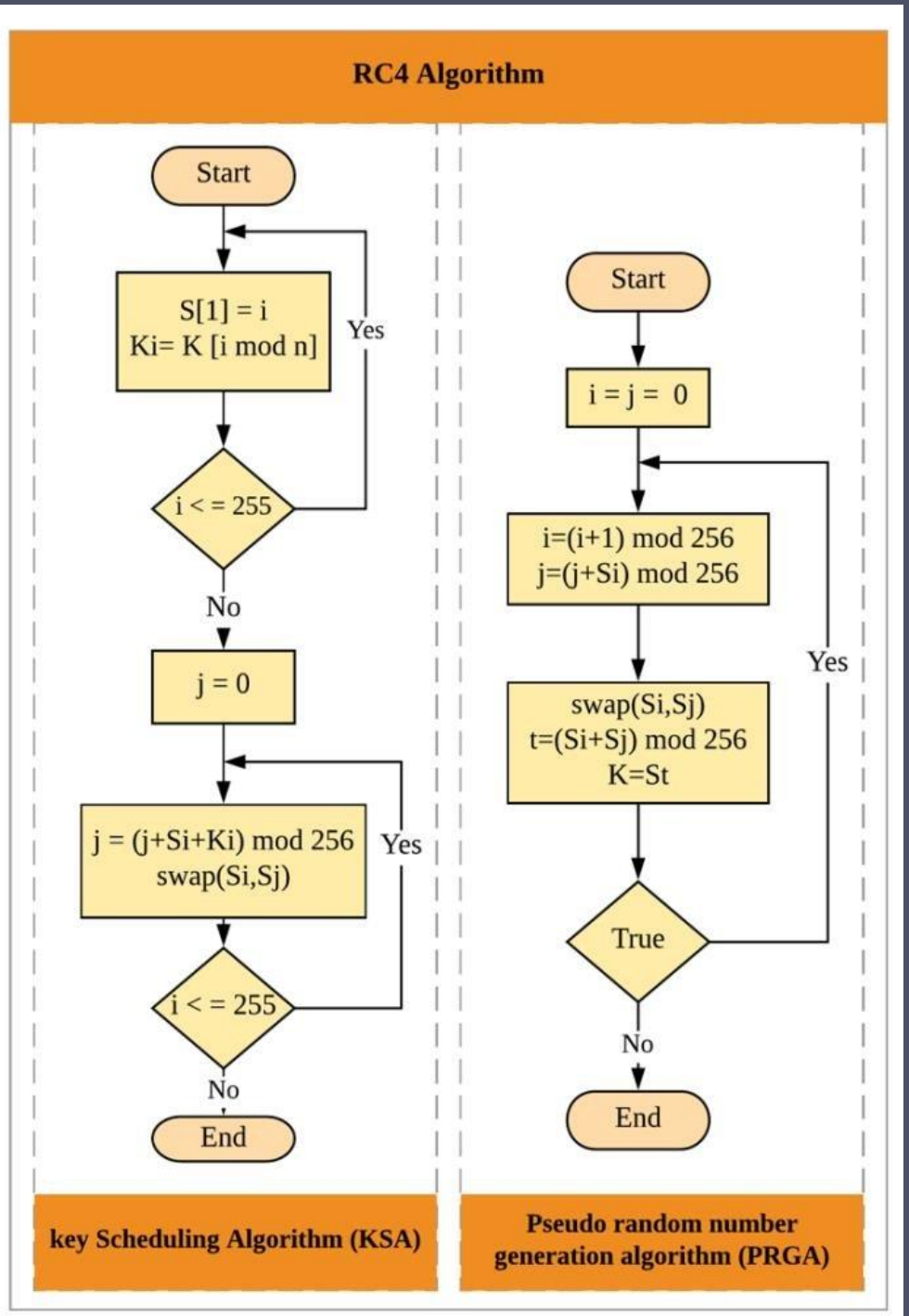


Figure 20.5 Performance Comparison of Symmetric Ciphers on a 3-GHz Processor


RC4 Algorithm
Start
S[1] = i
Ki= K [i mod n]
Yes
i < = 255
No
j = 0
j = (j+Si+Ki) mod 256
swap(Si,Sj)
Yes
i < = 255
No
End
key Scheduling Algorithm (KSA)
Start
i = j = 0
i=(i+1) mod 256
j=(j+Si) mod 256
swap(Si,Sj)
t=(Si+Sj) mod 256
K=St
Yes
True
No
End
Pseudo random number generation algorithm (PRGA)

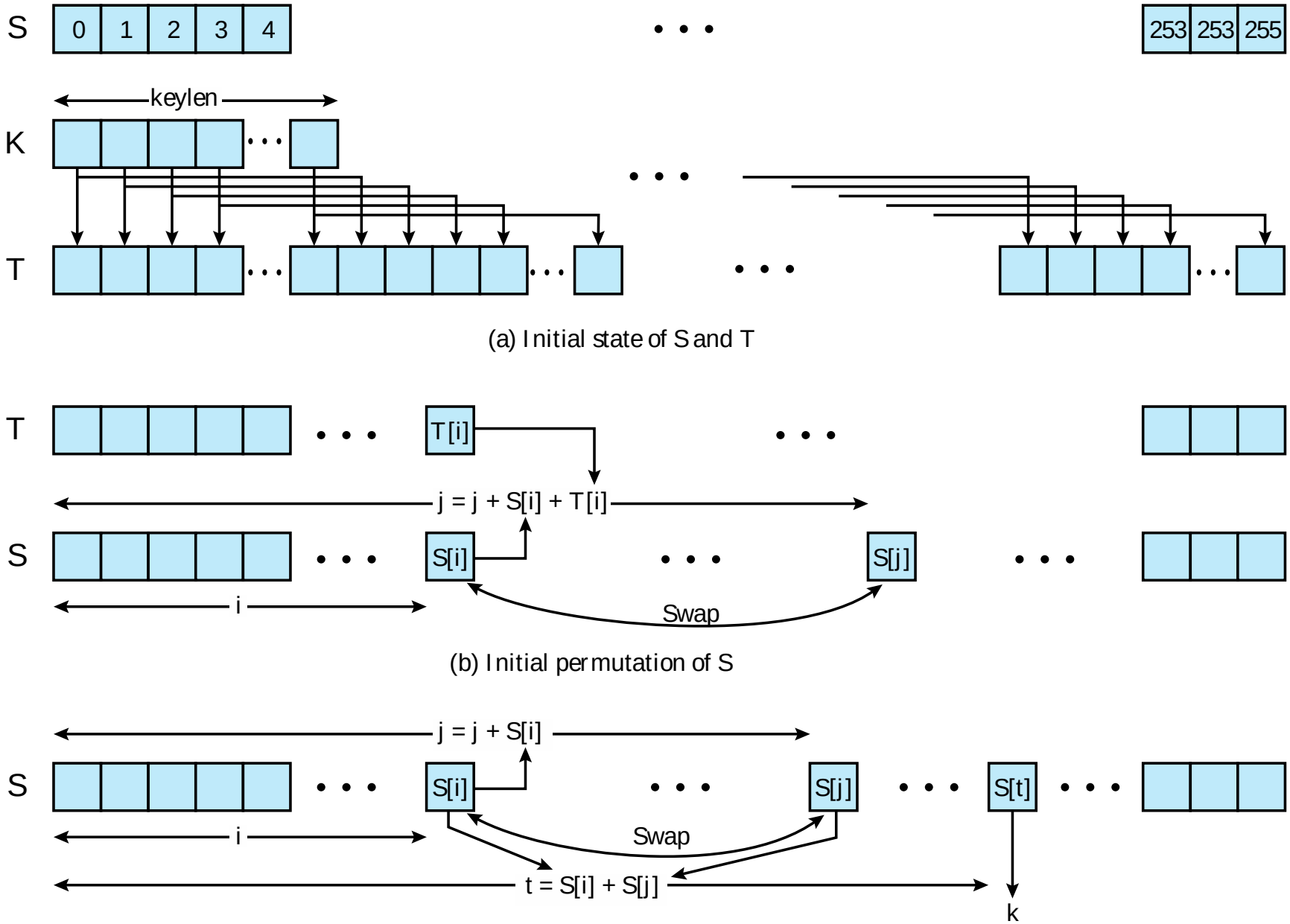


Figure 20.6 RC4

Blok Şifreleme Çalışma Modları

Mod	Tanım	Tipik Uygulama
Elektronik Kod kitabı (ECB)	64 düz metin bitlik her blok, aynı anahtar kullanılarak bağımsız olarak kodlanır.	• Tek değerlerin güvenli iletimi (ör. bir şifreleme anahtarı)
Şifreleme Blok Zincirleme (CBC)	Şifreleme algoritmasının girdisi, sonraki 64 bit düz metnin ve önceki 64 bit şifreli metnin XOR'udur	• Genel amaçlı blok yönelimli iletim • Kimlik Doğrulama
Şifreleme Geribildirimi (CFB)	Giriş, bir seferde s bit olarak işlenir. Önceki şifreli metin, sonraki şifreli metin birimini üretmek için düz metinle XOR'lanan sözde rasgele çıktı üretmek için şifreleme algoritmasına girdi olarak kullanılır.	• Genel amaçlı akış odaklı iletim • Kimlik doğrulama
Çıkış Geribildirimi (OFB)	CFB'ye benzer, tek farkı şifreleme algoritmasına girişin önceki DES çıkışı olmasıdır	• Gürültülü kanal üzerinden akış yönelimli iletim (örn. uydu iletişimi)
Sayaç (CTR)	Her düz metin bloğu, şifreli bir sayaçla XORlanır. Sayaç, sonraki her blok için artırılır.	• Genel amaçlı blok yönelimli iletim • Yüksek hız gereksinimleri için kullanışlıdır

Elektronik Kod Kitabı (ECB)

- En basit moddur
- Düz metin, her seferinde *b* bit olarak işlenir ve her blok aynı anahtar kullanılarak şifrelenir
- "Codebook" kullanılır çünkü her b bitlik düz metin bloğu için benzersiz bir şifreli metin vardır.
  - Tekrarlanan şifreli metinde tekrarlanan düz metin görüldüğü için uzun mesajlar için güvenli değildir
- Güvenlik eksikliklerinin üstesinden gelmek için, aynı düz metin bloğunun, tekrarlanırsa, farklı şifreli metin blokları ürettiği bir tekniğe ihtiyaç vardır.

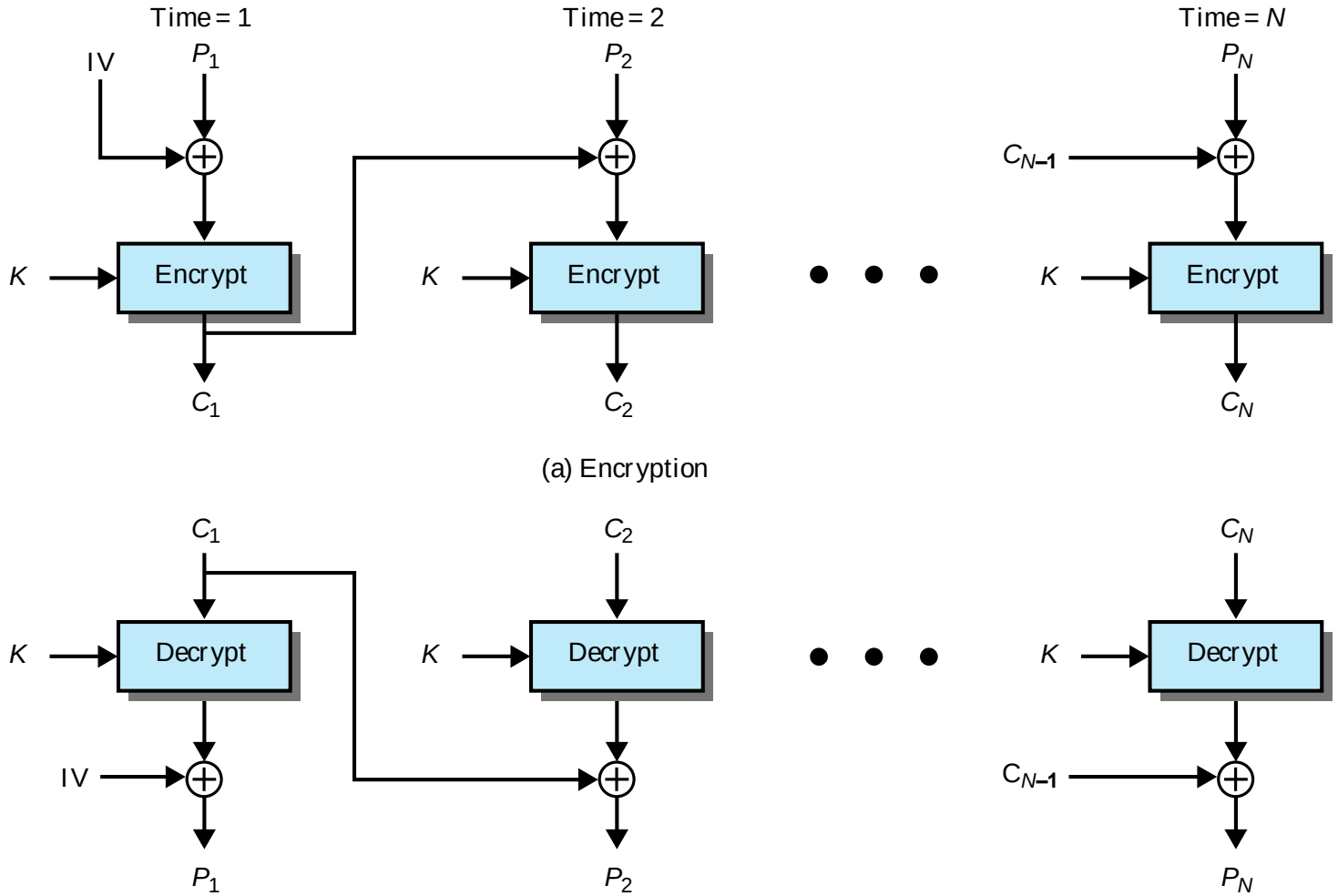


Figure 20.7 Cipher Block Chaining (CBC) Mode

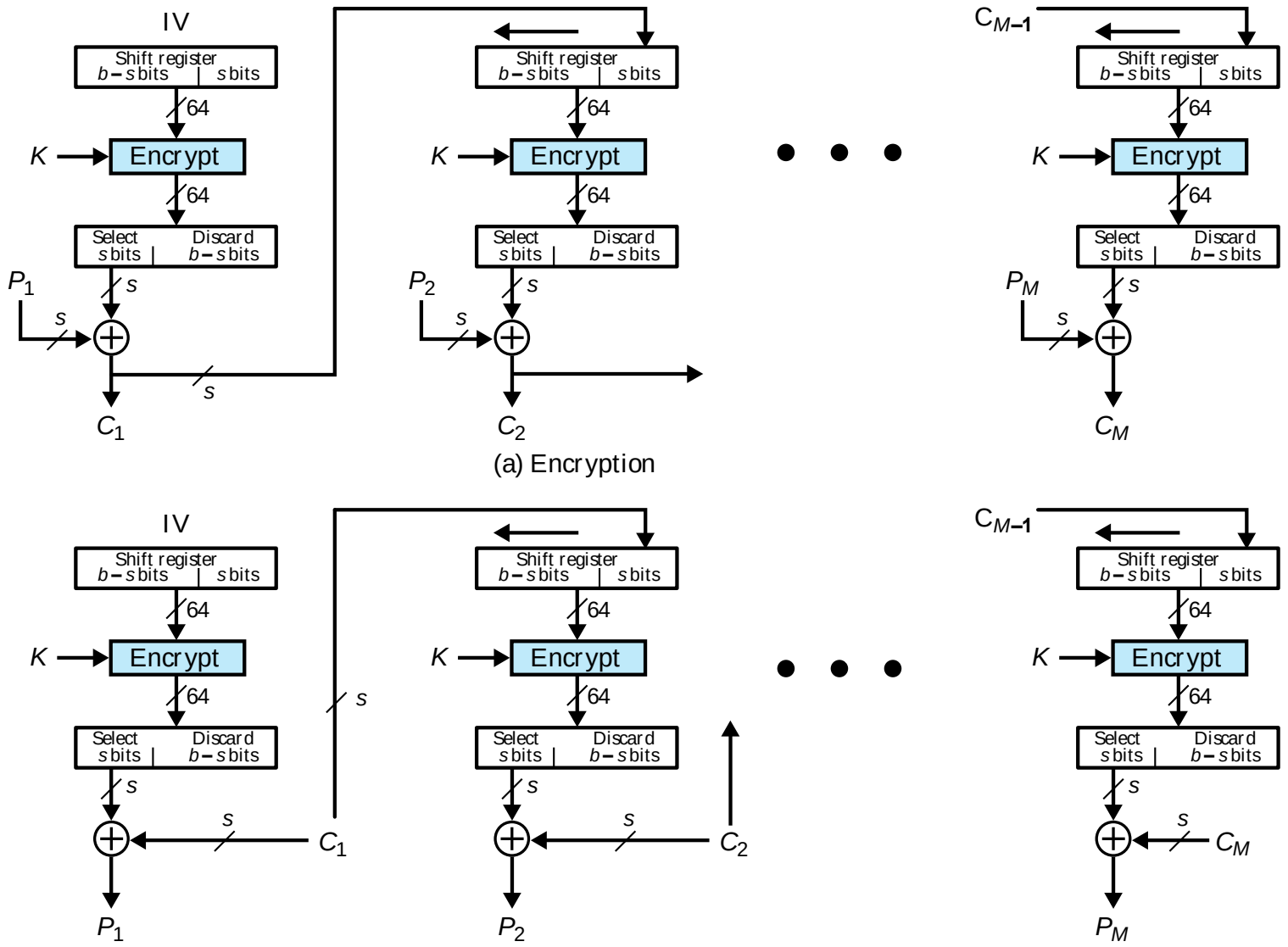


Figure 20.8 *s*-bit Cipher Feedback (CFB) Mode

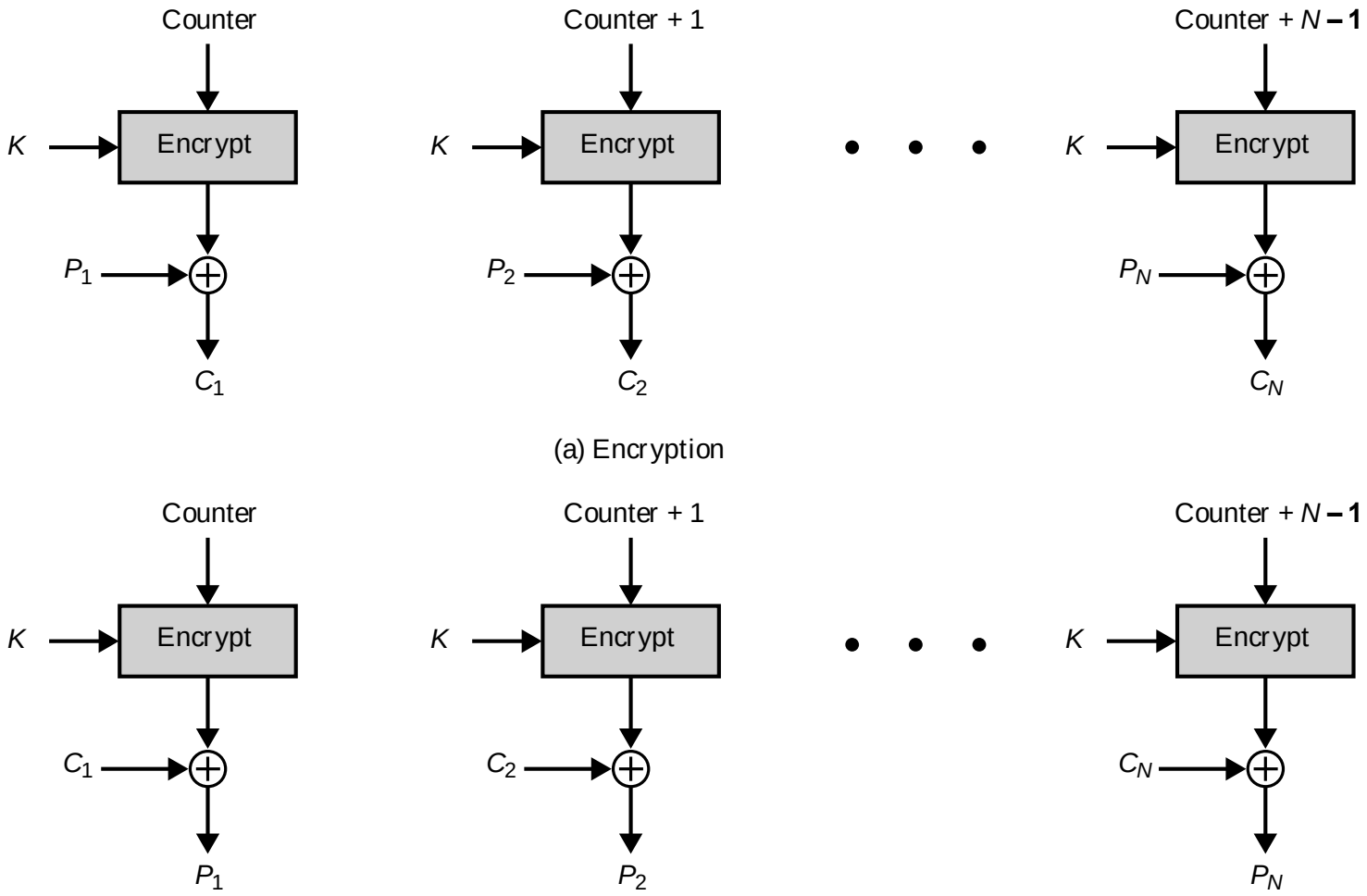


Figure 20.9 Counter (CTR) Mode

Anahtar Dağıtımı

- Başkalarının anahtarı görmesine izin vermeden veri alışverişi yapmak isteyen iki tarafa bir anahtar teslim etmenin yoludur
- İki taraf (A ve B) bunu şu şekilde başarabilir:

1. Bir anahtar A tarafından seçilebilir ve fiziksel olarak B'ye teslim edilebilir
2. Üçüncü bir taraf anahtarı seçebilir ve fiziksel olarak A ve B'ye teslim edebilir.
3. A ve B daha önce ve yakın zamanda bir anahtar kullanmışsa, taraflardan biri yeni anahtarı eski anahtar kullanılarak şifrelenmiş olarak diğerine iletebilir
4. A ve B'nin her birinin bir üçüncü taraf C ile şifreli bir bağlantısı varsa, C, A ve B'ye şifrelenmiş bağlantılarda bir anahtar teslim edebilir.

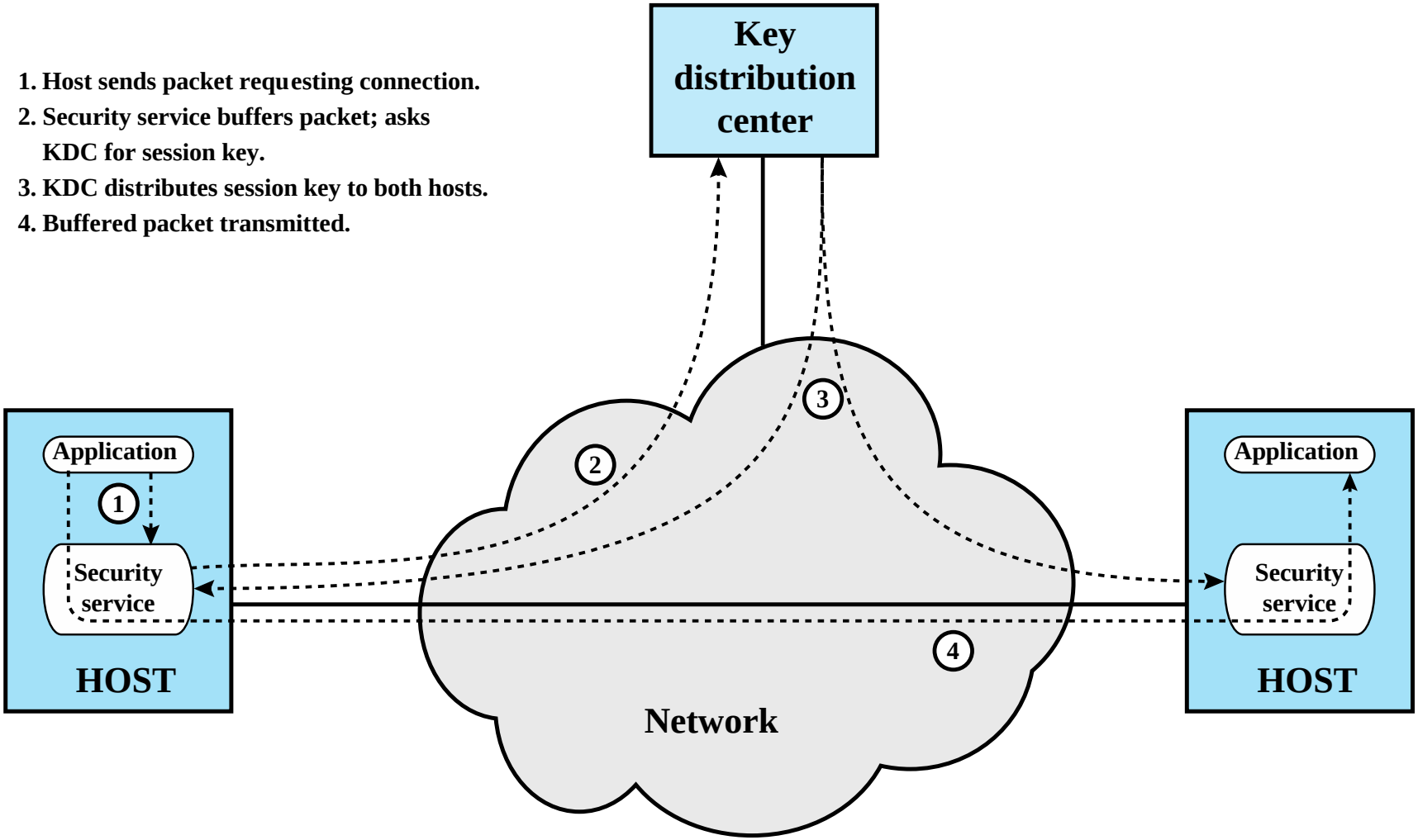


Figure 20.10 Automatic Key Distribution for Connection-Oriented Protocol