CSEC
CYBER SECURITY
EDUCATION CONSORTIUM

0100101010010101010101010011001010101010000101010101010101010100010100100

Encryption & Decryption – 2

Sujeet Shenoi
Tandy School of Computer Science
University of Tulsa, Tulsa, OK 74104
sujeet@utulsa.edu

NSF

ADVANCED
TECHNOLOGICAL
EDUCATION

Secret & Public Key Encryption Algorithms

01001010100101010101010100110010101010100001010101010101010101000101001001

Secret Key Algorithms (Symmetric)

- One key for encryption and decryption ($K_E = K_D = K$)
- $C = \{ P \}_K$ and $P = \{ C \}_K$
- One key per channel (#keys = $n \cdot (n-1)/2$)

Public Key Algorithms (Asymmetric)

- Separate keys for encryption and decryption ($K_E \neq K_D$)
- $C = \{ P \}_{K_E}$ and $P = \{ C \}_{K_D}$
- $C = \{ P \}_{K_D}$ and $P = \{ C \}_{K_E}$
- Two keys per user (#keys = $2 \cdot n$)

Secret Key Algorithms

- Data Encryption Standard (DES)
- Escrowed Encryption Standard (EES): Skipjack
- Advanced Encryption Standard (AES)

Secret Key Algorithms (Symmetric)

- Single Key for A-B Channel: (K_{AB})
- K_{AB}: Secret (known only to A and B)
- $A \rightarrow B$: $C = \{ P \}_{K_{AB}}$ (and $P = \{ C \}_{K_{AB}}$)
- $B \rightarrow A$: $C = \{ P \}_{K_{AB}}$ (and $P = \{ C \}_{K_{AB}}$)

Symmetric Key Systems

0100101010010101010101010011001010101010000101010101010101010100010100100

Problems

- Revealed keys
- Key distribution
- Large number of keys ($n \cdot (n-1)/2$ keys)

Data Encryption Standard (DES)

- NIST (1977)
- Developed for use by the general public
- Accepted as a cryptographic standard worldwide
- Hardware and software implementations
- Algorithm
  - Complex combination of substitution and transposition (Product Cipher)
  - 64-bit plaintext blocks; 56-bit keys
  - 16-round algorithm
  - Same algorithm for encryption and decryption

DES Algorithm (contd.)

Algorithm Description

- Initial Permutation
- 16 Cycles (with Key Transformation)
- Inverse Initial Permutation
- Cycle Description
  - Split into Left and Right Halves: 32 bits each
  - Expansion Permutation: 32 bits → 48 bits (Right Half only)
  - XOR with Transformed Key: 48 bits (Right Half only)
  - S-Box (Substitution Choice): 48 bits → 32 bits (Right Half only)
  - P-Box (Permutation): 32 bits (Right Half only)
  - XOR with Original Left Half: 32 bits (Right Half only)
  - Concatenation of Original Right Half and Right Half

DES Schematic

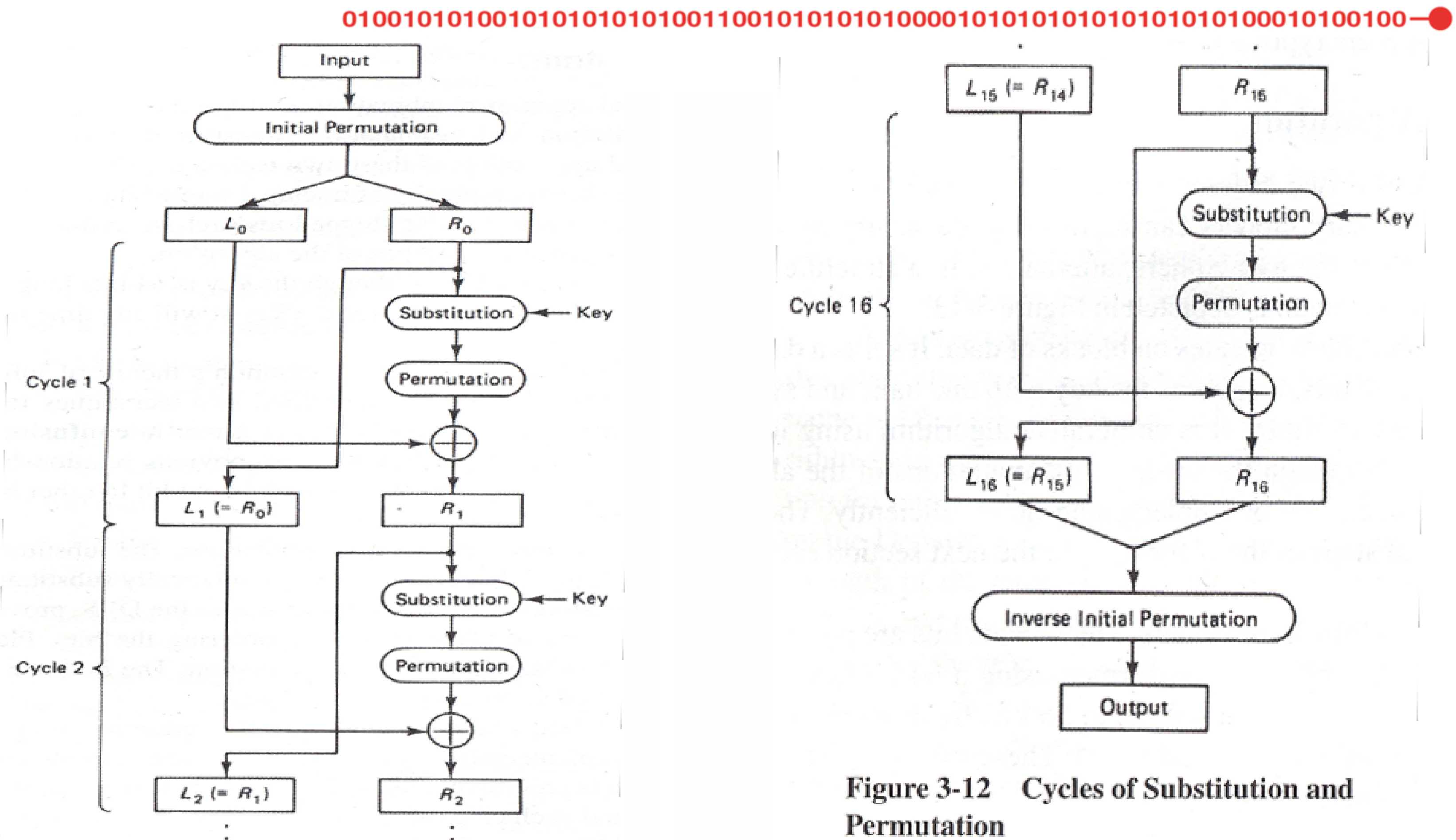


Figure 3-12 Cycles of Substitution and Permutation

Initial Permutation

01001010100101010101010011001010101010000101010101010101010100010100100

Table 3-8 Initial Permutation

Bit	Goes to Position							
1–8	40	8	48	16	56	24	64	32
9–16	39	7	47	15	55	23	63	31
17–24	38	6	46	14	54	22	62	30
25–32	37	5	45	13	53	21	61	29
33–40	36	4	44	12	52	20	60	28
41–48	35	3	43	11	51	19	59	27
49–56	34	2	42	10	50	18	58	26
57–64	33	1	41	9	49	17	57	25

Final Permutation

0100101010010101010101010011001010101010000101010101010101010100010100100

Table 3-9 Final Permutation (Inverse Initial Permutation)

Bit	Goes to Position							
1–8	58	50	42	34	26	18	10	2
9–16	60	52	44	36	28	20	12	4
17–24	62	54	46	38	30	22	14	6
25–32	64	56	48	40	32	24	16	8
33–40	57	49	41	33	25	17	9	1
41–48	59	51	43	35	27	19	11	3
49–56	61	53	45	37	29	21	13	5
57–64	63	55	47	39	31	23	15	7

DES Cycle

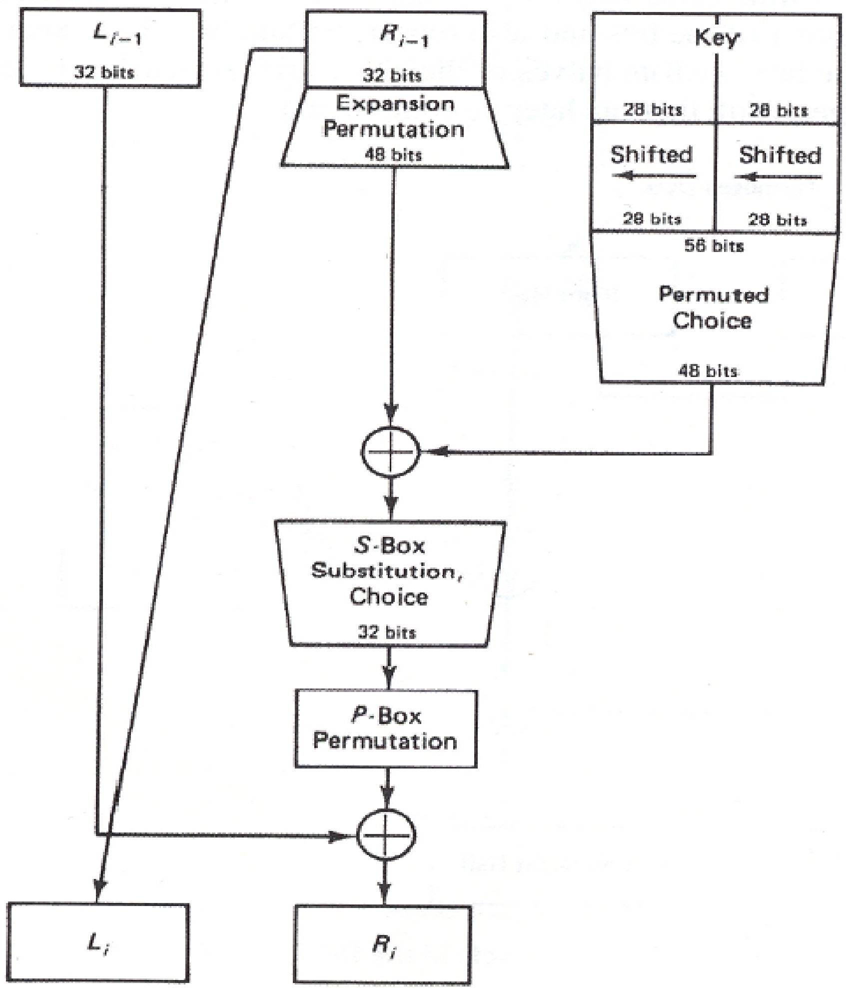


Figure 3-16

Expansion Permutation

01001010100101010101010100110010101010100001010101010101010100010100100

Table 3-3 Expansion Permutation

Bit	1	2	3	4	5	6	7	8
Moves to Position	2,48	3	4	5,7	6,8	9	10	11,13
Bit	9	10	11	12	13	14	15	16
Moves to Position	12,14	15	16	17,19	18,20	21	22	23,25
Bit	17	18	19	20	21	22	23	24
Moves to Position	24,26	27	28	29,31	30,32	33	34	35,37
Bit	25	26	27	28	29	30	31	32
Moves to Position	36,38	39	40	41,43	42,44	45	46	47,1

S-Boxes

0100101010010101010101010011001010101010000101010101010101010100010100100

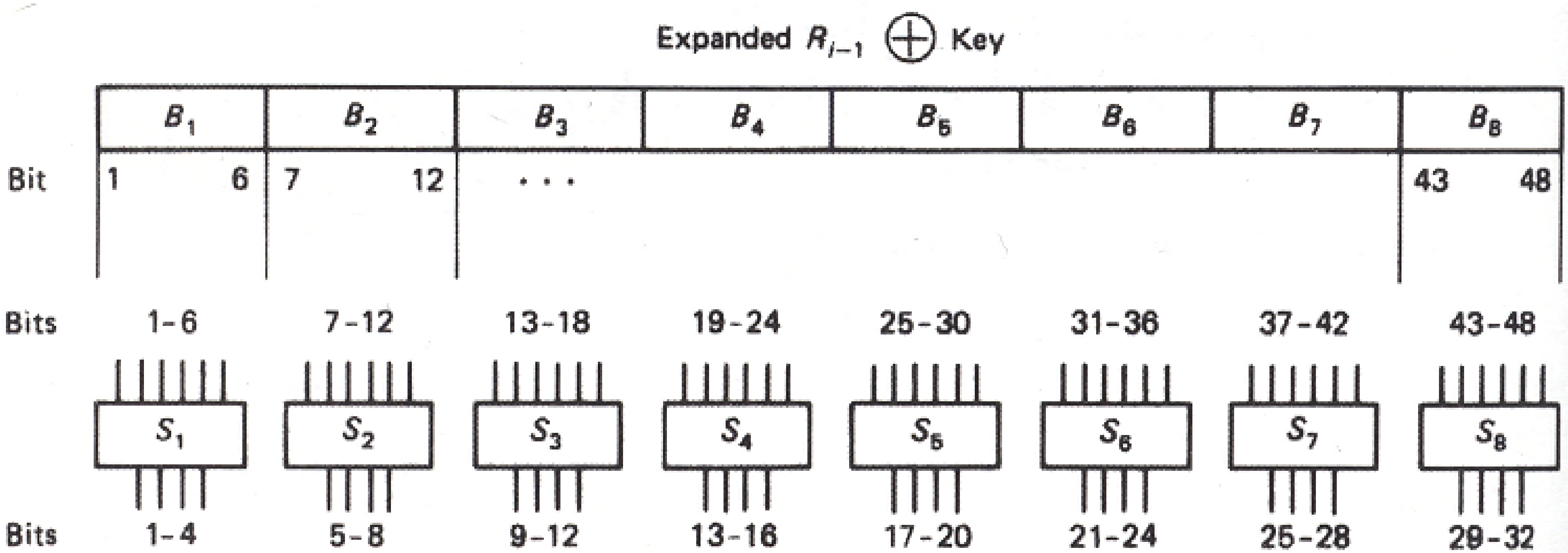


Figure 3-18 S-Boxes Operating on Eight 6-bit Blocks

S-Boxes

Table 3-6 S-Boxes of DES

Box	Row	Column															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1	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_2	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

P-Box

010010101001010101010101001100101010101000010101010101010101010100010100100

Table 3-7 Permutation Box *P*

Bit	Goes to Position							
1–8	9	17	23	31	13	28	2	18
9–16	24	16	30	6	26	20	10	1
17–24	8	14	25	3	4	29	11	19
25–32	32	12	22	7	5	27	15	21

DES Cycle

0100101010010101010101010011001010101010000101010101010101010100010100100

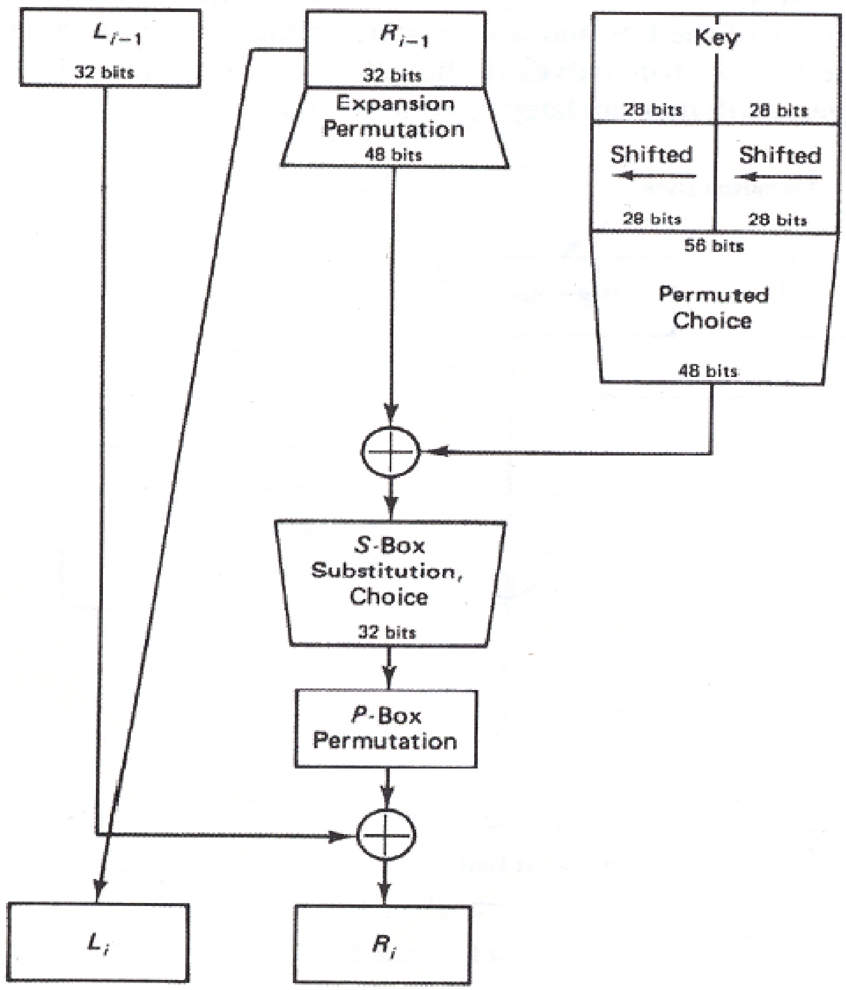


Figure 3-16

CSEC
CYBER SECURITY
EDUCATION CONSORTIUM

Key Shift

01001010100101010101010100110010101010100001010101010101010101000101001000

Table 3-4 Bits Shifted by Cycle Number

Cycle Number	Bits Shifted
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	2
10	2
11	2
12	2
13	2
14	2
15	2
16	1

NSF

ADVANCED
TECHNOLOGICAL
EDUCATION

CSEC CYBER SECURITY EDUCATION CONSORTIUM

Choice Permutation

01001010100101010101010011001010101010000101010101010101010100010100100

Table 3-5 Choice Permutation to Select 48 Key Bits

Key Bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Selected for Position	5	24	7	16	6	10	20	18	—	12	3	15	23	1
Key Bit	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Selected for Position	9	19	2	—	14	22	11	—	13	4	—	17	21	8
Key Bit	29	30	31	32	33	34	35	36	37	38	39	40	41	42
Selected for Position	47	31	27	48	35	41	—	46	28	—	39	32	25	44
Key Bit	43	44	45	46	47	48	49	50	51	52	53	54	55	56
Selected for Position	—	37	34	43	29	36	38	45	33	26	42	—	30	40

NSF

ADVANCED TECHNOLOGICAL EDUCATION

DES Cycle

0100101010010101010101010011001010101010000101010101010101010100010100100

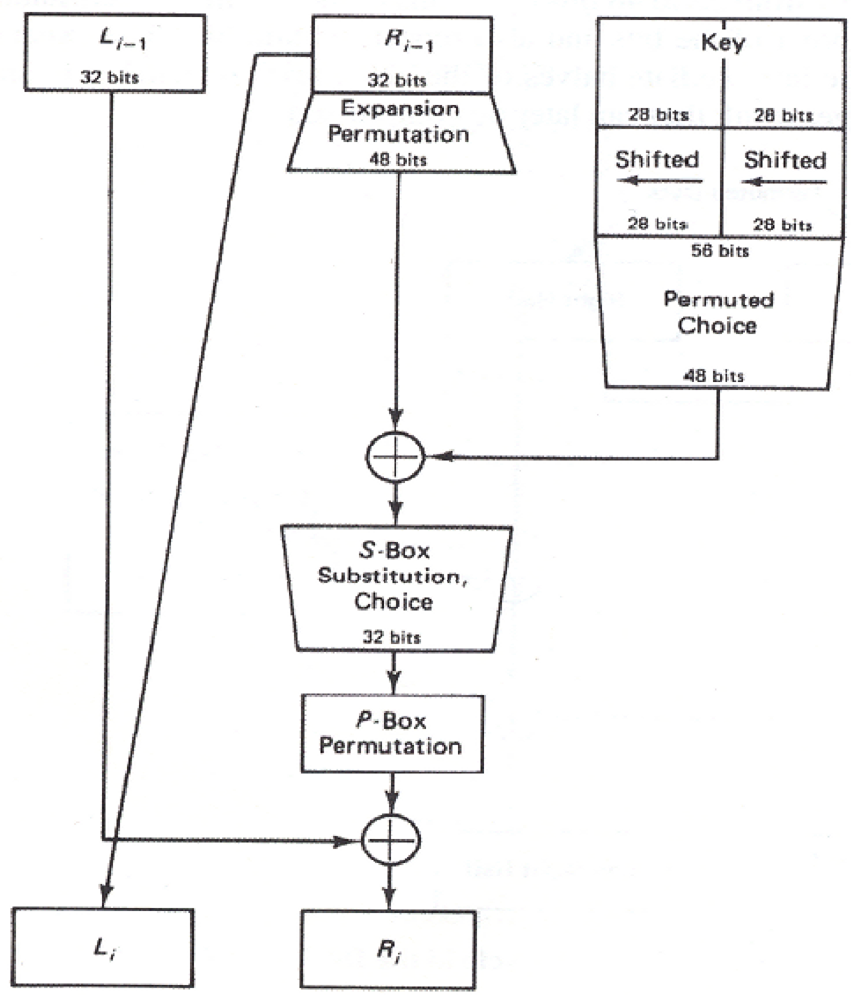


Figure 3-16

DES Algorithm (contd.)

Encryption

- $L_j = R_{j-1}$ (1)
- $R_j = L_{j-1} \oplus f(R_{j-1}, k_j)$ (2)

Decryption

- $R_{j-1} = L_j$ (3)
- $L_{j-1} = R_j \oplus f(R_{j-1}, k_j)$ (4)
- $L_{j-1} = R_j \oplus f(L_j, k_j)$ (5) (sub 3 in 4)
- Same hardware can be used for decryption
- Keys are submitted in reverse order $k_{16}, k_{15} \ldots k_1$

Security Issues

- Design of Algorithm
  - Secrecy: Rationale for S-boxes, P-boxes and key transformations was not released. Congressional inquiry exonerated NSA, but details are still secret
  - Possible Design Flaws: NSA released information about S-boxes. No S-box is a linear function of its input. Diffusion: Changing one S-box input changes at least two output bits. S-boxes were chosen to minimize differences between the number of 1s and 0s when any single input bit is held constant
- Number of Iterations
  - Are 16 cycles sufficient? Experiments indicate 8 cycles are sufficient to eliminate any observed dependence

Security Issues (contd.)

010010101001010101010101001100101010101000010101010101010101010100010100100

- Key Length (Brute Force Attacks)
  - Lucifer (IBM) has 128 bit keys; DES keys have 56 bits
  - 10 keys/s ⇒ 228 million years; 1 keys/μs ⇒ 2,280 years
  - Parallel Attack (Diffie and Hellman, 1977): 10^6 chips, each testing 1 key/μs, would require 20 hours for a brute force attack; \$50 million machine would cost \$20,000 per solution
  - 1997: Parallel Attack: 3,500 machines took 120 days (linear approach; 35,000 machines would require 12 days)
  - 1998: \$130,000 machine cracked a DES key in 112 hours
  - January 1999: EFF Team broke DES in 22 hours and 15 minutes using the Deep Crack supercomputer and 100,000 PCs; Speed was 256 billion keys/s
  - NSA will not re-certify DES

DES Weaknesses

- Complements
  - If $C = DES(P, k)$, then $\neg C = DES(\neg P, \neg k)$
  - Not a serious problem
- Weak Keys (4)
  - Keys for which $C = DES(P, k)$ and $P = DES(C, k)$
  - Same sub-key is generated for each round
  - Occurs when each key half consists only of 0s or 1s
- Semi-Weak Keys
  - Keys for which $C = DES(P, k_1) = DES(P, k_2)$ …
  - Multiple keys can decrypt message

Weak DES Keys

010010101001010101010101001100101010101000010101010101010101010001010010100

Table 3-10 Weak DES Keys

Left Half	Right Half	Weak Key Value			
zeros	zeros	0101	0101	0101	0101
ones	ones	FEFE	FEFE	FEFE	FEFE
zeros	ones	1F1F	1F1F	0E0E	0E0E
ones	zeros	E0E0	E0E0	F1F1	F1F1

CYBER SECURITY EDUCATION CONSORTIUM

Semi-Weak DES Keys

0100101010010101010101010011001010101010000101010101010101010100010100100

Table 3-11 Semi-Weak DES Key Pairs

01FE	01FE	01FE	01FE	FE01	FE01	FE01	FE01
1FE0	1FE0	0EF1	0EF1	E01F	E01F	F10E	F10E
01E0	01E0	01F1	01F1	E001	E001	F101	F101
1FFE	1FFE	0EFE	0EFE	FE1F	FE1F	FE0E	FE0E
011F	011F	010E	010E	1F01	1F01	0E01	0E01
E0FE	E0FE	F1FE	F1FE	FEE0	FEE0	FEF1	FEF1

ADVANCED TECHNOLOGICAL EDUCATION

DES Weaknesses (contd.)

- Design Weaknesses
  - Expansion permutation repeats first and fourth bits of every 4-bit series, crossing bits from neighboring 4-bit series
  - S-box S_4 derives the last three output bits the same way as the first by complementing some of the input bits
  - Two different, but carefully chosen, inputs to S-boxes can produce the same output
- Key Clustering
  - Two or more keys produce the same encryption
  - In addition to semiweak keys, other key clusters exist

DES Weaknesses (contd.)

- Differential Cryptanalysis
  - Powerful code breaking technique
  - Uses carefully selected pairs of plaintext with subtle differences and studies the effects of these differences on the resulting ciphertext pairs
  - 6 key rounds: 2^8 tests
  - 10 key rounds: 2^{35} tests
  - 15 key rounds: 2^{52} tests
  - 16 key rounds: 2^{58} tests (brute force requires 2^{56} tests)
- NSA will not re-certify DES

Double Encryption

0100101010010101010101010011001010101010000101010101010101010100010100100

DES is "weak"

Can we use two 56-bit DES keys back to back?

- $\{\,\{\text{ Message }\}_{K_1}\}_{K_2}$
- 56-bit key $\Rightarrow$ 2^{56} possibilities
- Two 56-bit keys $\Rightarrow$ 2^{112} possibilities?
- No!
- 2^{57} possibilities (Merkle, 1981)

Triple DES (TDES)

01001010100101010101010100110010101010100001010101010101010101000101001 00

Same hardware/software

Encryption (EDE)

- TDES: $C = DES_{Encrypt}(DES_{Decrypt}(DES_{Encrypt}(P,\ k_1)\ ,\ k_2)\ ,\ k_3)$

Decryption (DED)

- TDES: $P = DES_{Decrypt}(DES_{Encrypt}(DES_{Decrypt}(C,\ k_3)\ ,\ k_2)\ ,\ k_1)$

nTDES

- 3TDES ($k_1 \neq k_2 \neq k_3$): Key Size (168 bits) Effective Size (112 bits)
- 2TDES ($k_1 = k_3 \neq k_2$): Key Size (112 bits) Effective Size (80 bits)
(Because of "Meet-in-the-Middle Attacks")
- 1TDES ($k_1 = k_2 = k_3$): Key Size (56 bits) (1TDES = DES)

Escrowed Encryption Standard (EES)

- Developed by NSA (1980s) to allow “legal” wiretapping
- AT&T encrypted telephone devices (1993)
  - Analog → Digital → Encrypt → … → Decrypt → Digital → Analog
  - Unique key was generated for each session and transmitted
- Unit keys would be split into halves and kept by different escrow agencies
- Law enforcement agents would need court orders to obtain key halves (using information in LEAF)
- Sealed encryption devices

Clipper Chip

- Skipjack (algorithm)
- Clipper (chip implementing Skipjack and LEAF)
- MOSAIC (program)
- Capstone (cryptographic device with key exchange)
- Tessera (Capstone chip)
- Fortezza (Capstone chip)
- Escrowed Encryption Standard (EES)

Clipper (contd.)

Clipper Message Format

- $S \rightarrow R$: $\{ M \}_k \cdot \{ \{ k \}_u \cdot \{ n, a \} \}_f$
  - LEAF: $\{ \{ k \}_u \cdot \{ n, a \} \}_f$
  - M: 64-bit block
  - k: 80-bit session key (randomly generated and transmitted)
  - u: 80-bit unit key (unique to Clipper unit; held in escrow)
  - n: 30-bit unit ID (unique to Clipper unit)
  - a: Escrow authenticator
  - f: 80-bit law enforcement key (common to Clipper family)

Skipjack Algorithm

0100101010010101010101010011001010101010000101010101010101010100010100100

Algorithm Description

- 64-bit block (4 16-bit words: w_1, w_2, w_3, w_4)
- 32 Cycles (80-bit Key (10-bytes): cv_0, … cv_9)
- Cycle Description
  - Rule A (8 Steps) {Decryption: Rule B^{-1} (8 Steps)}
  - Rule B (8 Steps) {Decryption: Rule A^{-1} (8 Steps)}
  - Rule A (8 Steps) {Decryption: Rule B^{-1} (8 Steps)}
  - Rule B (8 Steps) {Decryption: Rule A^{-1} (8 Steps)}
  - G^k Permutation {Decryption: $[G^k]^{-1}$}
    (4-round Feistel structure)
  - F Table (Fixed-byte substitution table)

Skipjack Algorithm (contd.)

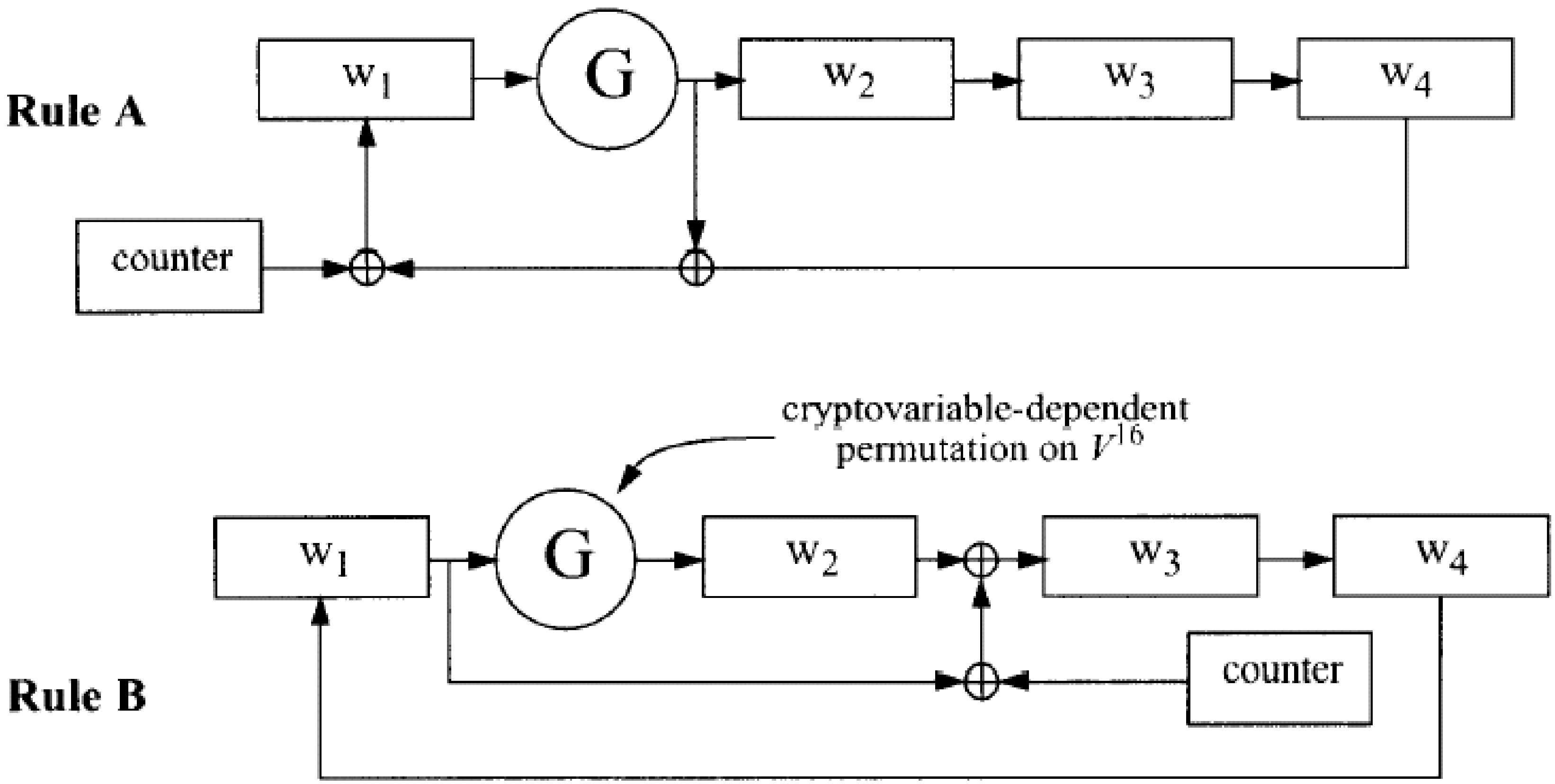


Figure 5. "SKIPJACK Stepping Rules"

Encryption Rules

01001010100101010101010100110010101010100001010101010101010101000101001000

ENCRYPT

Rule A

$$w_1^{k+1} = G^k(w_1^k) \oplus w_4^k \oplus counter^k$$

$$w_2^{k+1} = G^k(w_1^k)$$

$$w_3^{k+1} = w_2^k$$

$$w_4^{k+1} = w_3^k$$

Rule B

$$w_1^{k+1} = w_4^k$$

$$w_2^{k+1} = G^k(w_1^k)$$

$$w_3^{k+1} = w_1^k \oplus w_2^k \oplus counter^k$$

$$w_4^{k+1} = w_3^k$$

Decryption Rules

01001010100101010101010100110010101010100001010101010101010100010100100

DECRYPT

Rule A^{-1}

$$w_1^{k-1} = [G^{k-1}]^{-1}(w_2^k)$$

$$w_2^{k-1} = w_3^k$$

$$w_3^{k-1} = w_4^k$$

$$w_4^{k-1} = w_1^k \oplus w_2^k \oplus counter^{k-1}$$

Rule B^{-1}

$$w_1^{k-1} = [G^{k-1}]^{-1}(w_2^k)$$

$$w_2^{k-1} = [G^{k-1}]^{-1}(w_2^k) \oplus w_3^k \oplus counter^{k-1}$$

$$w_3^{k-1} = w_4^k$$

$$w_4^{k-1} = w_1^k$$

G-Permutation

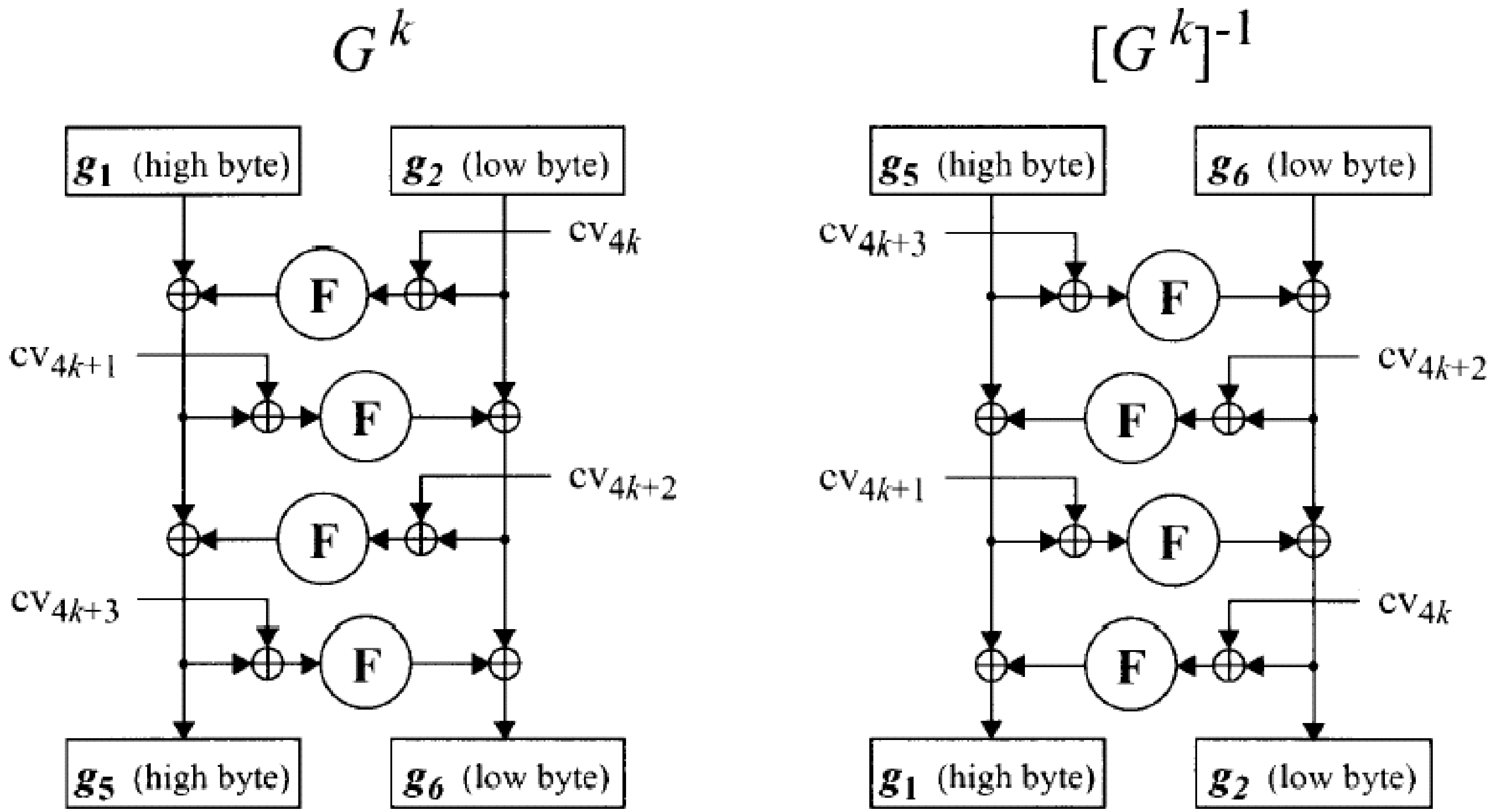


Figure 6. " G-permutation diagram"

CSEC
CYBER SECURITY
EDUCATION CONSORTIUM

F-Table

0100101010010101010101001100101010101000010101010101010101000101001000

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	a3	d7	09	83	f8	48	f6	f4	b3	21	15	78	99	b1	af	f9
1x	e7	2d	4d	8a	ce	4c	ca	2e	52	95	d9	1e	4e	38	44	28
2x	0a	df	02	a0	17	f1	60	68	12	b7	7a	c3	e9	fa	3d	53
3x	96	84	6b	ba	f2	63	9a	19	7c	ae	e5	f5	f7	16	6a	a2
4x	39	b6	7b	0f	c1	93	81	1b	ee	b4	1a	ea	d0	91	2f	b8
5x	55	b9	da	85	3f	41	bf	e0	5a	58	80	5f	66	0b	d8	90
6x	35	d5	c0	a7	33	06	65	69	45	00	94	56	6d	98	9b	76
7x	97	fc	b2	c2	b0	fe	db	20	e1	eb	d6	e4	dd	47	4a	1d
8x	42	ed	9e	6e	49	3c	cd	43	27	d2	07	d4	de	c7	67	18
9x	89	cb	30	1f	8d	c6	8f	aa	c8	74	dc	c9	5d	5c	31	a4
Ax	70	88	61	2c	9f	0d	2b	87	50	82	54	64	26	7d	03	40
Bx	34	4b	1c	73	d1	c4	fd	3b	cc	fb	7f	ab	e6	3e	5b	a5
Cx	ad	04	23	9c	14	51	22	f0	29	79	71	7e	ff	8c	0e	e2
Dx	0c	ef	bc	72	75	6f	37	a1	ec	d3	8e	62	8b	86	10	e8
Ex	08	77	11	be	92	4f	24	c5	32	36	9d	cf	f3	a6	bb	ac
Fx	5e	6c	a9	13	57	25	b5	e3	bd	a8	3a	01	05	59	2a	46

NSF

ADVANCED TECHNOLOGICAL EDUCATION

Skipjack Algorithm (contd.)

0100101010010101010101010011001010101010000101010101010101010100010100100

Expected to be 36 years before the cost of breaking Skipjack is equal to the cost of breaking DES today

- Skipjack was classified until 1998
- Abruptly declassified
- Problems still exist
  - Once unit key (u) is known, all past, present and future transmissions are compromised
  - Knowing the unit key (u) makes it possible to fabricate messages

Advanced Encryption Standard (AES)

CSEC CYBER SECURITY EDUCATION CONSORTIUM

01001010100101010101010100110010101010100001010101010101010101000101001 00

Rijndael Algorithm (Daeman & Rijmen, 2000)

- Federal standard (FIPS 197) in December 2001
- Features
  - A system breaking DES in 1 second would take 149 trillion years to break a 128-bit AES key (smallest key size)
  - Very good performance in hardware and software
  - Wide range of computing environments
  - Variable block and key lengths, and number of cycles
  - Simplicity, low memory requirements, sound design
  - Suitable for ATM, HDTV, B-ISDN, voice, satellite (> 1 Gbps requires dedicated hardware)

NSF

ADVANCED TECHNOLOGICAL EDUCATION

AES (contd.)

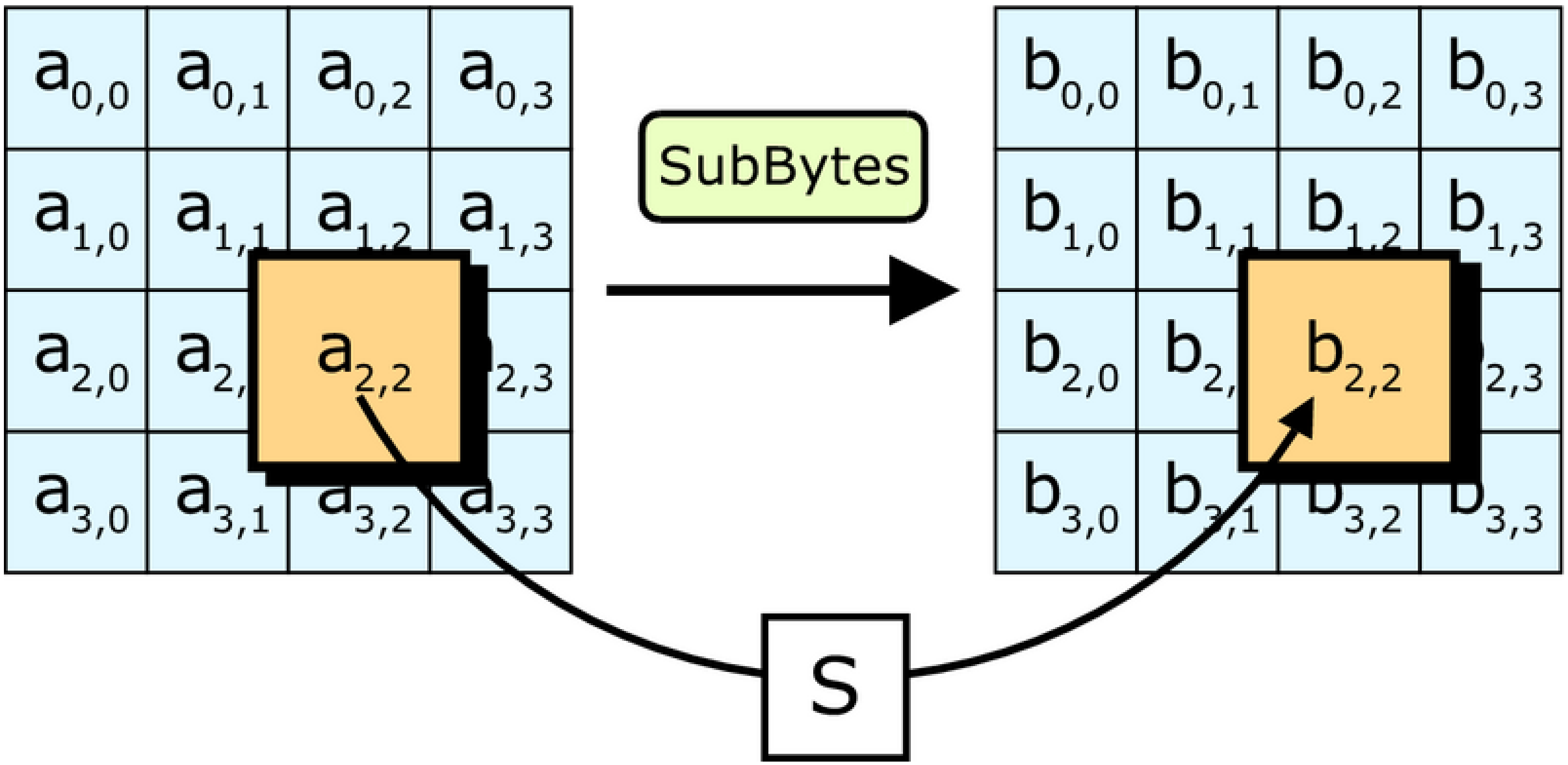
010010101001010101010101001100101010101000010101010101010101010100010100100

Details of AES Algorithm

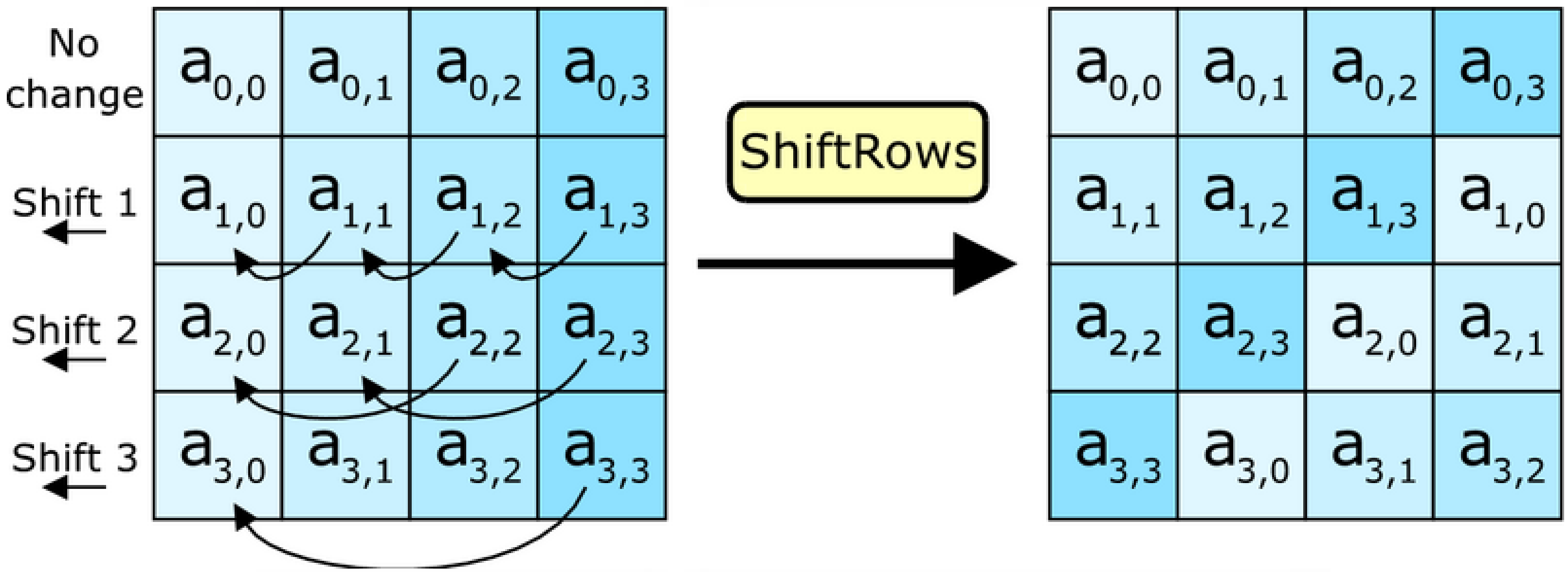
- Substitution and permutation network
  - Most ciphers use a Feistel structure (some of the bits in intermediate states are simply transposed)
- AES uses three distinct invertible uniform transformations (layers)
  - Operates on 4x4 matrix (128-bit blocks) using a finite field
- AES Algorithm
  - SubBytes: Affine S-boxes (confusion)
  - ShiftRows: Mixes bytes of rows (diffusion)
  - MixColumns: Mixes, transforms bytes of columns (diffusion)
  - AddRoundKey: XOR of key to State (confusion)

AES (contd.)

01001010100101010101010100110010101010100001010101010101010100010100100

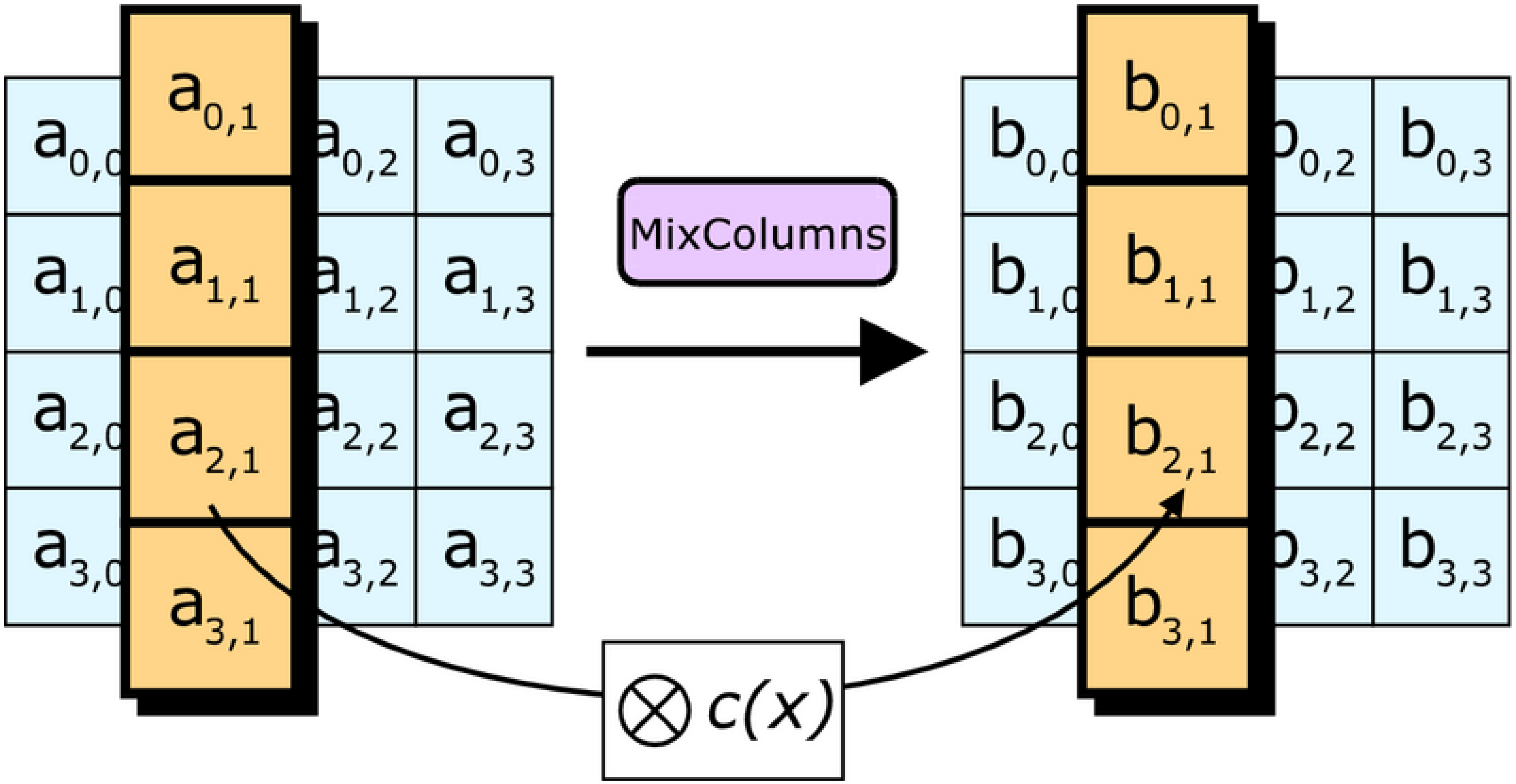


AES (contd.)



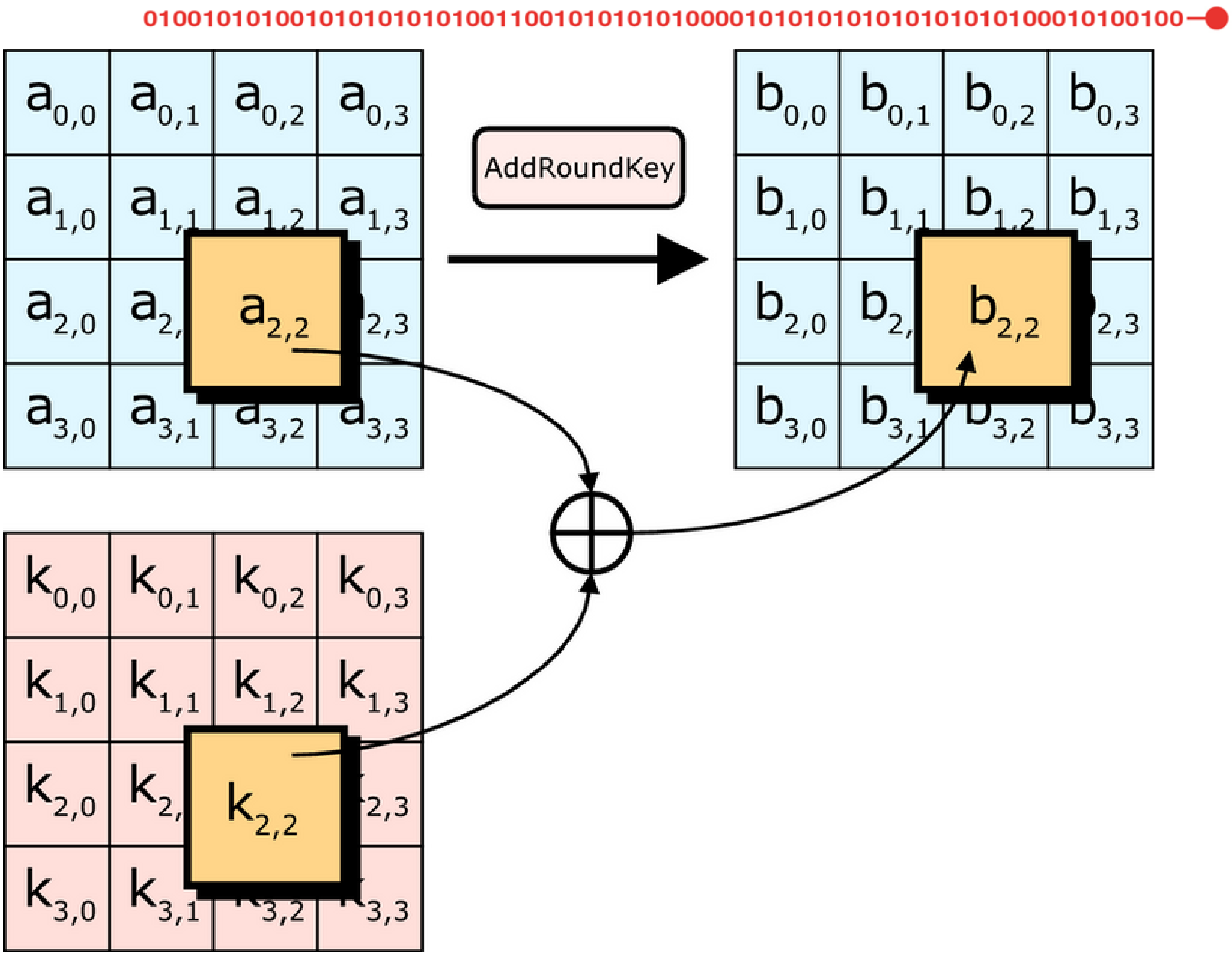
No change
Shift 1
Shift 2
Shift 3
a0,0 a0,1 a0,2 a0,3
a1,0 a1,1 a1,2 a1,3
a2,0 a2,1 a2,2 a2,3
a3,0 a3,1 a3,2 a3,3
ShiftRows
a0,0 a0,1 a0,2 a0,3
a1,1 a1,2 a1,3 a1,0
a2,2 a2,3 a2,0 a2,1
a3,3 a3,0 a3,1 a3,2

AES (contd.)



$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
MixColumns
$\otimes c(x)$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

AES (contd.)



01001010100101010101010011001010101010000101010101010101010100010100100
AddRoundKey
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,3}$
$a_{2,0}$ $a_{2,2}$
$a_{3,0}$ $a_{3,1}$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,3}$
$b_{2,0}$ $b_{2,2}$
$b_{3,0}$
$k_{0,0}$ $k_{0,1}$ $k_{0,2}$ $k_{0,3}$
$k_{1,0}$ $k_{1,1}$ $k_{1,2}$ $k_{1,3}$
$k_{2,0}$ $k_{2,2}$
$k_{3,0}$ $k_{3,1}$

AES (contd.)

0100101010010101010101010011001010101010000101010101010101010100010100100

- Resistant to all known attacks
- Speed, code compactness, wide range of platforms (including smart card applications)
- Design simplicity; Strong math foundation
- Number of Rounds (N_r) (Text: defined as $N_r - 1$)
- Variable Block (N_b) and Key (N_k) sizes (4-byte words)

	$N_b = 4$	$N_b = 6$	$N_b = 8$
$N_k = 4$:	$N_r = 10$	$N_r = 12$	$N_r = 14$
$N_k = 6$:	$N_r = 12$	$N_r = 12$	$N_r = 14$
$N_k = 8$:	$N_r = 14$	$N_r = 14$	$N_r = 14$