Chapter 20

Symmetric Encryption and Message Confidentiality

Cryptography

Classified along three independent dimensions:

The type of operations used for transforming plaintext to ciphertext

- Substitution – each element in the plaintext is mapped into another element
- Transposition – elements in plaintext are rearranged

The number of keys used

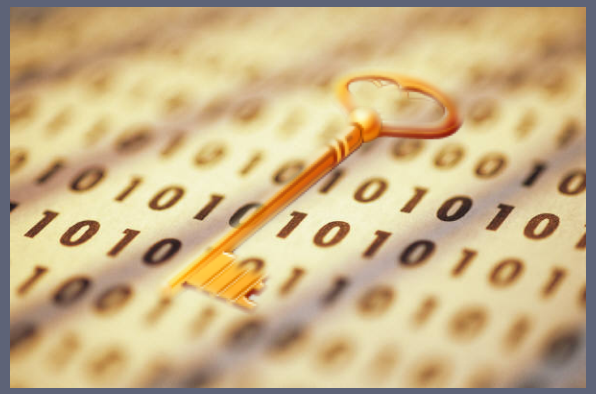
- Sender and receiver use same key – symmetric
- Sender and receiver each use a different key - asymmetric

The way in which the plaintext is processed

- Block cipher – processes input one block of elements at a time
- Stream cipher – processes the input elements continuously

Symmetric Encryption

- Also referred to as:
  - Conventional encryption
  - Secret-key or single-key encryption
- Only alternative before public-key encryption in 1970's
  - Still most widely used alternative
- Has five ingredients:
  - Plaintext
  - Encryption algorithm
  - Secret key
  - Ciphertext
  - Decryption algorithm



Transposition Cipher

- Columnar Transposition
- Write the message in a rectangle
- Example:

  Plaintext: attack postponed until two am

  Key: 4312567

	4	3	1	2	5	6	7
Encrypt:	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

  Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

- Detecting
  - Single letter frequencies match English frequencies,
  - Two or more letter frequencies do not

Substitution Ciphers

- Change characters in plaintext to produce ciphertext
- Example (Caesar cipher)
  - Uses a left shift of *k* to protect messages
  - Plaintext is HELLO WORLD
  - *K*=3: Change each letter to the third letter following it (X goes to A, Y to B, Z to C)
  - PT: 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
  - CT: 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
  - Ciphertext is KHOOR ZRUOG

How to break it? Brute Force.

- Ciphertext: phhw ph diwhu wkh wrjd sduwb
- This is only possible because:
  - The encryption / decryption algorithm is known
  - The small key space.
  - The plaintext language is known

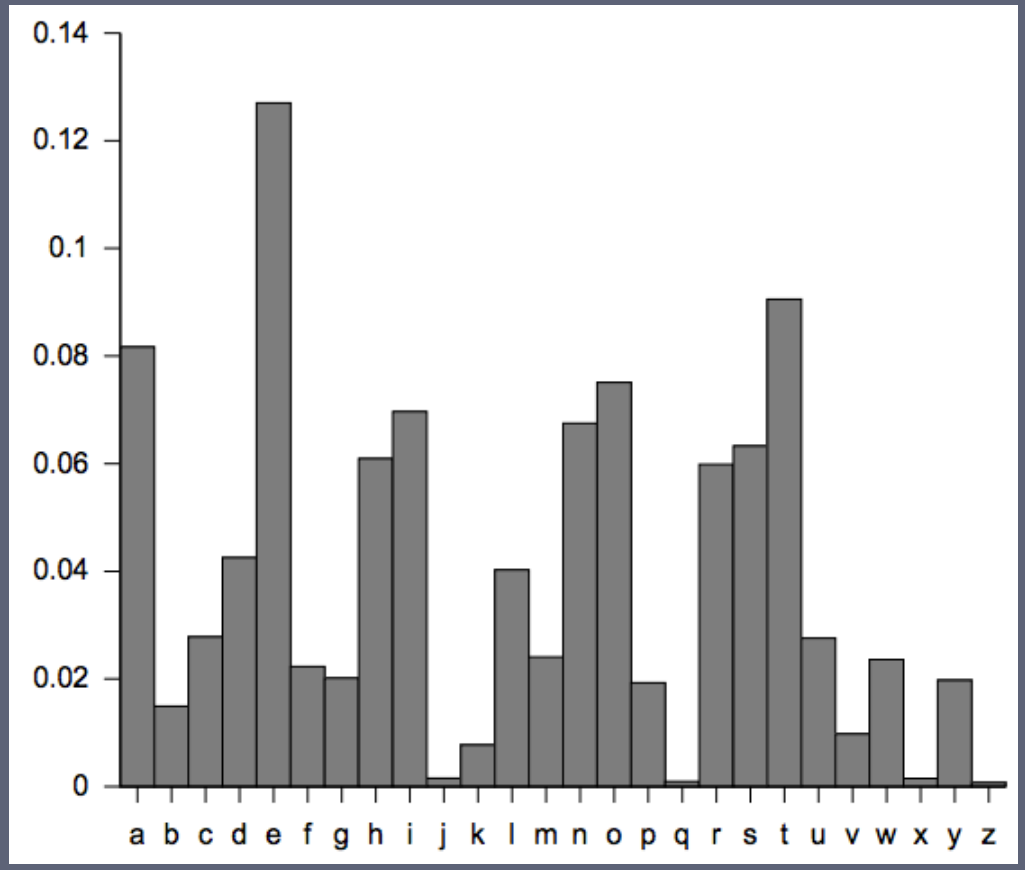
KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sqd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

How to break it? Statistical Attack.

- Susceptible to statistical attacks
- Statistical correlation function, OR
  - Find letter that has highest frequency.
  - Assume “e”.
  - Find distance from “e”
  - Decipher the rest of the message using distance as the key.

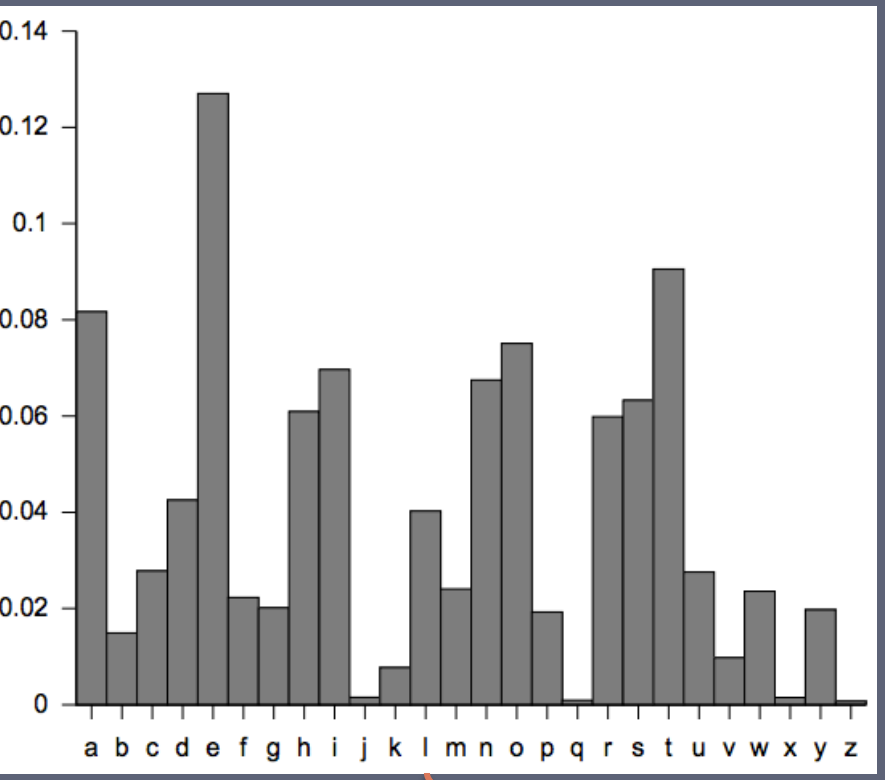
Transposition

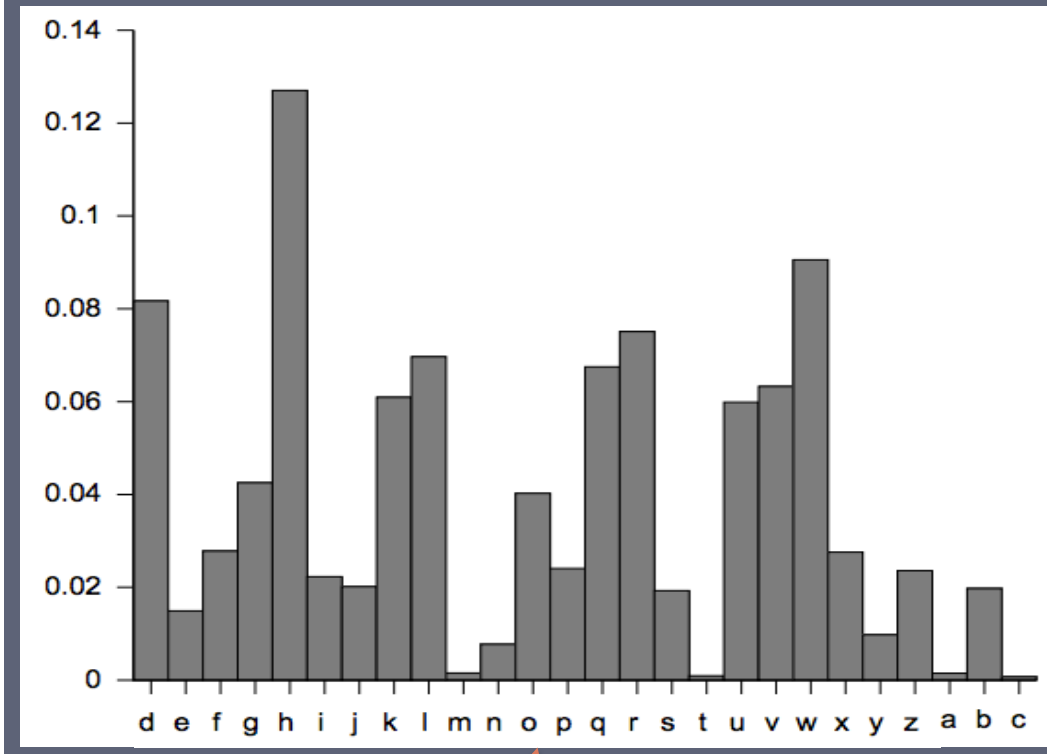
- Plaintext: **ATTACKP**OSTPONEDUNTILTWOAMXYZ
- Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ
-

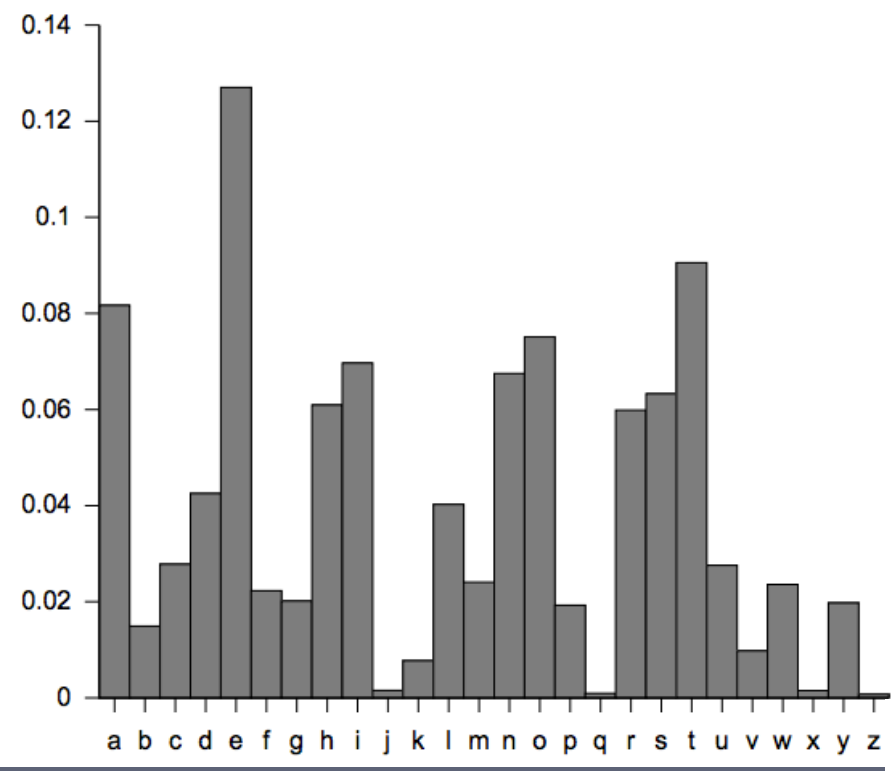


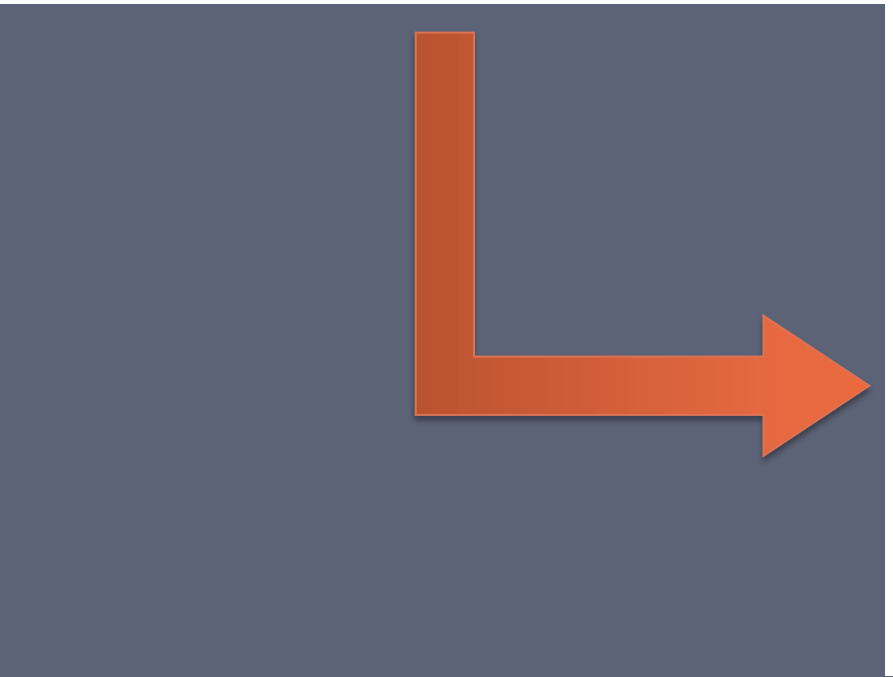
Substitution

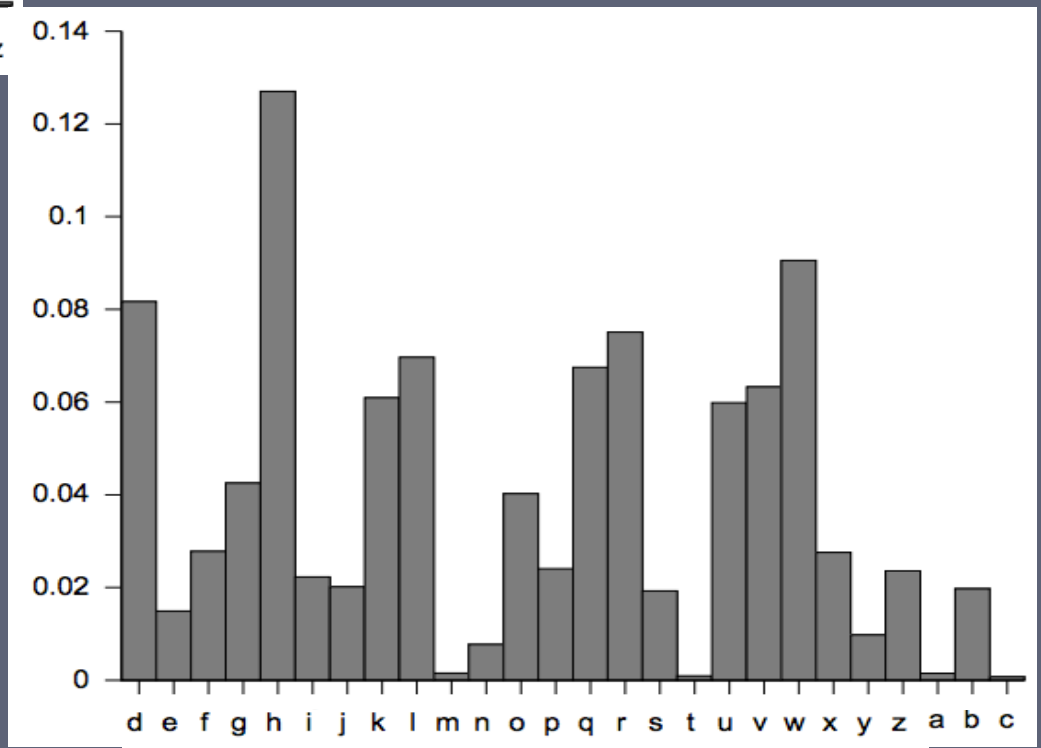
- Plaintext: HELLOWORLD
- Ciphertext: KHOORZRUOG






0.14
0.12
0.1
0.08
0.06
0.04
0.02
0
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




0.14
0.12
0.1
0.08
0.06
0.04
0.02
0
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

Possible direction for improvement

- Make key longer
  - Key space??
  - Does that solve the statistically exposed language statistics problem?
- Allow for arbitrary substitution
  - Keys space??
  - Does that solve the statistically exposed language statistics problem?
- Multiple letters in key
  - A cipher *is polyalphabetic* if the key has several *different* letters.
  - A cipher *is monoalphabetic* if the key has one letter.

Vigenère Cipher

- Pronounced "vedj-ih-nair"
- Like Caesar cipher, but use a string for key
- Example
  - Message THE BOY HAS THE BALL
  - Key V I G (21,8,6)
  - Encipher using Caesar cipher for each letter:

PT	T	E	S	T	T	H	E	C	I	P	H	E	R	T	X	T
K	V	I	G	V	I	G	V	I	G	V	I	G	V	I	G	V
CT	O	M	Y	O	B	N	Z	K	O	K	P	K	M	B	D	O

Vigenère Cipher

- Pronounced "vedj-ih-nair"
- Like Caesar cipher, but use a string for key
- Example
  - Message THE BOY HAS THE BALL
  - Key V I G (21,8,6)
  - Encipher using Caesar cipher for each letter:

PT	T	H	E	B	O	Y	H	A	S	T	H	E	B	A	L	L
K	V	I	G	V	I	G	V	I	G	V	I	G	V	I	G	V
CT	O	P	K	W	W	E	C	I	Y	O	P	K	W	I	R	G

The Target Cipher

- We want to break this cipher:

lvpsysrzwfxhsedgcysnwdeatjcdskzsrlftsqrfevznxccygkghsekwllsgsbsaevzpajsflrvsbyucsfdocsfpc
caddeswulndgboapeccnzfutnrkwlaevhcamwfdeulvppruwqitlvpslfoapvsfpdrkoehzfftnxtssi
evhsedgcytfhszpcwwyaesfconhoehrdcygkzsneelscowlvptisqvwyaqsbvyoyiekcftywfycyab
lhvsjjccgiosftgnuiwrehvnwpwzfvznxccygsmhcejarpnkkcqtfcmzaevcehvjqttzwgheiwomlvlc
reksgaetlonucsfgivotzrrtcftwgicmzfieejsfzuevgpvvfhsiilmewfsaxoevojszphsiilmewfhaptjmbo
apwjpnkkkprvzswdrlgnhfgzdaevafsvmadieboaaeovtlveoyydgfppvgdwekgcvielvpuemgf
acsgerffcxitszpvvfhltygapoigbdtiwsecfjbprjsteeiovtzqabratjcdskzsaatattckzsdhrvchedwfre
ugjpregfehvjbnacatzreaolnukcftywfyoiwuznnzscekzcfsrfrdowhszpcwoetvfrpdgsfeivkhzwrl
qstywsgeelhsewafdtkgoapvsftnkzsfnzlsoskshpsjabneeabptvwbyiewhjffmfpxgwfesnsfyeulvl
tygdpfldjtenwfdsygiwdeghaevjiaaklvpsbqkttygiesgwqtacnwpwzfupqladxeelgtntwzzoba
braklvpslfkttylvpnrcsoepwqlntsidesdwydewgddvjsvrrdgeoesdcowwgdiffowpyghzgisdseik
otdywideuskpluabrfzdhprkgqlpkmfpauafpcknwpwfxsnlzhgpielvpffghsicdglbfnszrfnwwlvuo
wiwgfyirzsdhrjsotywdsokgcycefwceggfenflwygkzscakzscscaadwrlvzfkzsrlftshhfucfluksptyw
wxpruhzfkzspccaddeiszdtffgliuzshaelsotfwblbcwhseiwgeowlvpwfjzotfksphfoqwerjwelfgyp
dkghsojwcqujovzwvjsqoiliyakwsyolyveojwsttkzsdlznscowkiysyabptywberrnsweukcftywodtr
ufzsjusytiszyemsrlsfmhseifieaysbonfjhseifociqgblaevhseefshmvpwnozldlsjwrzvvjowbliiprhms
yenesiitgomollgpvvfhsiilmqoljdxnzfsehzjhjffmfamvlppffjsaekwftnxgieerkhzfcmpmotchpxrko
ncfjrtnxlcyajs

Attack the Cipher by Recognizing repetitions

- Notice cipher

PT	T	H	E	B	O	Y	H	A	S	T	H	E	B	A	L	L
K	V	I	G	V	I	G	V	I	G	V	I	G	V	I	G	V
CT	O	P	K	W	W	E	C	I	Y	O	P	K	W	I	R	G

- Can be a coincidence:
- K : 2 1 3
- PT: B A D
- CT: D B G

- K : 3 2 1
- PT: A Z F
- CT: D B G

Attack the Cipher by Recognizing repetitions

- We want to break this cipher:

lvpsysrzwfxhsedgcysnwdeatjcdskzsrlftsqrfevznxccygkghsekwllsgsbsaevzpajsflrvsbyucsfdocsfpc
caddeswulndgboapeccnzfutnrkwlaevhcamwfdeulvppruwqitlvpslfoapvsfpdrkoehzfftnxtssi
evhsedgcytfhszpcwwyaesfconhoehrdcygkzsneelscowlvptisqvwyaqsbvyoyiekcftywfycyab
lhvsjjccgiosftgnuiwrehvnwpwzfvznxccygsmhcejarpnkkcqtfcmzaevcehvjqttzwgheiwomlvlc
reksgaetlonucsfgivotzrrtcftwgicmzfieejsfzuevgpvvfhsiilmewfsaxoevojszphsiilmewfhaptjmbo
apwjpnkkkprvzswdrlgnhfgzdaevafsvmadieboaaeovtlveoyydgfppvgdwekgcvielvpuemgf
acsgerffcxitszpvvfhltygapoigbdtiwsecfjbprjsteeiovtzqabratjcdskzsaatattckzsdhrvchedwfre
ugjpregfehvjbnacatzreaolnukcftywfyoiwuznnzscekzcfsrfrdowhszpcwoetvfrpdgsfeivkhzwrl
qstywsgeelhsewafdtkgoapvsftnkzsfnzlsoskshpsjabneeabptvwbyiewhjffmfpxgwfesnsfyeulvl
tygdpfldjtenwfdsygiwdeghaevjiaaklvpsbqkttygiesgwqtacnwpwzfupqladxeelgtntwzzoba
brаklvpslfkttylvpnrcsoepwqlntsidesdwydewgddvjsvrrdgeoesdcowwgdiffowpyghzgisdseik
otdywideuskpluabrfzdhprkgqlpkmfpauafpcknwpwfxsnlzhgpielvpffghsicdglbfnszrfnwwlvuo
wiwgfyirzsdhrjsotywdsokgcycefwceggfenflwygkzscakzscscaadwrlvzfkzsrlftshhfucfluksptyw
wxpruhzfkzspccaddeiszdtffgliuzshaelsotfwblbcwhseiwgeowlvpwfjzotfksphfoqwerjwelfgyp
dkghsojwcqujovzwvjsqoiliyakwsyolyveojwsttkzsdlznscowkiysyabptywberrnsweukcftywodtr
ufzsjusytiszyemsrlsfmhseifieaysbonfjhseifociqgblaevhseefshmvpwnozldlsjwrzvvjowbliiprhms
yenesiitgomollgpvvfhsiilmqoljdxnzfsehzjhjffmfamvlppffjsaekwftnxgieerkhzfcmpmotchpxrko
ncfjrtnxlcyajs

Attack the Cipher by Recognizing repetitions

Find Repeated Sequences

Vigenere Repeat Distance: Repeated Sequence	Spacing	Possible length of key (or factors) 02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
LVP	130	x			x					x			x							
LVP	10	x			x					x										
LVP	75		x		x										x					
LVP	265				x															
LVP	290	x			x					x										
LVP	50	x			x					x										
LVP	10	x			x					x										
LVP	120	x	x	x	x	x		x		x		x			x					x
LVP	165		x		x						x				x					
JFFMF	635				x															
AKLVP	50	x			x					x										
KLVPS	50	x			x					x										

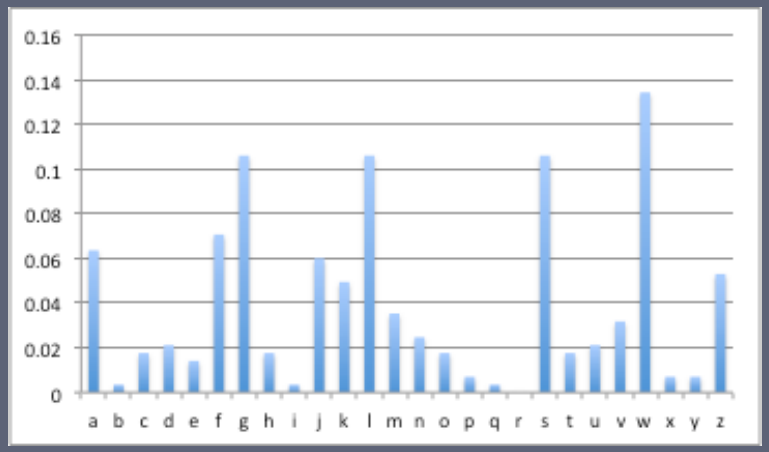
http://www.simonsingh.net/The_Black_Chamber/vigenere_cracking_tool.html

Attacking the Cipher Caesar Frequency Analysis

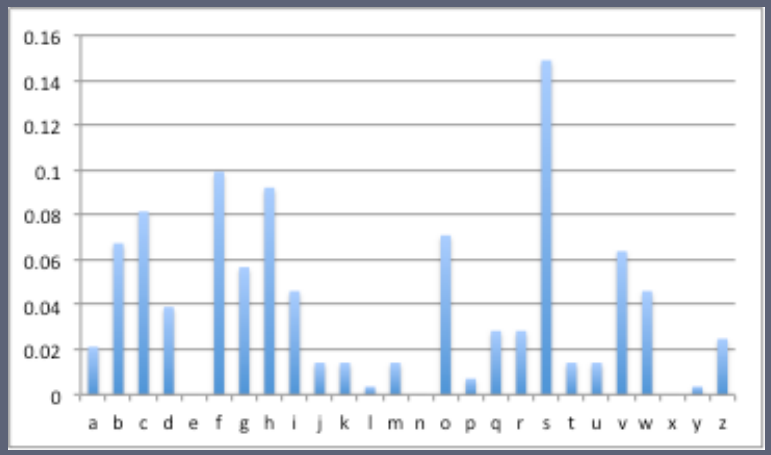
- lsxgwjztecgwsvssssawgefkvwlulfskftvghwshdzllsaykwasgtwnfcmakcvjwwlslsotgf svflsvplhmwkzlgvmboeggglmsfsfggwjsoajzazvwggjaakwwzzfhwfsklwlagszlsaaw wmwslgdwggjlqgwnfalwalflcwsdwjdswfgskwsadgmanxhlgdnnugzjwgfglzzalztu kwuzasfzlwwwljkojggwojlwywznkawnkwuussmfsjfgvfplwjimeglfljfjmljwgkmckjls
- vrhcdcssvchlbzfbffdubcuwhfvwvofofshcswfocssvqqocfbjigrwvchrcmcqgocgo ftciifghmaohmabjksgzaaovofdcvggczhabsbtvbcstscfjfbtocfuscrsorfhqshfofssh bbbhfffvdjfihivkiqwudgzbvkvsqiwgsgdgohdoikbhqffwsgvhgswofssdcwfwssavss cswhsdzgssbhgvzsqwyhcvsisvsssibbscofszrhibhobhswdroissoghmdshfpsfihphorc
- pzsyedrqzyslsplydpdloctlcdpqpapetssyzyceyncpvsyfyljonepzycpqzethmrangzf cezpsexjsepoppwndfdatypwvpfexplpdepetrdatdhrpenzlfyzcfdzepezsgsdatfo pnpyjpeylptdwaaptetppxtzrptpoldydvecdwzstdprplpppnppslzwwydosyceycc dzrhfpxzpddlholsepopwepsqzqyyetdcypewfdzyylseosclshnlzwpyimpsqxejapat ezmpnty
- lwesaslrngesaaruocenannaaepispdhnietpaohgeotwbitchcsuhwngentahtelee uirtmeuviwosiwtanrdhasialypeiuarivtotcrezasacheerharntonesoptdiwteetpnns setifxsetfesdeastsawqenoastneneddrooipgedelfrpacwlifibrliihtocengaswflhltpf cetiatbeowtheldouwoaootlostrettsteseaneiaemosvbreiovionhfmfenefoxcna
- yfdntkffxkkgejvcccsdpzremurtlvrzxedfcenrkewiyveyyvcfivzxsjkfevzivktcvrwzjevif ezifjpkvrfeveevdvkeecftvyiifjiqtktkrduevceuyinkrwcvgvryewkvkzkjevefgnuylnye vkbygczletbklyrptsevrewfyiiyuuzkkukfzefcffvwrrykegfkkcrkffuyrkcifuefciwfffrfkjjvi kljkzwyyruyrjimfiyfiqeevzjvlhntlvilzzfvfkxrctrfxj

Attacking the Cipher
Caesar Frequency Analysis

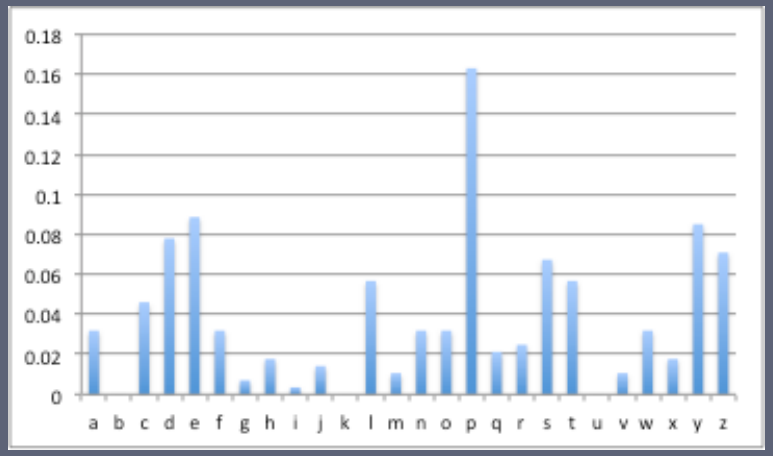
Set 1



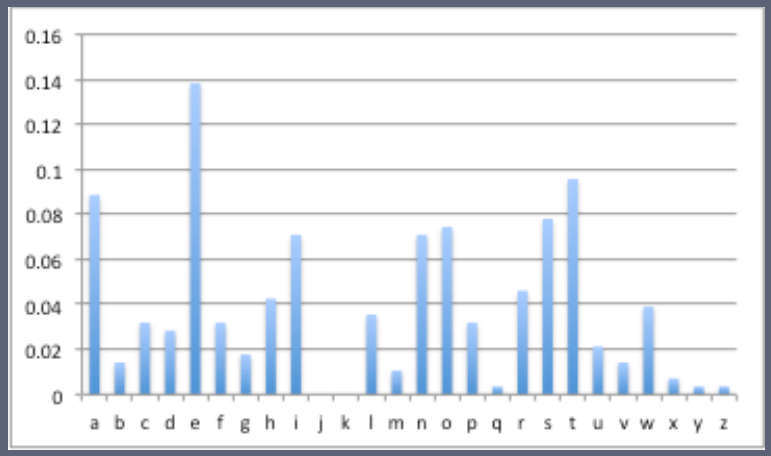
Set 2



Set 3

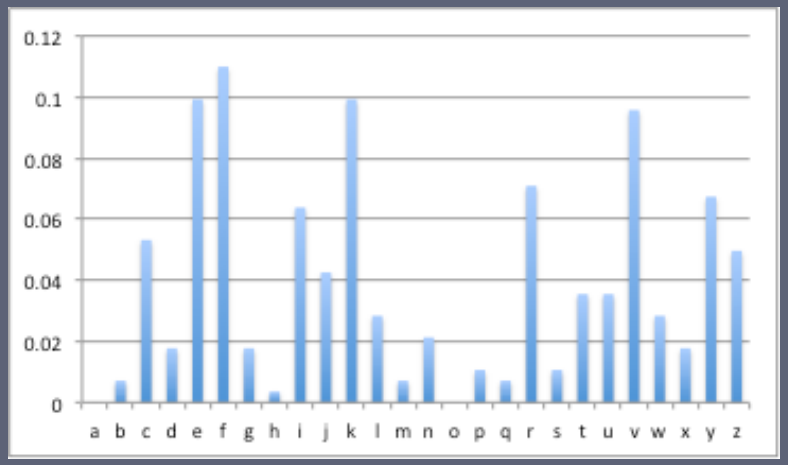


Set 4



Attacking the Cipher Caesar Frequency Analysis

Set 5



- So the key is "solar"

theshadowofthemoonsweptacrosstheglobefromhongkongtothetexaspanhandleasarareannularsolareclipsebeganmondaymorningi
nasiaandtraversedthepacificthesunappearedasathinringbehindthemoontopeopleinanarrowpathalongthecenterofthetrackwhichbe
ganinsouthernchinaheavycloudsobscuredtheviewinhongkongbutresidentsoftokyoandothercitieswereabletogetaspectacularviewfo
raboutfourminutesaroundseventhirtytwoammondaysixthirtytwopmetsundayeventswereheldatschoolsandmuseumsinjapanwhile
manymorepeopletookintheunusualastronomicaleventathomeoronstreetcornersafterwhizzingacrossthepacifictheshadowemerged
overnortherncaliforniaandsouthernoregonwherethousandsofpeopleattendedpartiestowatchtheeventthefirsttoappearintheuniteds
tatessincenineteenninetyfourexpertswarnedthathopefulviewersshouldnotpeerupattheskywithoutspecialviewingequipmentsincelo
okingatthesunwiththenakedeyecancauseblindnessderekralstonaprofessionalphotographersaidheusedaweldingfiltertocaptureadir
ectviewofeclipseinthefoothillsaboveorovillecaliforniahesharedthephotooncnnireportnotingtheratherslimswathoftheglobewhocoul
dseetheimpactoftheeclipseralstonsaidhewantedtoenabletherestoftheworldtoseehowclearitlookedtothoseofuswhowerefortunatee
noughtoseeitthesliverofsunshinethentraveledsoutheastacrosscentralnevadasouthernutahandnorthernarizonaandthennewmexicoi
tpassedoveralbuquerquenewmexicoaboutseventhirtyfourpmninethirtyfourpmetbeforepeteringouteastoflubbocktexasaccordingto
nasa

One-Time Pad

- A Vigenère cipher with:
  - A random key at least as long as the message
  - Encrypts/decrypts a single message
- Ciphertext is random and bears no statistical relationship to plaintext
- Provably unbreakable

One-Time Pad

- Ciphertext
  - ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
- KEY
  - PXLMVMSYDOFUYRVZWCTNLEBNECVGDUPAHFZZLMNYIH
- PLAINTEXT
  - MR MUSTARD WITH THE CANDLESTICK IN THE HALL

One-Time Pad

- Ciphertext
  - ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
- KEY
  - MFUGPMIYDGAXGOUFHKLLLMHSQDQOGTEWBQFGYOVUHWT
- PLAINTEXT
  - MISS SCARLET WITH THE KNIFE IN THE LIBRARY
- Which one is the correct key?
- Which one is the more likely key?

One-Time Pad

- In practice
  - Making large quantities of truly random keys
  - Key distribution and protection
    - For every message an equally long key needs to be sent to the receiver.
- Hence, mechanism is of limited utility

Rotor Machines

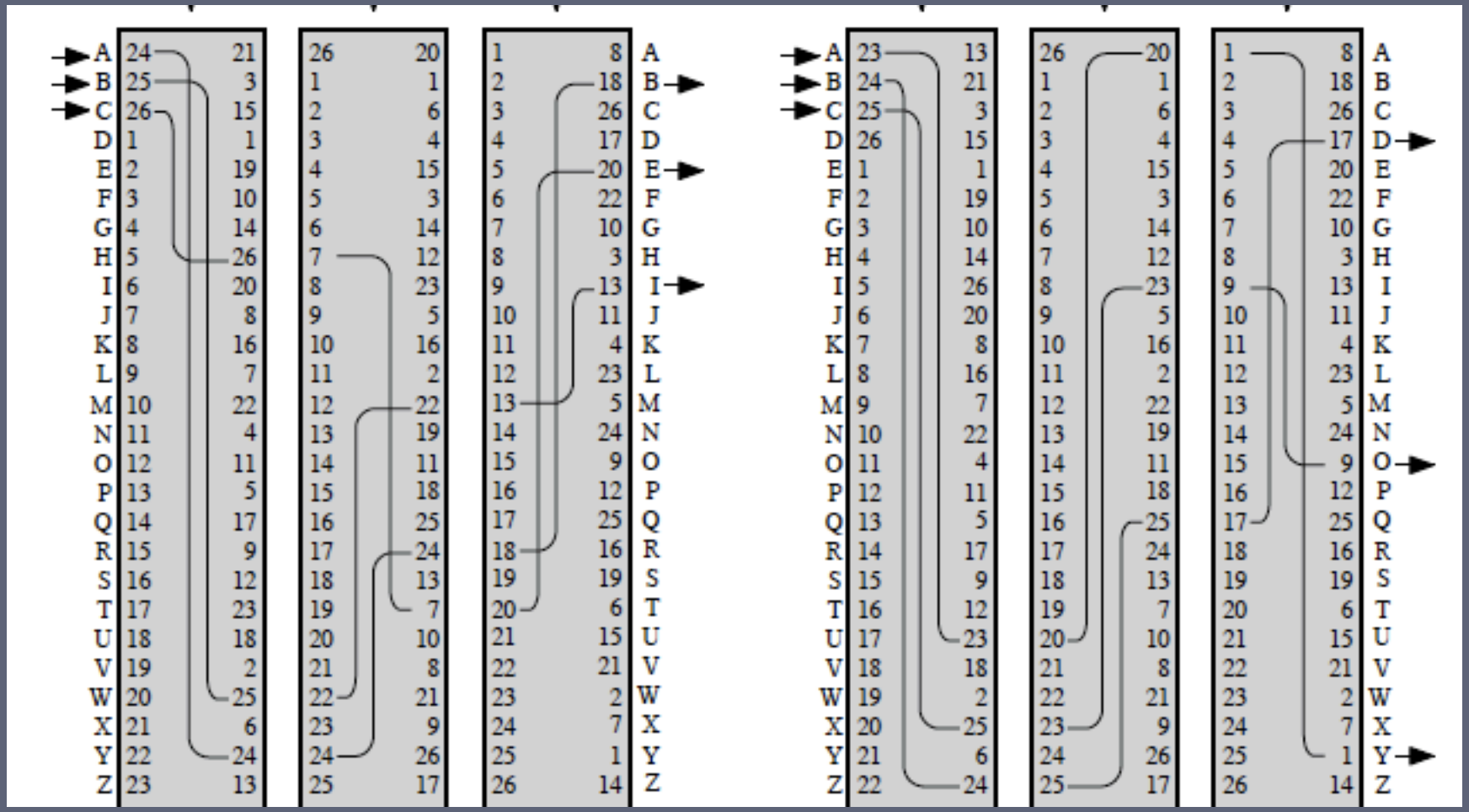


Table 20.1 Types of Attacks on Encrypted Messages

Type of Attack	Known to Cryptanalyst
Ciphertext only	•Encryption algorithm •Ciphertext to be decoded
Known plaintext	•Encryption algorithm •Ciphertext to be decoded •One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	•Encryption algorithm •Ciphertext to be decoded •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Computationally Secure Encryption Schemes

- Encryption is computationally secure if:
  - Cost of breaking cipher exceeds value of information
  - Time required to break cipher exceeds the useful lifetime of the information
- Usually very difficult to estimate the amount of effort required to break
- Can estimate time/cost of a brute-force attack

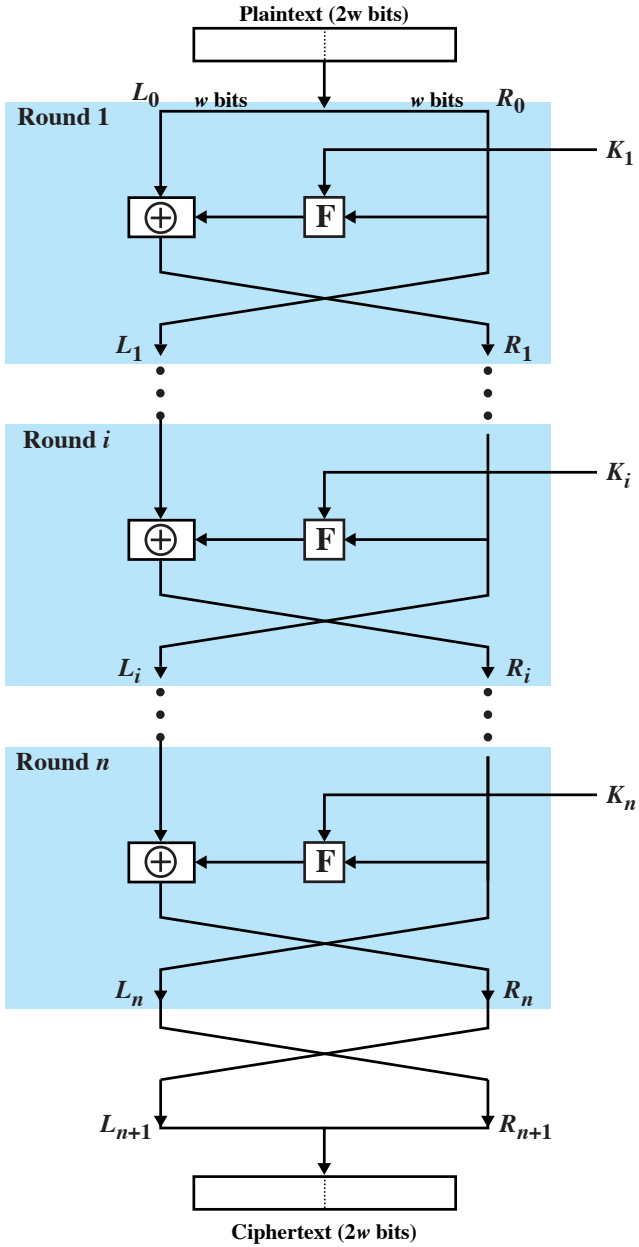
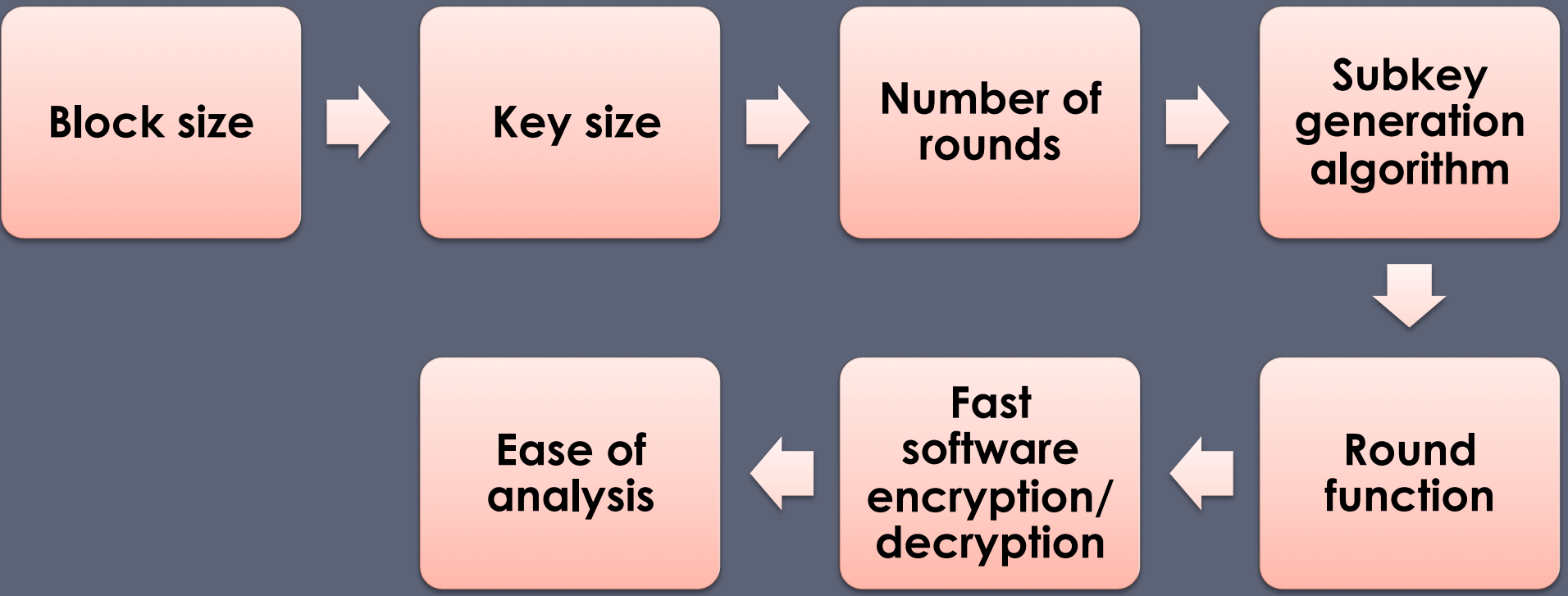


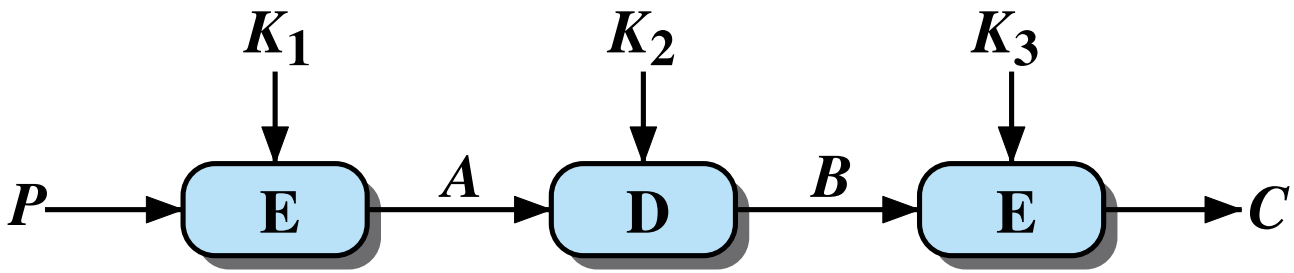
Figure 20.1 Classical Feistel Network

Block Cipher Structure

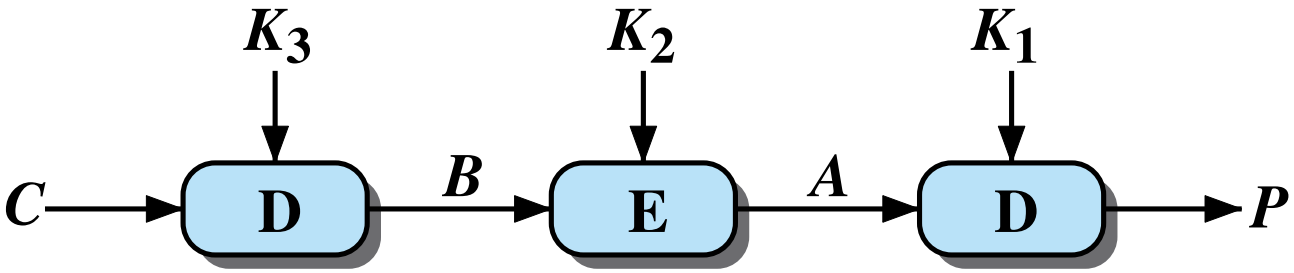
- Symmetric block cipher consists of:
  - A sequence of rounds
  - With substitutions and permutations controlled by key
- Parameters and design features:



- Most widely used encryption scheme
- Adopted in 1977 by National Bureau of Standards (Now NIST)
- FIPS PUB 46
- Algorithm is referred to as the Data Encryption Algorithm (DEA)
- Minor variation of the Feistel network

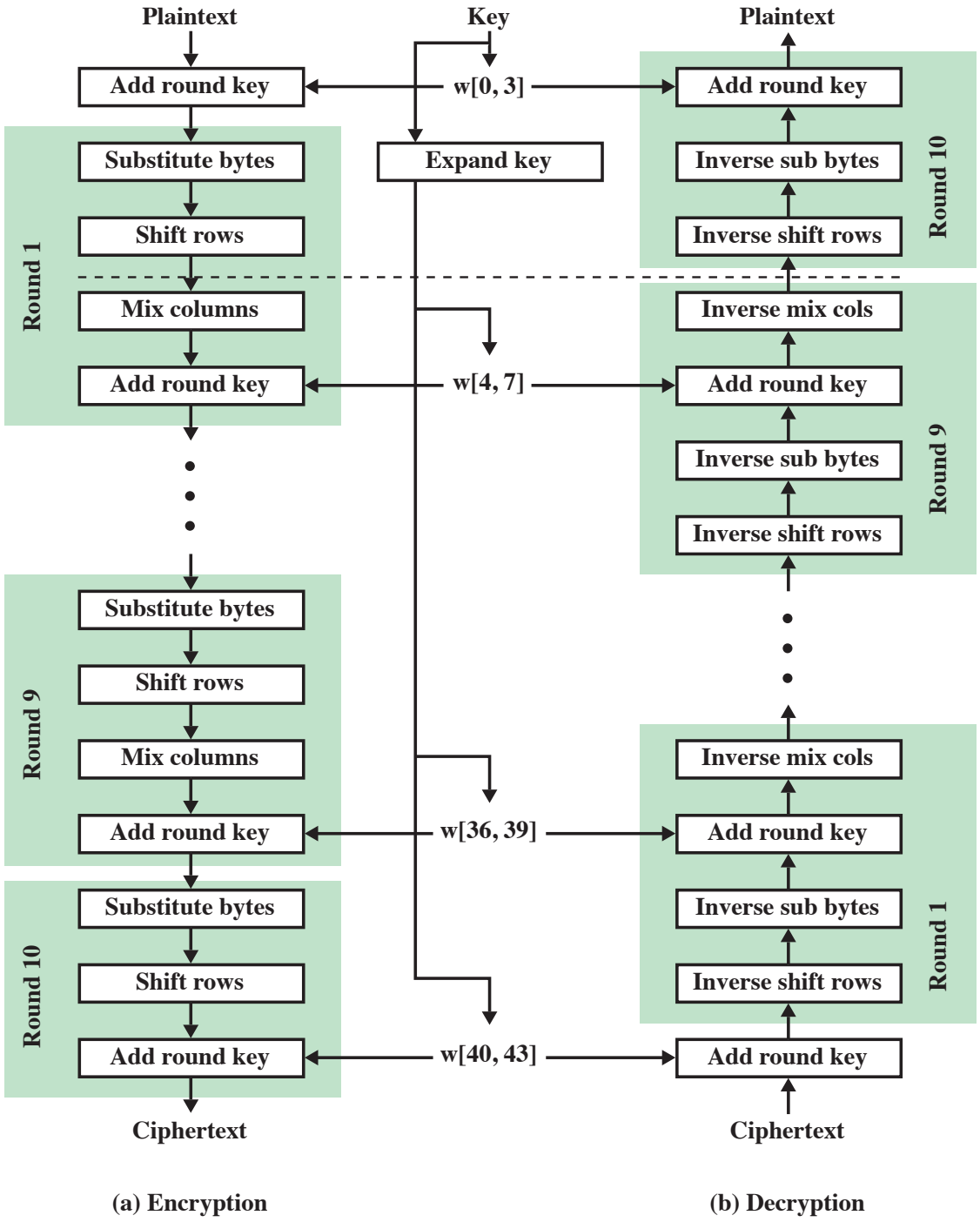


(a) Encryption



(b) Decryption

Figure 20.2 Triple DES



AES

- U.S. FIPS PUB 197
- Block cipher
- Three different key sizes: 128, 192, 256
- 10 rounds
- S-Boxes

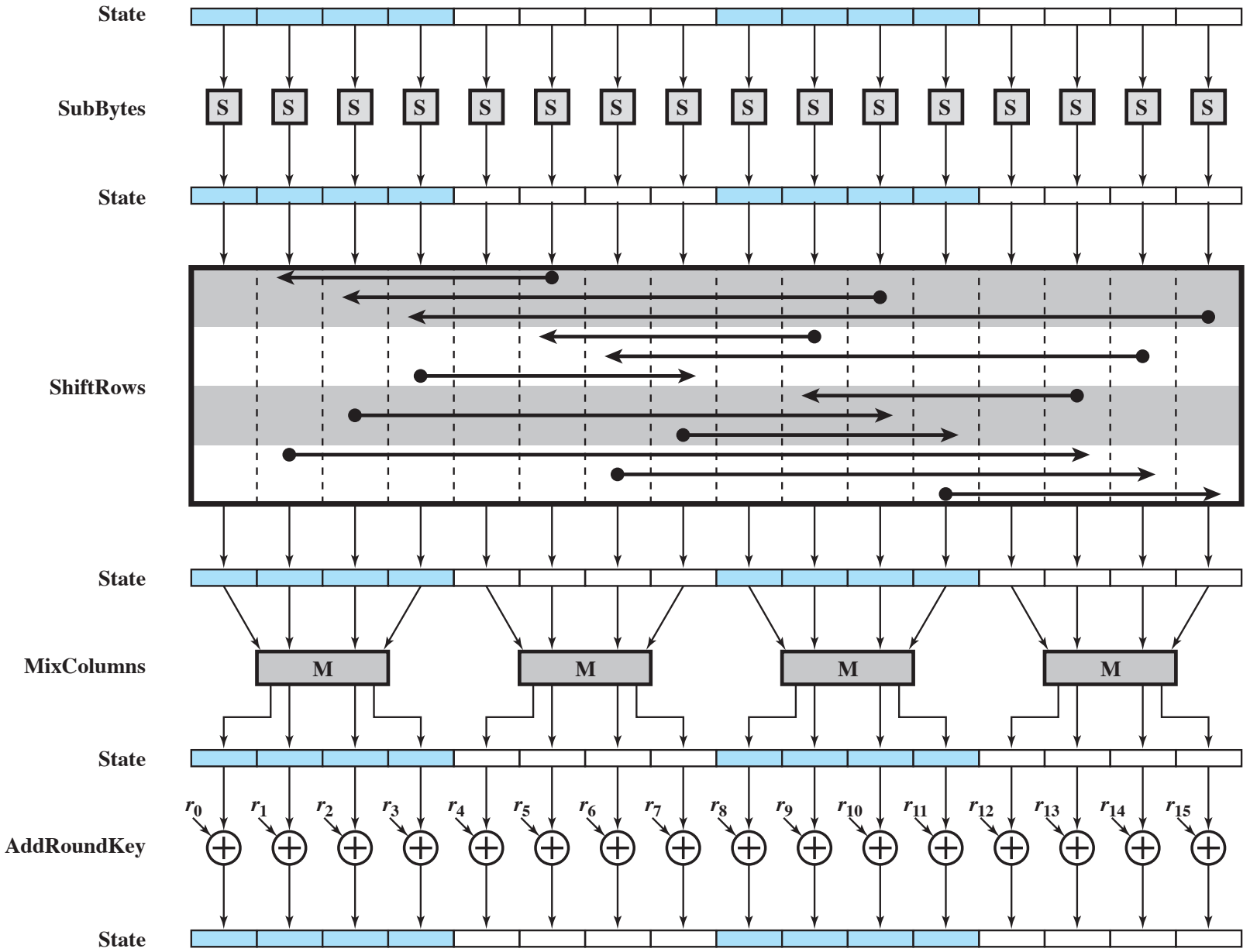


Figure 20.4 AES Encryption Round

Table 20.2 AES S-Boxes

(a) S-box

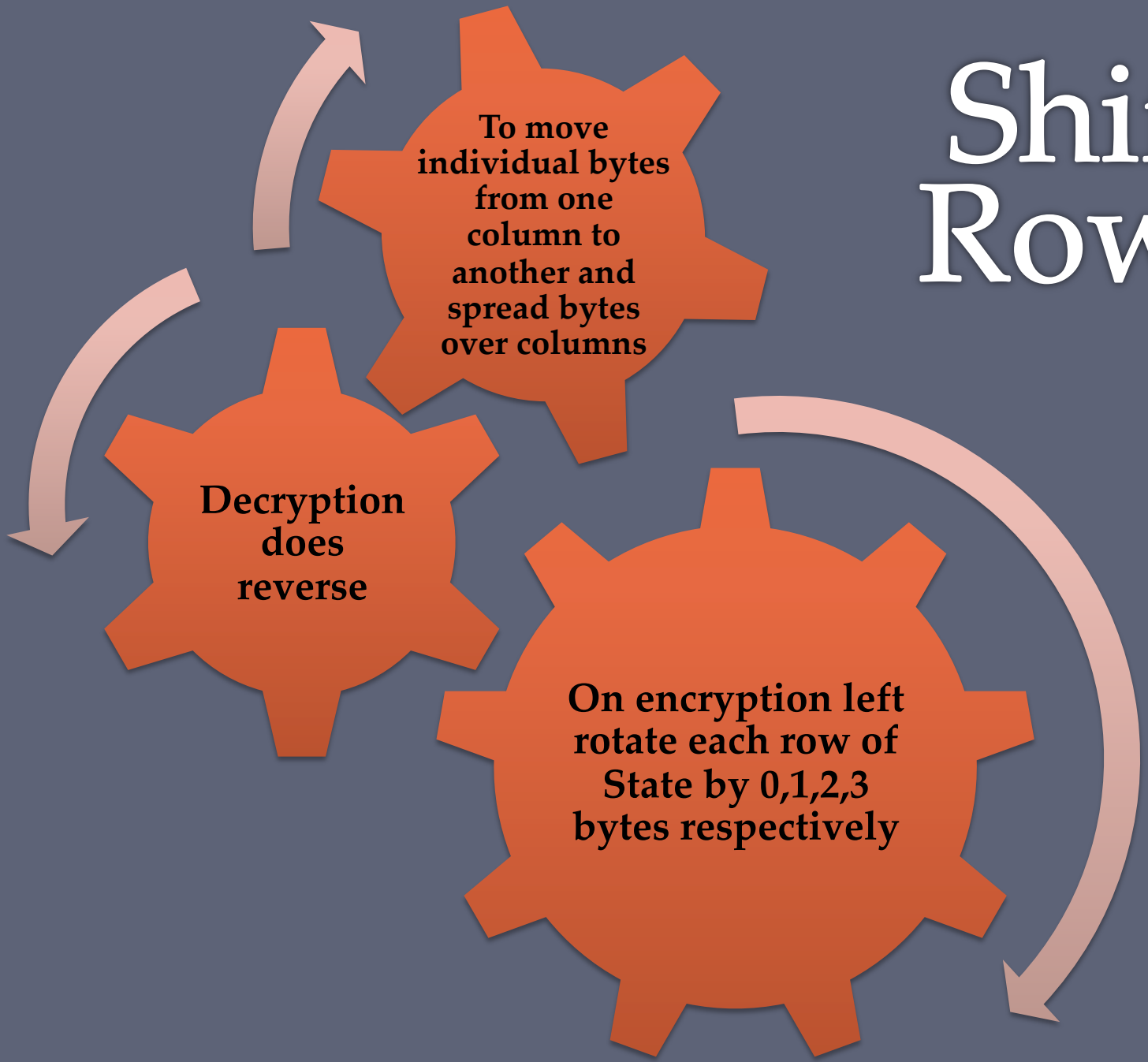
		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	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

Table 20.2 AES S-Boxes

(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

Shift Rows

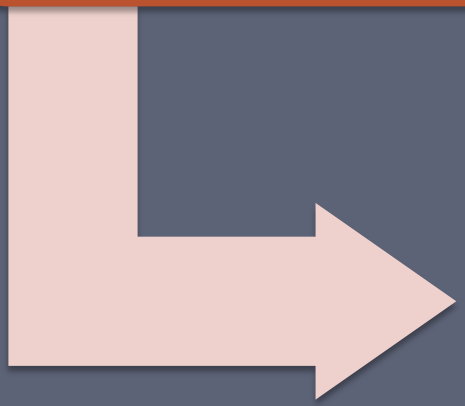

To move individual bytes from one column to another and spread bytes over columns
Decryption does reverse
On encryption left rotate each row of State by 0,1,2,3 bytes respectively

Mix Columns and Add Key

- Mix columns
  - Operates on each column individually
  - Mapping each byte to a new value that is a function of all four bytes in the column
  - Use of equations over finite fields
  - To provide good mixing of bytes in column
- Add round key
  - Simply XOR State with bits of expanded key
  - Security from complexity of round key expansion and other stages of AES

Stream Ciphers

Processes input elements continuously



Key input to a pseudorandom bit generator

- Produces stream of random like numbers
- Unpredictable without knowing input key
- XOR keystream output with plaintext bytes

Table 20.3 Speed Comparisons of Symmetric Ciphers on a Pentium 4

Cipher	Key Length	Speed (Mbps)
DES	56	21
3DES	168	10
AES	128	61
RC4	Variable	113

Source: http://www.cryptopp.com/benchmarks.html

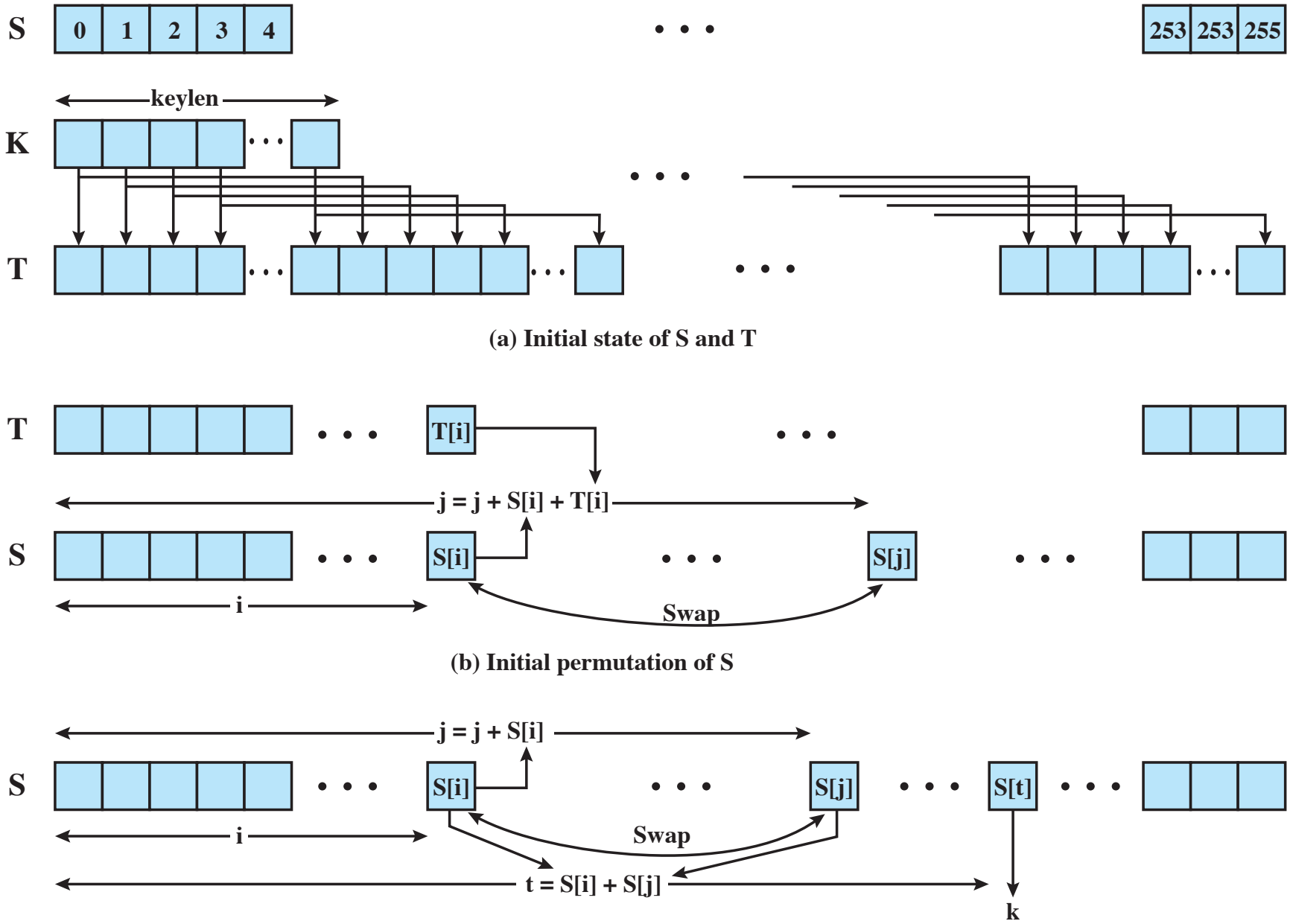


Figure 20.5 RC4

Table 20.4
Block Cipher Modes of Operation

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 plaintext bits is encoded independently using the same key.	•Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	•General-purpose block-oriented transmission •Authentication
Cipher Feedback (CFB)	Input is processed *s* bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	•General-purpose stream-oriented transmission •Authentication
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding DES output.	•Stream-oriented transmission over noisy channel (e.g., satellite communication)
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	•General-purpose block-oriented transmission •Useful for high-speed requirements

Electronic Codebook (ECB)

- Simplest mode
- Plaintext is handled *b* bits at a time and each block is encrypted using the same key
- "Codebook" because have unique ciphertext value for each plaintext block
  - Not secure for long messages since repeated plaintext is seen in repeated ciphertext
- To overcome security deficiencies you need a technique where the same plaintext block, if repeated, produces different ciphertext blocks

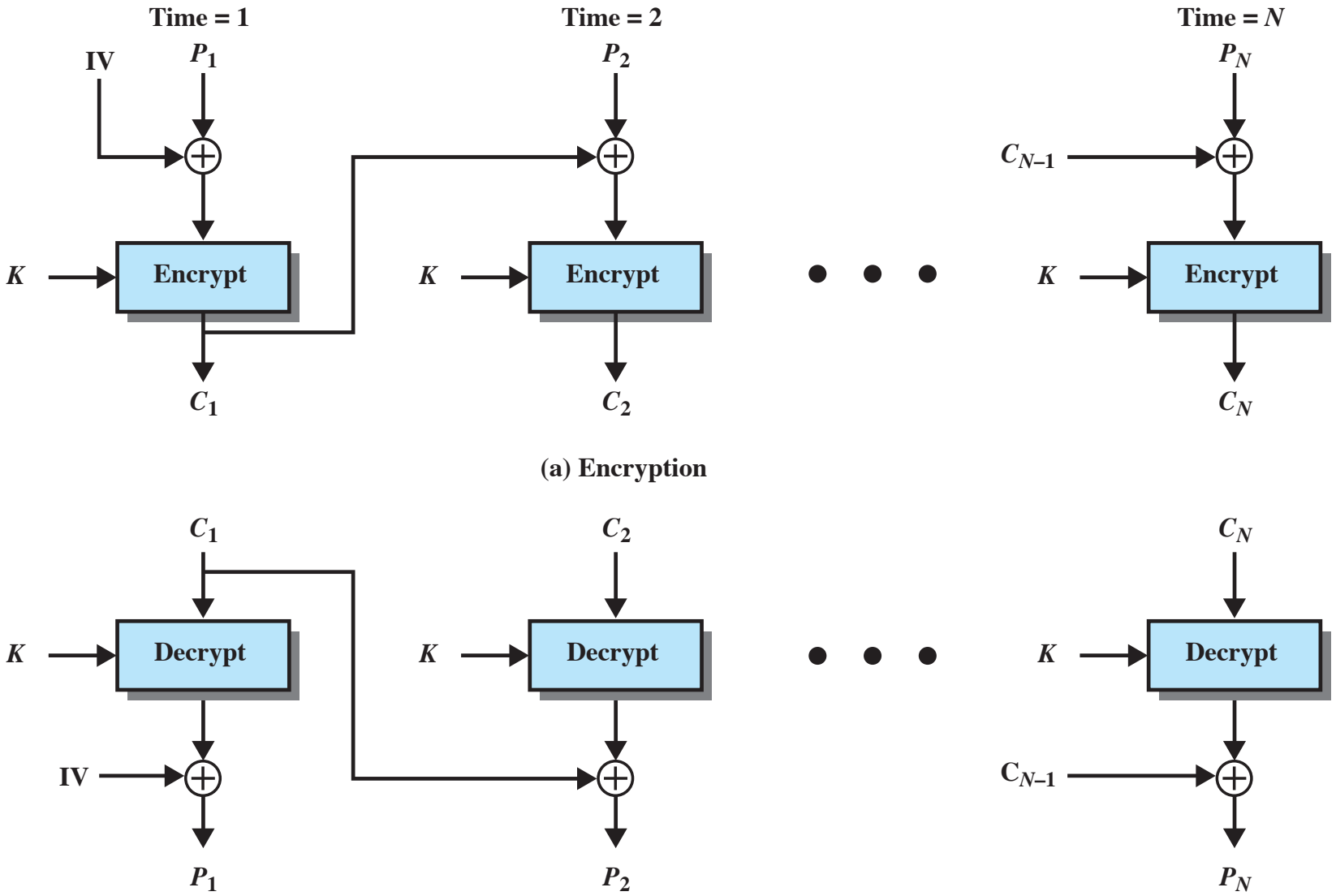


Figure 20.6 Cipher Block Chaining (CBC) Mode

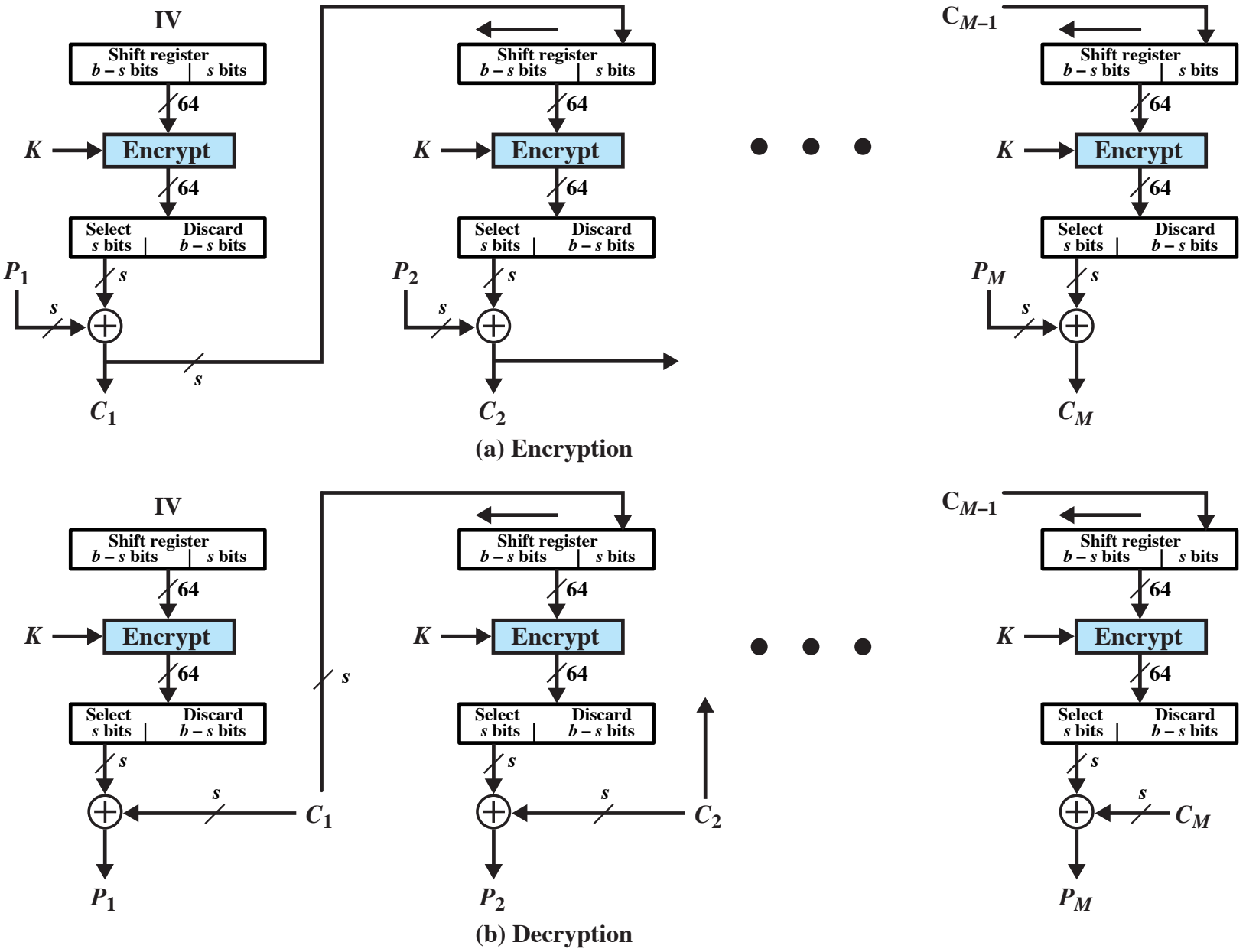
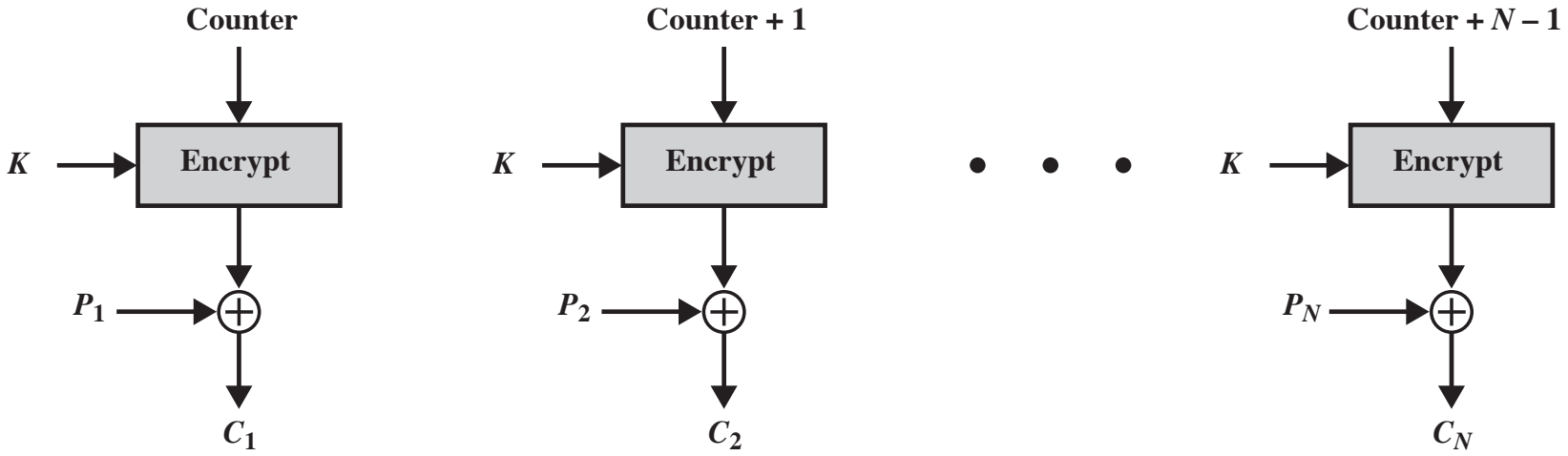
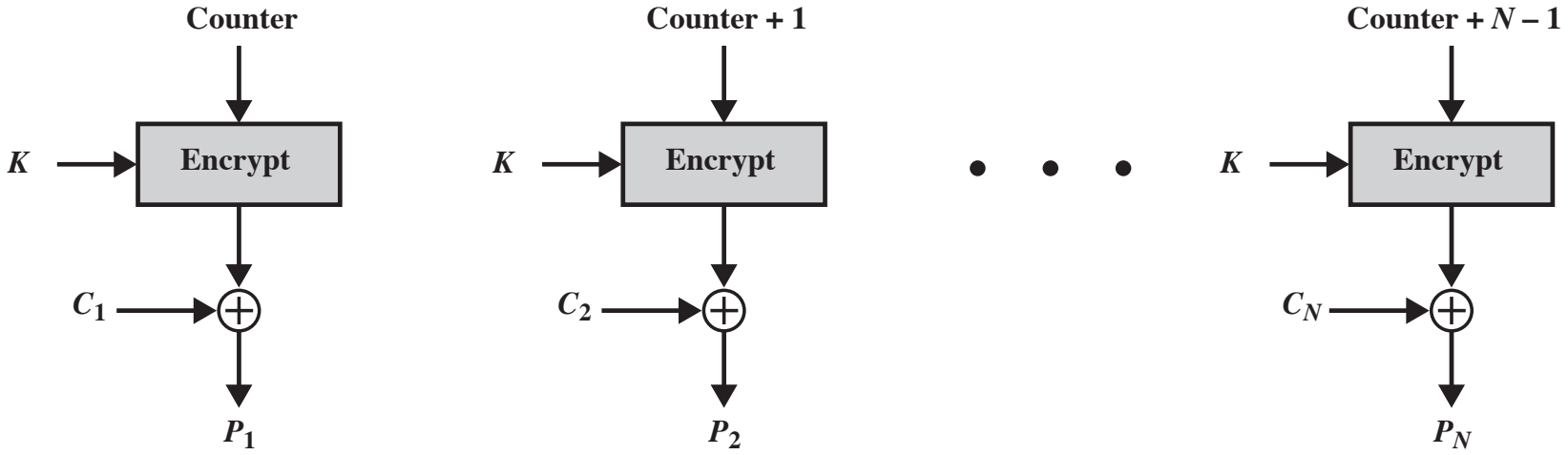


Figure 20.7 *s*-bit Cipher Feedback (CFB) Mode



(a) Encryption



(b) Decryption

Figure 20.8 Counter (CTR) Mode

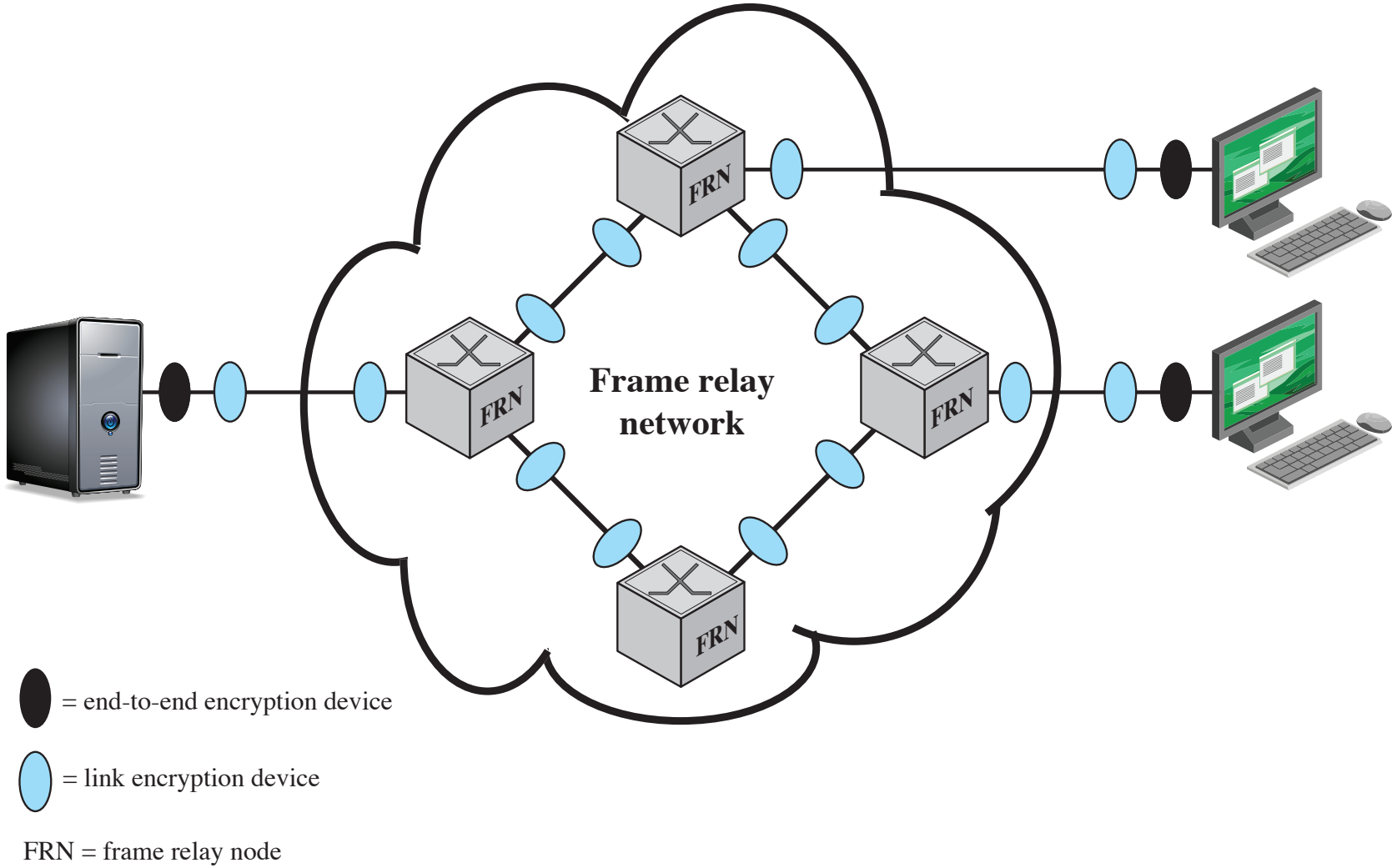


Figure 20.9 Encryption Across a Frame Relay Network

Key Distribution

- The means of delivering a key to two parties that wish to exchange data without allowing others to see the key
- Two parties (A and B) can achieve this by:

1. A key could be selected by A and physically delivered to B
2. A third party could select the key and physically deliver it to A and B
3. If A and B have previously and recently used a key, one party could transmit the new key to the other, encrypted using the old key
4. If A and B each have an encrypted connection to a third party C, C could deliver a key on the encrypted links to A and B

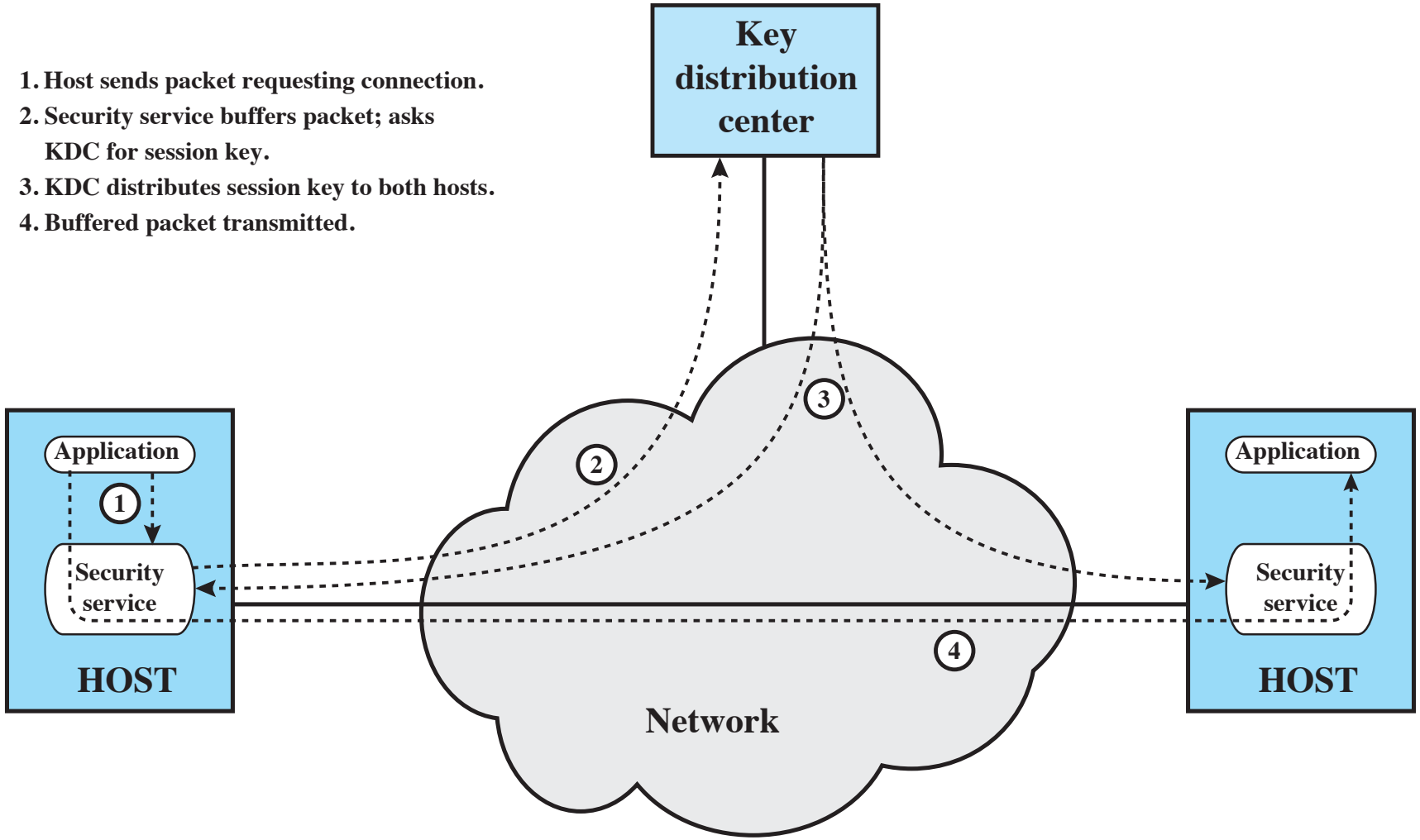


Figure 20.10 Automatic Key Distribution for Connection-Oriented Protocol

Summary

- Symmetric encryption principles
  - Cryptography
  - Cryptanalysis
  - Feistel cipher structure
- Data encryption standard
  - Data encryption standard
  - Triple DES
- Advanced encryption standard
  - Overview of the algorithm
  - Algorithm details

- Stream ciphers and RC4
  - Stream cipher structure
  - The RC4 algorithm
- Cipher block modes of operation
  - Electronic codebook mode
  - Cipher block chaining mode
  - Cipher feedback mode
  - Counter mode
- Location of symmetric encryption devices
- Key distribution