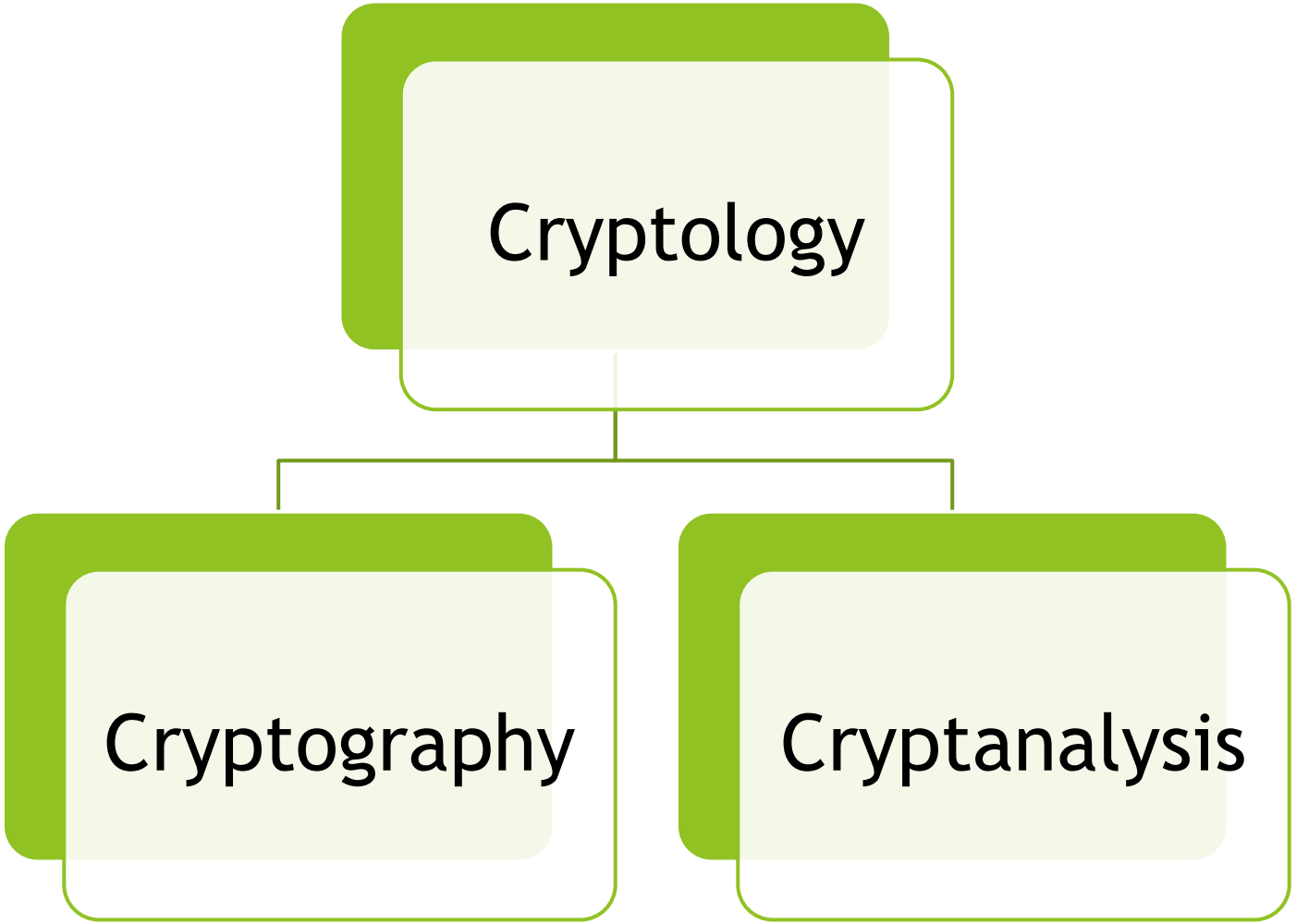
Cryptology
Cryptography
Symmetric Key Encryption

Cryptology



Cryptography and Cryptanalysis

- *Cryptography is the art and science of making a cryptosystem that is capable of providing information security.*
- *The art and science of breaking the cipher text is known as cryptanalysis.*

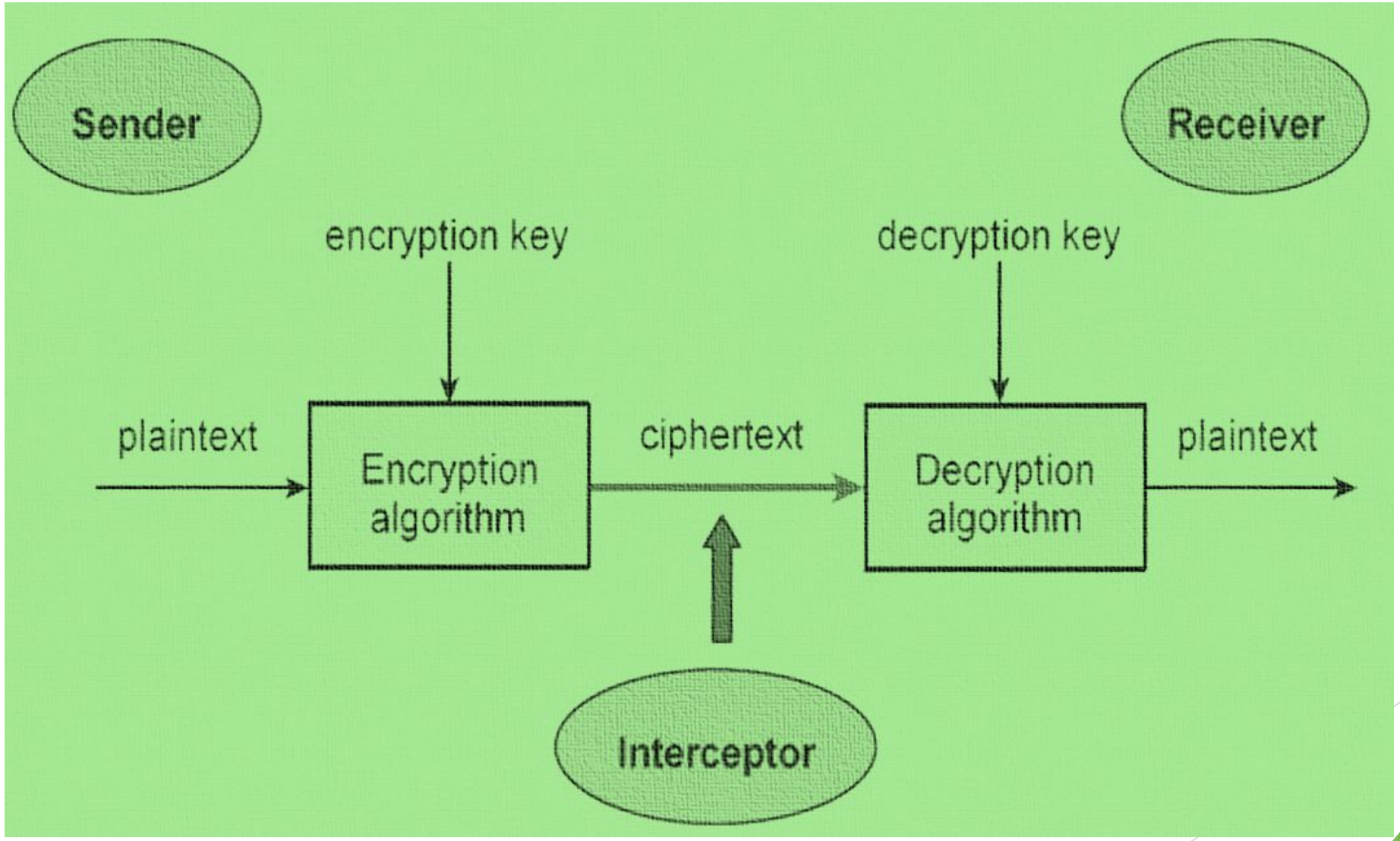
Cryptography Primitives

- Encryption
- Hash functions
- Message Authentication codes (MAC)
- Digital Signatures

Cryptography Primitives

Primitives Service	Encryption	Hash Function	Message Authentication codes	Digital Signatures
Confidentiality	+	-	-	-
Data Integrity	-	+	+	+
Authentication	-	-	+	+

Basic model of cryptosystems



Types of Cryptosystems

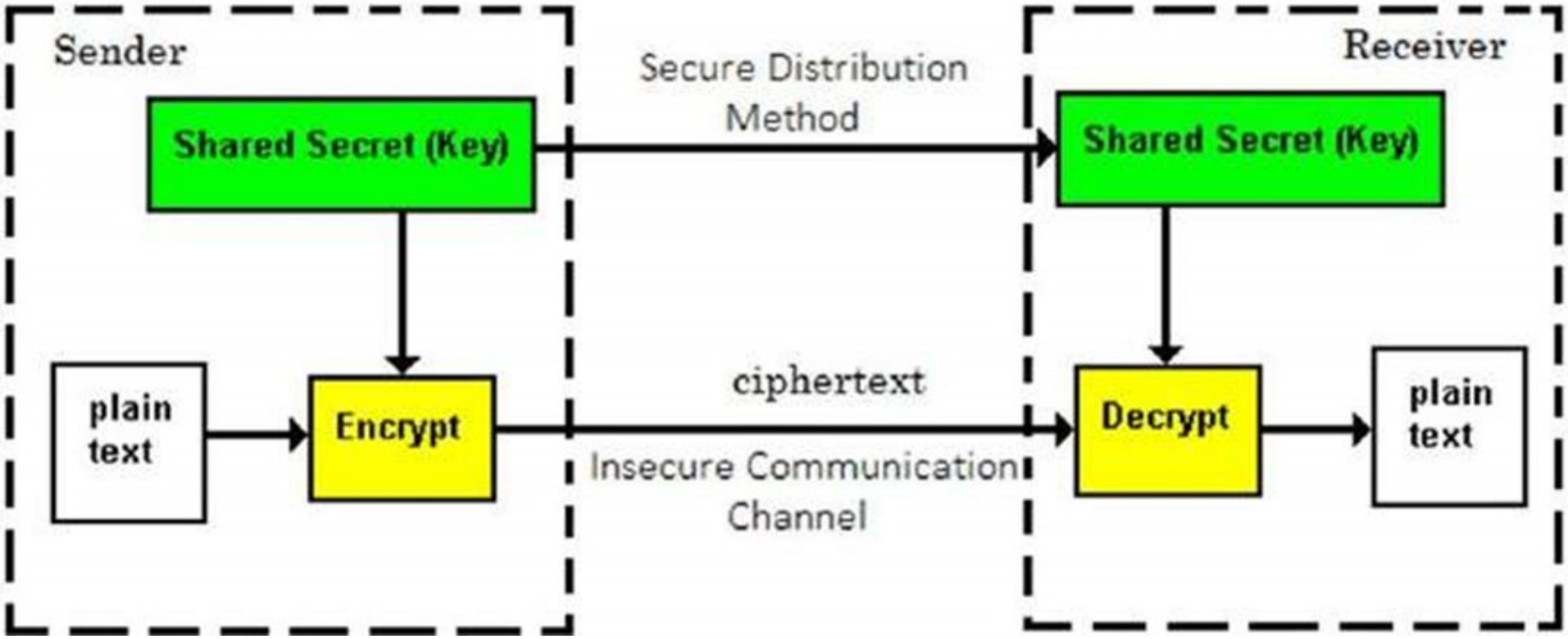
- Symmetric Key Encryption
- Asymmetric Key Encryption

The main difference between these cryptosystems is the relationship between the encryption and the decryption key.

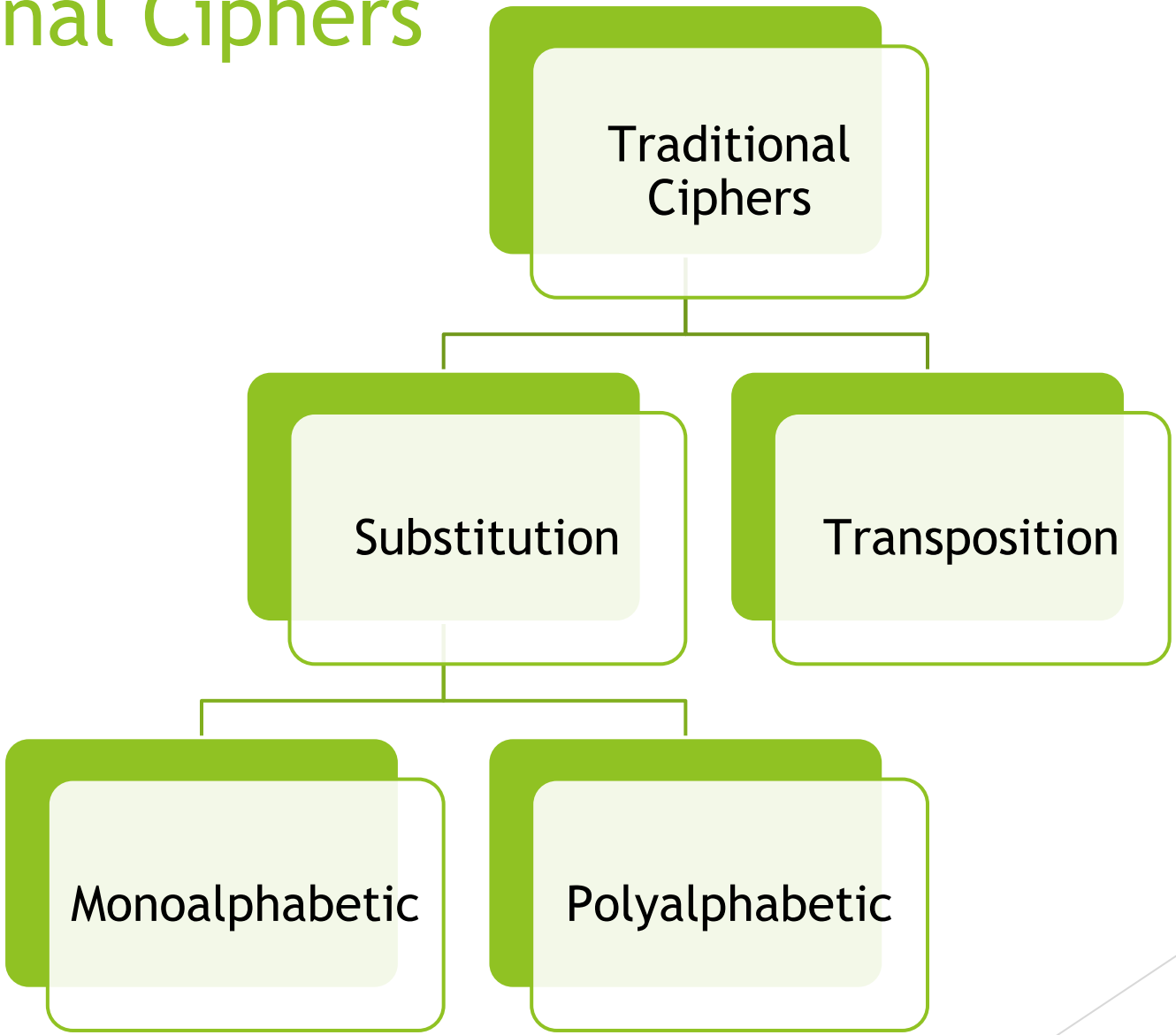
Symmetric Key Encryption

- Advanced Encryption Standard (AES)
- Digital Encryption Standard (DES)
- Triple-DES (3DES)
- IDEA
- BLOWFISH

Symmetric Key Encryption



Traditional Ciphers



Modern Symmetric Key Encryption

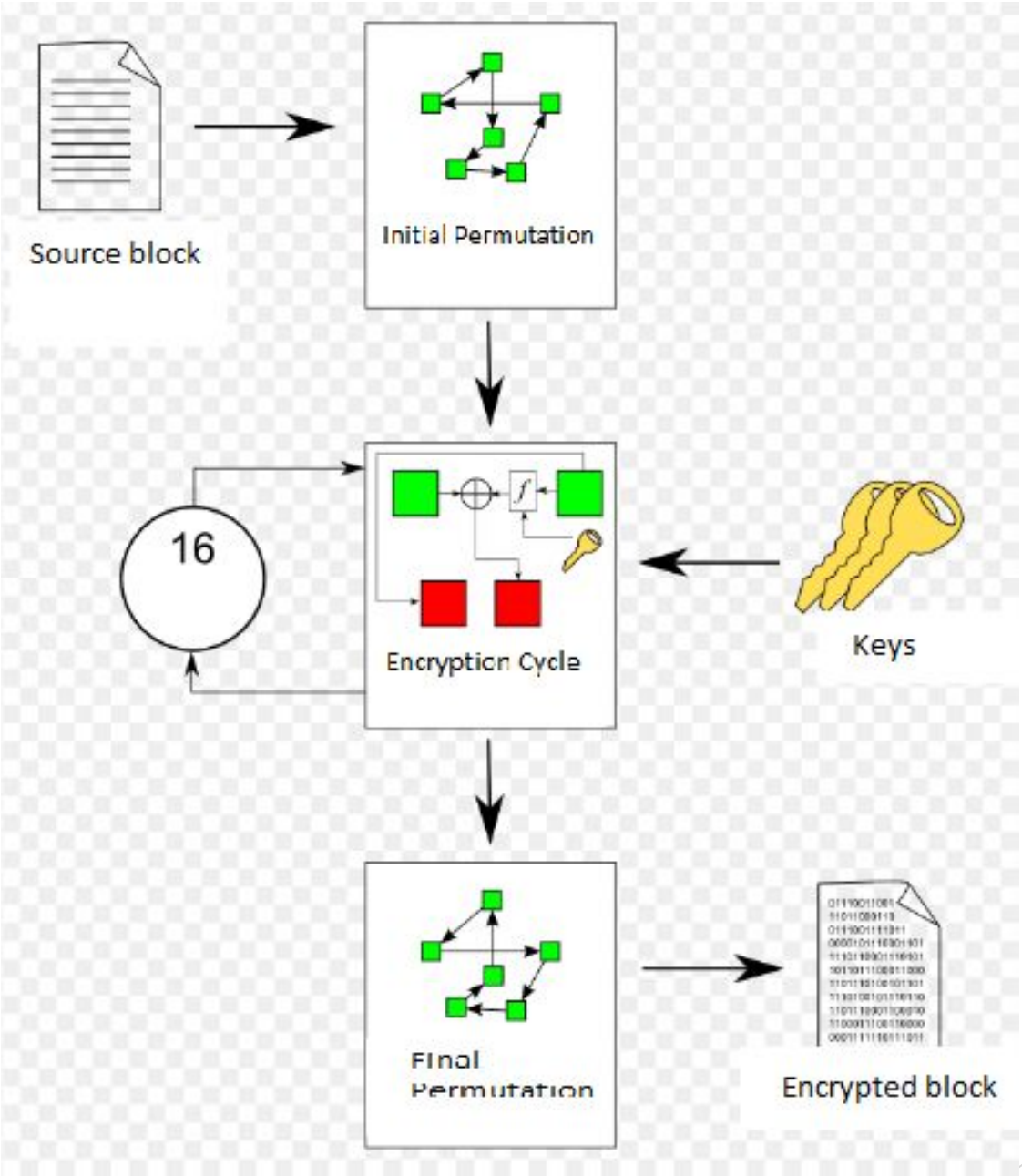
Digital data is represented in strings of binary digits (bits) unlike alphabets. Modern cryptosystems need to process this binary strings to convert in to another binary string. Based on how these binary strings are processed, a symmetric encryption schemes can be classified in to −

- Block Ciphers
- Stream Ciphers

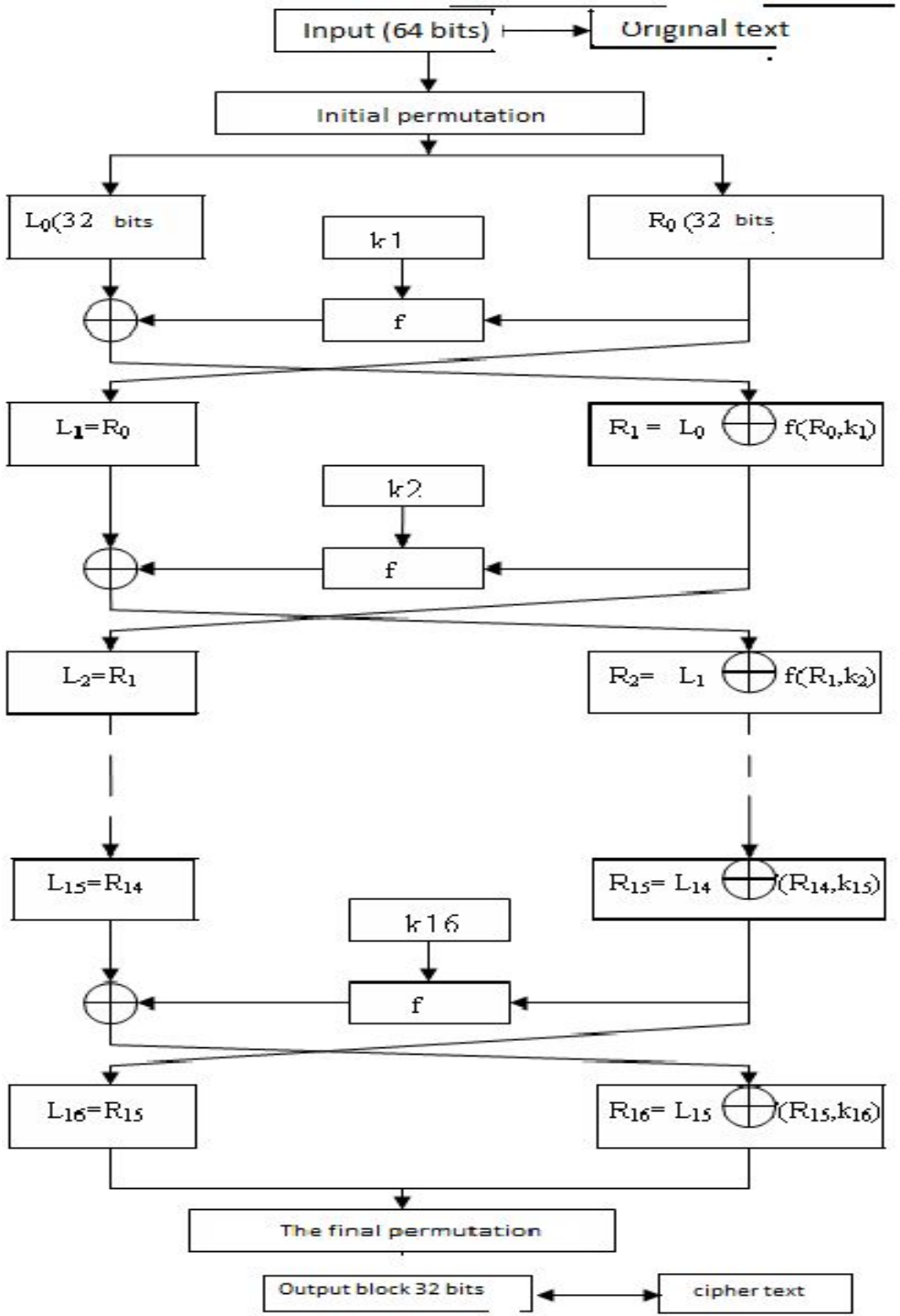
Block Cipher Schemes

- **Digital Encryption Standard (DES)** – The popular block cipher of the 1990s. It is now considered as a 'broken' block cipher, due primarily to its small key size.
- **Triple DES** – It is a variant scheme based on repeated DES applications. It is still a respected block ciphers but inefficient compared to the new faster block ciphers available.
- **Advanced Encryption Standard (AES)** – It is a relatively new block cipher based on the encryption algorithm **Rijndael** that won the AES design competition.
- **IDEA** – It is a sufficiently strong block cipher with a block size of 64 and a key size of 128 bits. A number of applications use IDEA encryption, including early versions of Pretty Good Privacy (PGP) protocol. The use of IDEA scheme has a restricted adoption due to patent issues.
- **Twofish** – This scheme of block cipher uses block size of 128 bits and a key of variable length. It was one of the AES finalists. It is based on the earlier block cipher Blowfish with a block size of 64 bits.
- **Serpent** – A block cipher with a block size of 128 bits and key lengths of 128, 192, or 256 bits, which was also an AES competition finalist. It is a slower but has more secure design than other block cipher.

Data Encryption Standard



A detailed DES encryption scheme



Initial permutation

- The initial text T (64 bit block) is converted using the initial permutation, which is determined by Table 1:

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

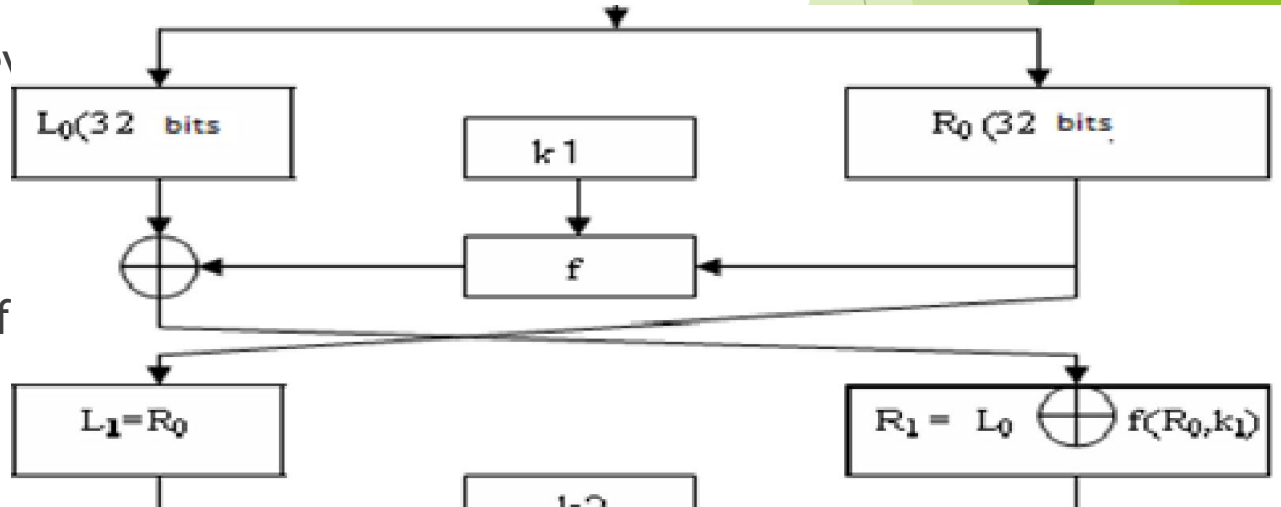
Encryption Cycles

- Obtained after the initial permutation, the 64-bit IP (T) block participates in 16 Feistel transformation cycles.
  - 16 Feistel transformation cycles:
  Split IP (T) into two parts
  L 0, R 0, where L 0, R 0 - respectively 32 high-order bits and 32 low-order bits of the block
  T 0 IP (T) = L 0 R 0

  T i - 1 = L i - 1 R i - 1 T_ {i-1} = L_ {i-1} R_ {i-1}} the result of (i-1) iteration, then the result of the i-th iteration T i = L i R i is determined by:
  L i = R i - 1
  R i = L i - 1 ⊕ f (R i - 1, k i)

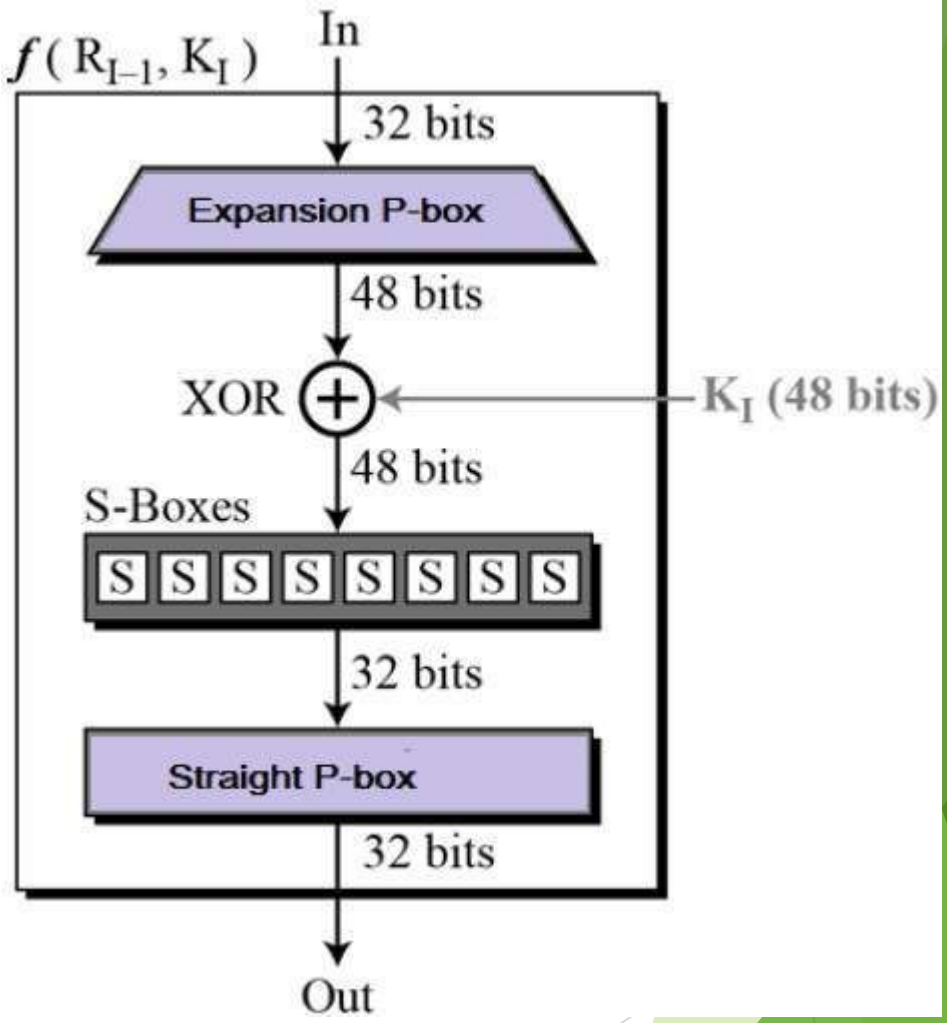
- The left half
  L i {\ displaystyle is equal to the right half of the prev
  L i - 1 R i - 1. And the right half R i Is

a bit-by-bit addition by modulo 2.
L i - 1 and f (R i - 1, k i)
In 16-cycles of the Feistel transformation, the function f encryption.



function f

- Arguments of the function f are a 32-bit vector R i – 1 and a 48-bit key k i , which is the result of converting the 56-bit cipher source key k .
  To calculate the function f consistently used
- expansion function E,
- addition modulo 2 with a key k i
- Transformation S, consisting of 8 transformations S –blocks S 1, S 2, S 3 ... S 8,
- straight P
  .



expansion function E

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

Transformation S

	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	S_1
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	
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	S_2
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	
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	S_3
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	
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	S_4
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	
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	S_5
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	
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	S_6
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	
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	S_7
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	
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	S_8
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	

straight P

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

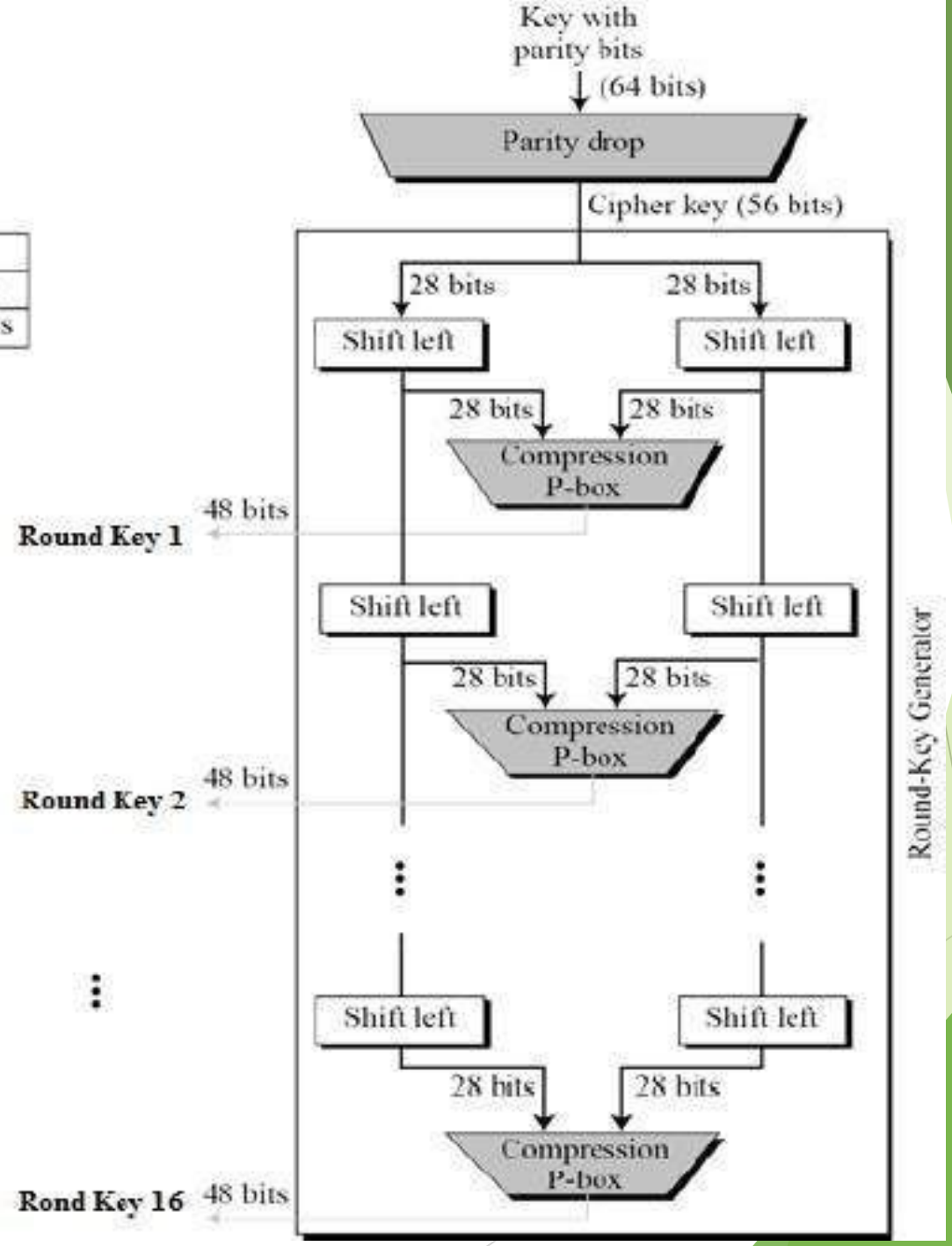
Final permutation

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

Key Generation

Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Others	two bits



Parity drop

57	49	41	33	25	17	9	1	58	50	42	34	26	18	C_0
10	2	59	51	43	35	27	19	11	3	60	52	44	36	
63	55	47	39	31	23	15	7	62	54	46	38	30	22	D_0
14	6	61	53	45	37	29	21	13	5	28	20	12	4	

shifting

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
_	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Compression P-box

14	17	11	24	1	5	3	28	15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2	41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56	34	53	46	42	50	36	29	32

homework

- cryptographic primitives: definitions, examples of use;
- stream symmetric algorithms: definitions, examples, purposes of use;
- advantages and disadvantages of DES.

- Martin Keith M. Everyday Cryptography: Fundamental Principles and Applications 2nd Edition. — Oxford University Press, 2017. — 773 p. — ISBN-10 0198788002; ISBN-13 978-0198788003.
- Bruce Schneier. Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Edition.- Wiley, 2017.- 784p.