CS326 – Systems Security

Lecture 3

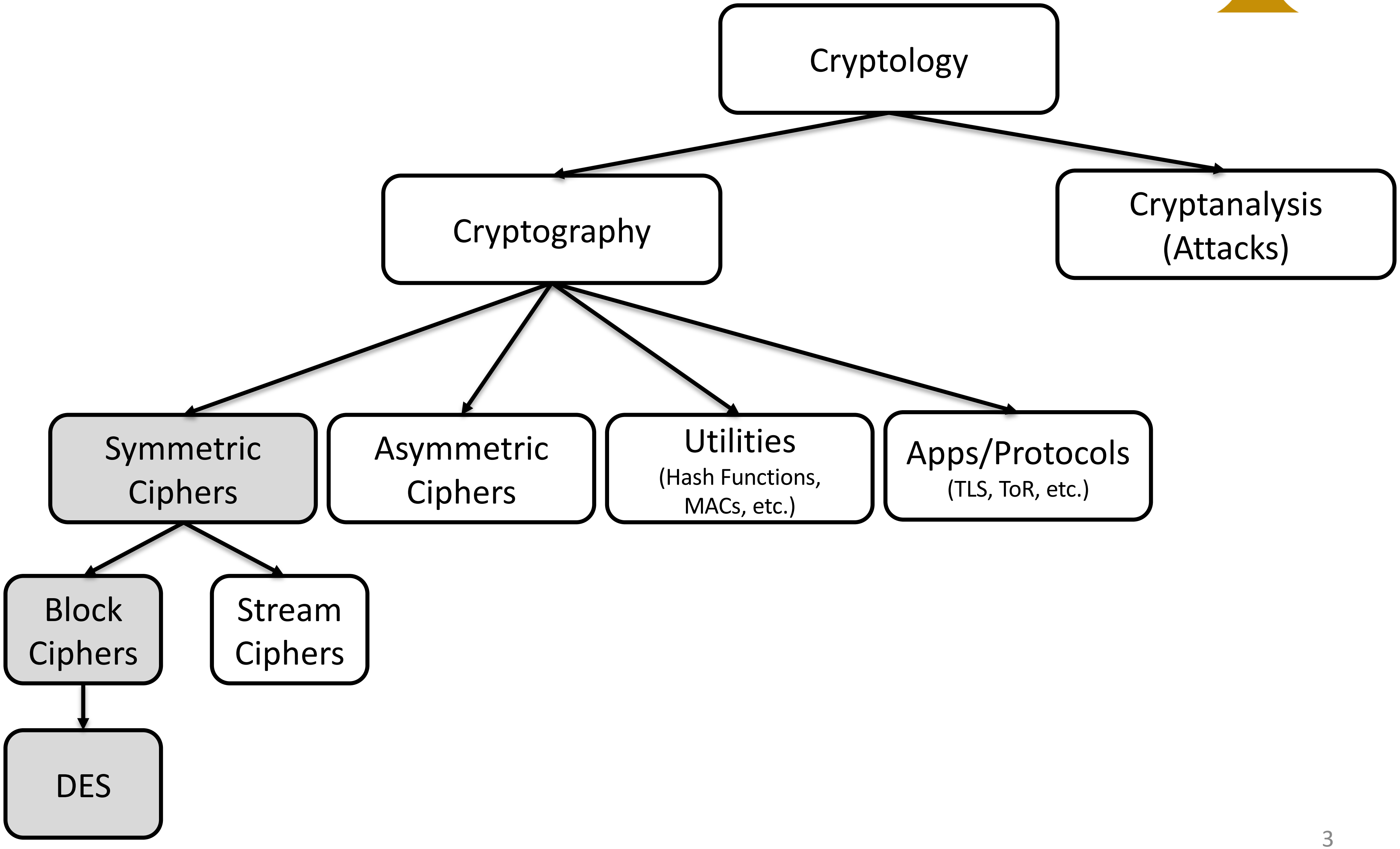
Data Encryption Standard (DES)

Elias Athanasopoulos
athanasopoulos.elias@ucy.ac.cy

Sections of this Lecture

- History of DES
- High-level overview of DES
- Details of a DES round

Cryptography Roadmap



HISTORY OF DES

DES

- Developed by IBM based on the cipher Lucifer under influence of the National Security Agency (NSA), the design criteria for DES have not been published
- Most popular block cipher for most of the last 30 years and by far best studied symmetric algorithm
- Nowadays considered insecure due to the small key length of 56 bit
  - But: 3DES yields very secure cipher, still widely used today
- Replaced by the Advanced Encryption Standard (AES) in 2000

HIGH-LEVEL OVERVIEW OF DES

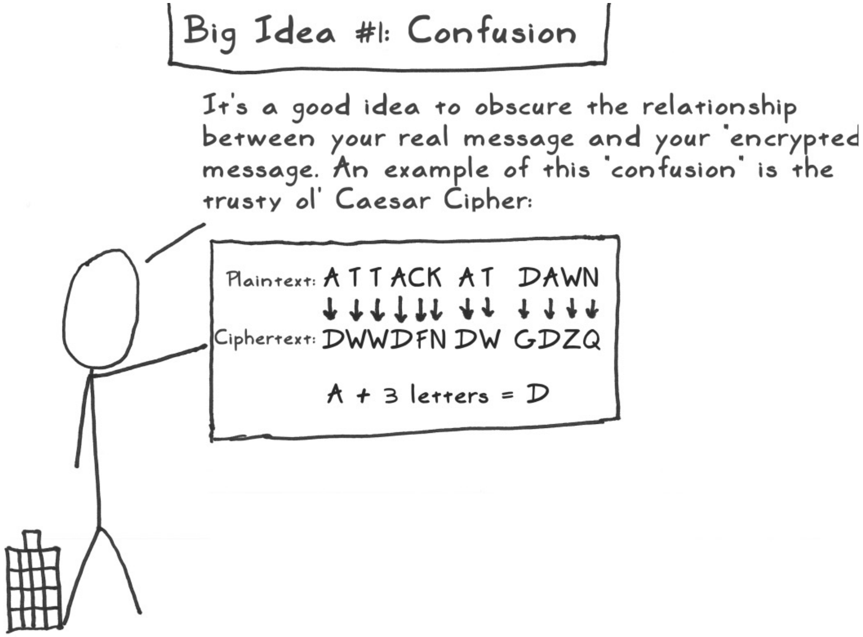
DES is a Block Symmetric Cipher

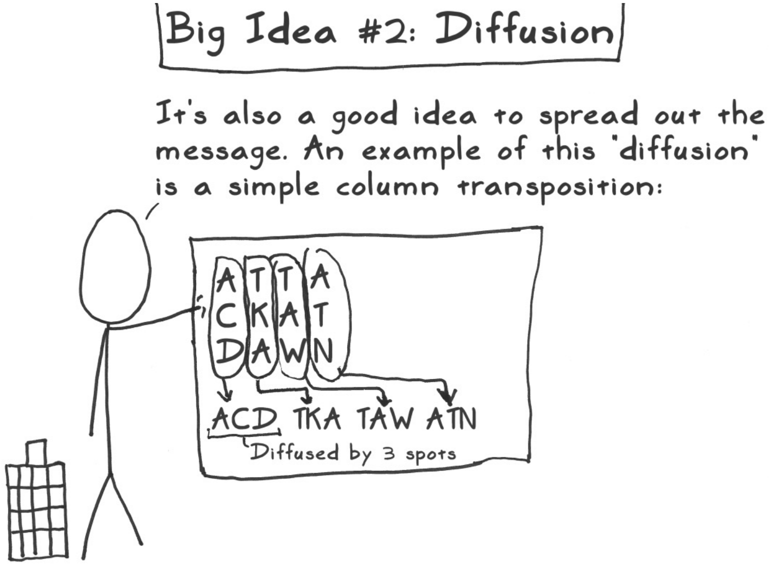
- Symmetric Ciphers
  - Use a single key to encrypt and decrypt
  - DES key size: 56 bits
  - Operate on bits not letters!
  - Implementation of DES is hardware-oriented
- Block Ciphers
  - Treat the message as a series of blocks (a few bits each)
  - Encryption and decryption operate on each block
  - Several ways to handle blocks (see future lecture for *modes of operation*)
  - DES block size: 64

How to encrypt?

- Claude Shannon: There are two primitive operations with which strong encryption algorithms can be built

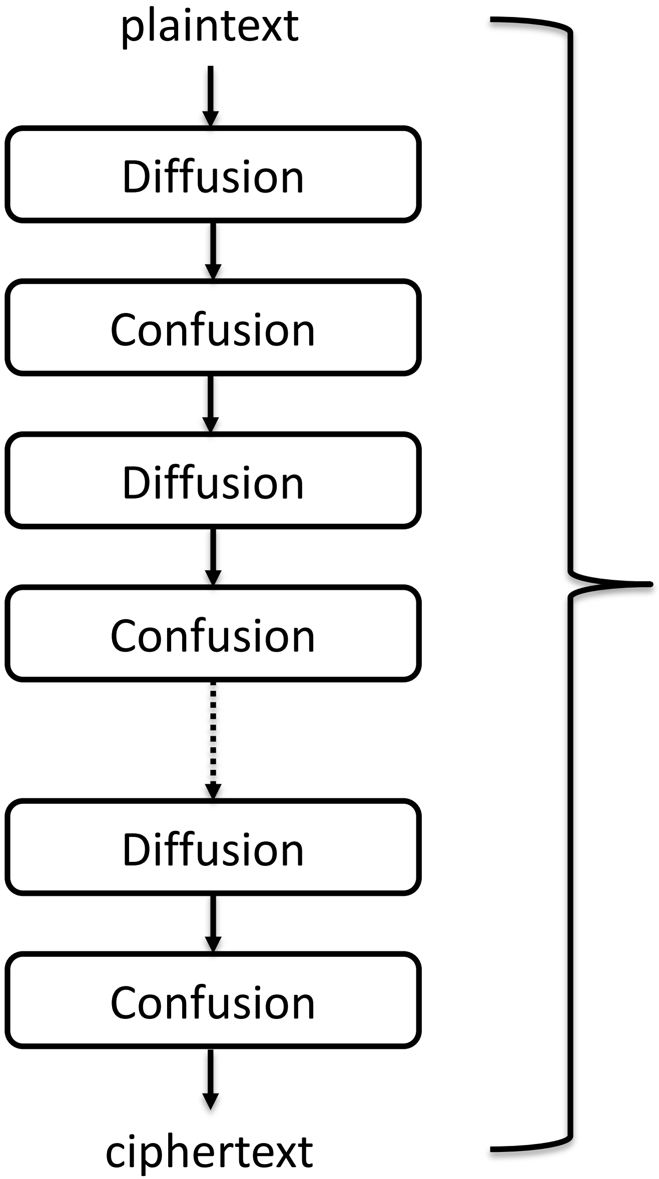
1. **Confusion**
   - An encryption operation where the relationship between key and ciphertext is obscured
   - A common element for achieving confusion is **substitution**
2. **Diffusion**
   - An encryption operation where the influence of one plaintext symbol is spread over many ciphertext symbols with the goal of hiding statistical properties of the plaintext
   - A common element for achieving diffusion is through **permutations** (i.e., transposition)


Big Idea #1: Confusion
It's a good idea to obscure the relationship between your real message and your "encrypted" message. An example of this "confusion" is the trusty ol' Caesar Cipher:
Plaintext: ATTACK AT DAWN
Ciphertext: DWWDFN DW GDZQ
A + 3 letters = D


Big Idea #2: Diffusion
It's also a good idea to spread out the message. An example of this "diffusion" is a simple column transposition:
ATTA
CKAT
DAWN
ACD TKA TAW ATN
Diffused by 3 spots

Rounds of Basic Operations

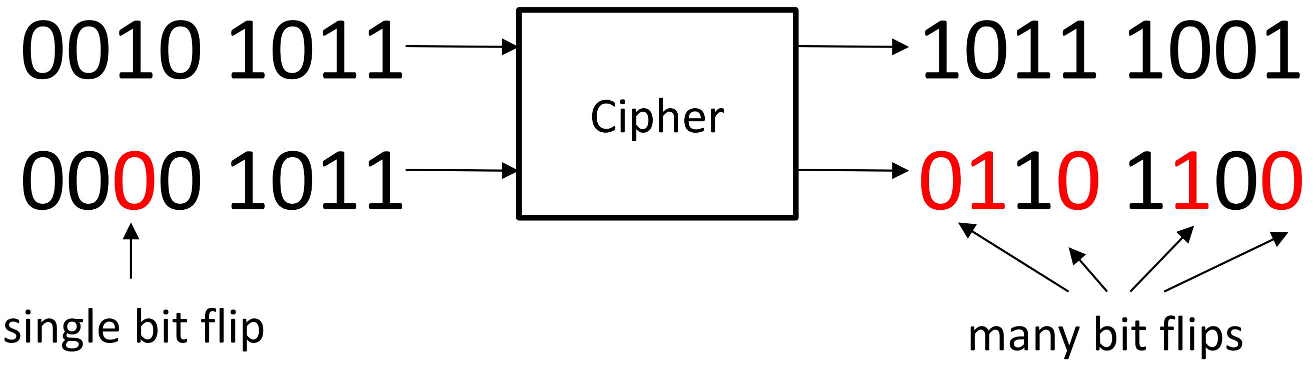
Ciphers with such structure, which combine several Diffusion and Confusion rounds are called *product ciphers*



Several Rounds
DES: 16 rounds

Avalanche Effect

- Ideally, we want a single bit flip at the plaintext to introduce many bit flips at the ciphertext



0010 1011

0000 1011

Cipher

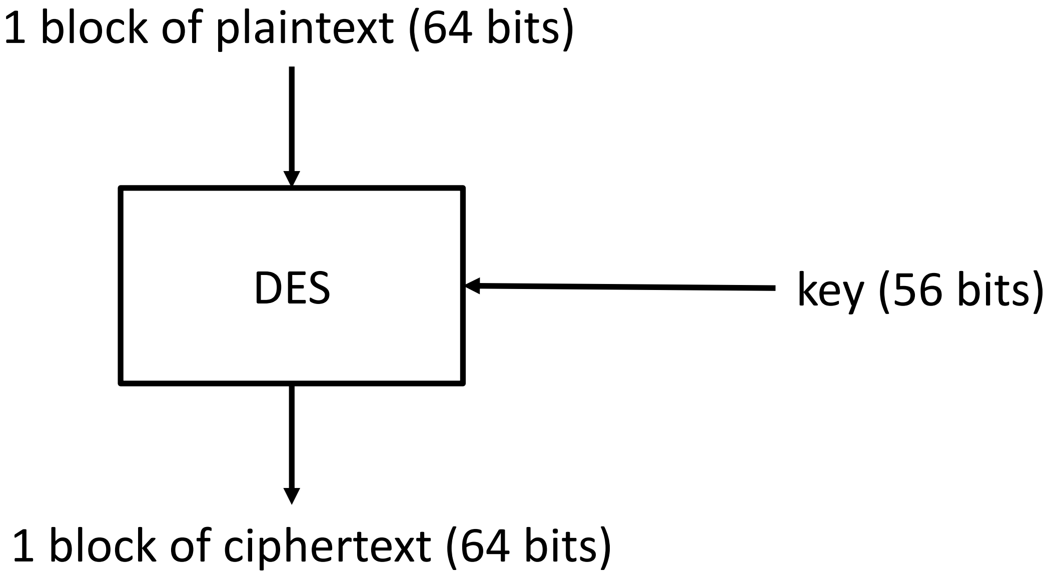
1011 1001

0110 1100

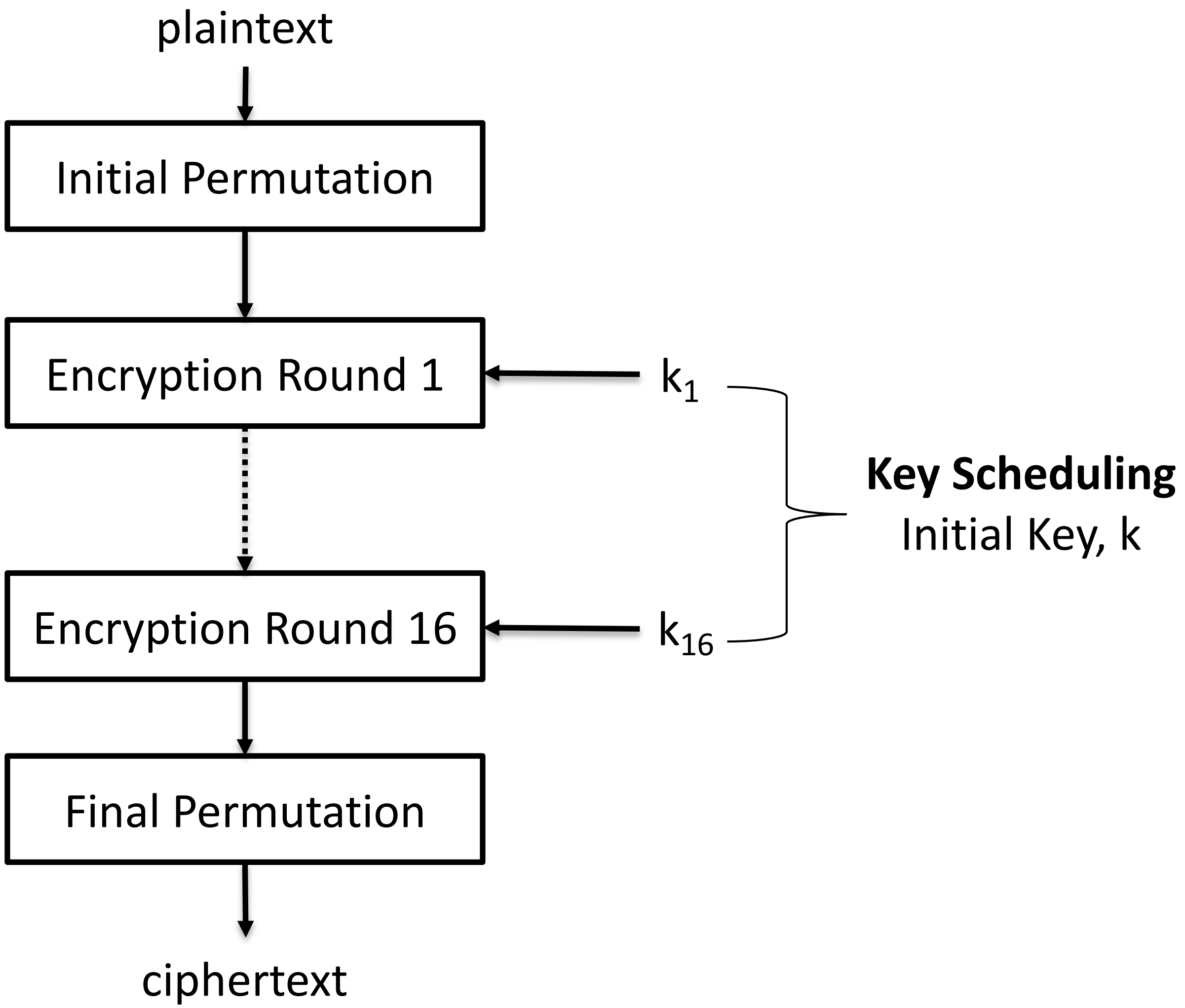
single bit flip

many bit flips

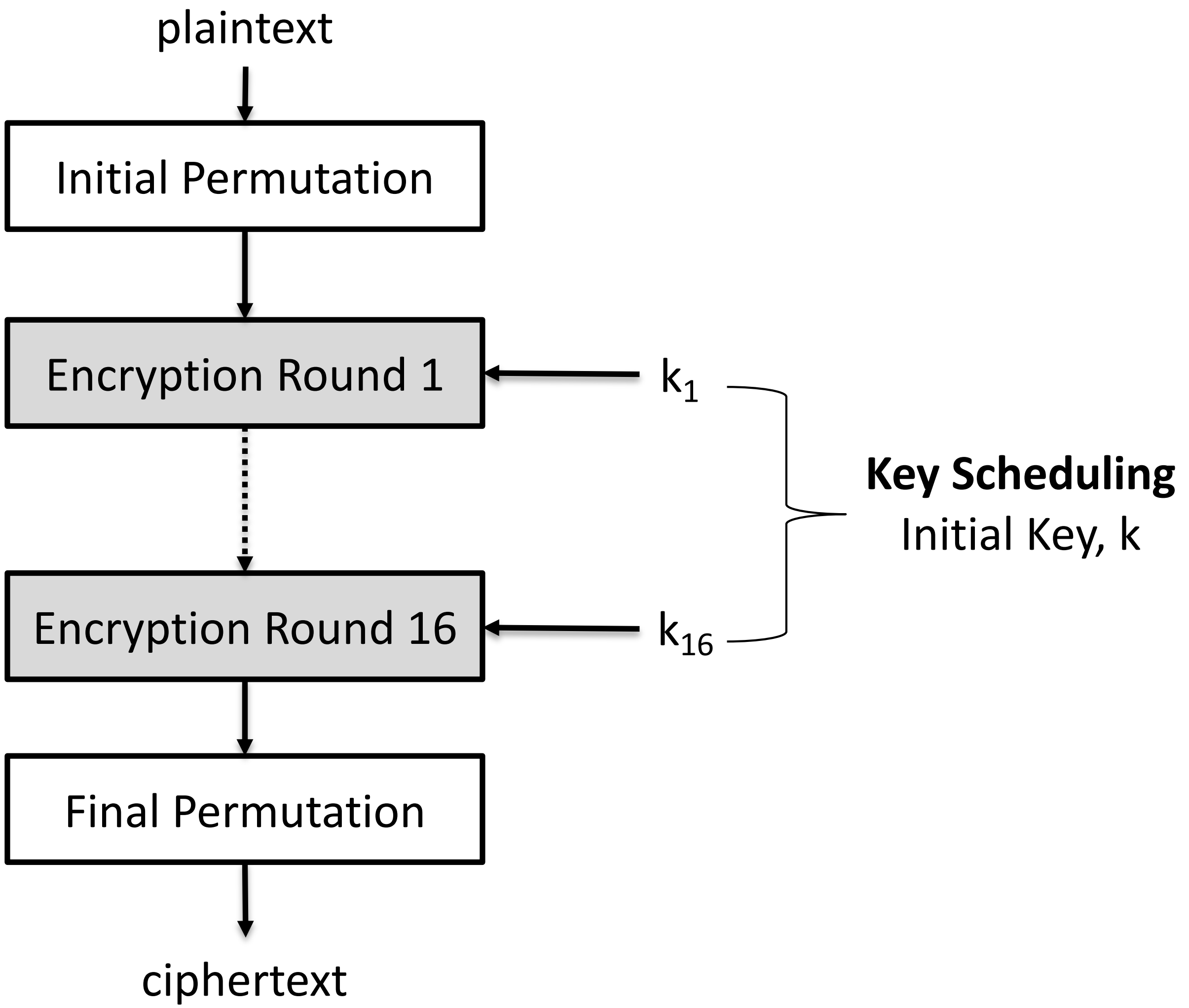
High-level View of DES


1 block of plaintext (64 bits)
DES
key (56 bits)
1 block of ciphertext (64 bits)

DES Structure



DES Structure

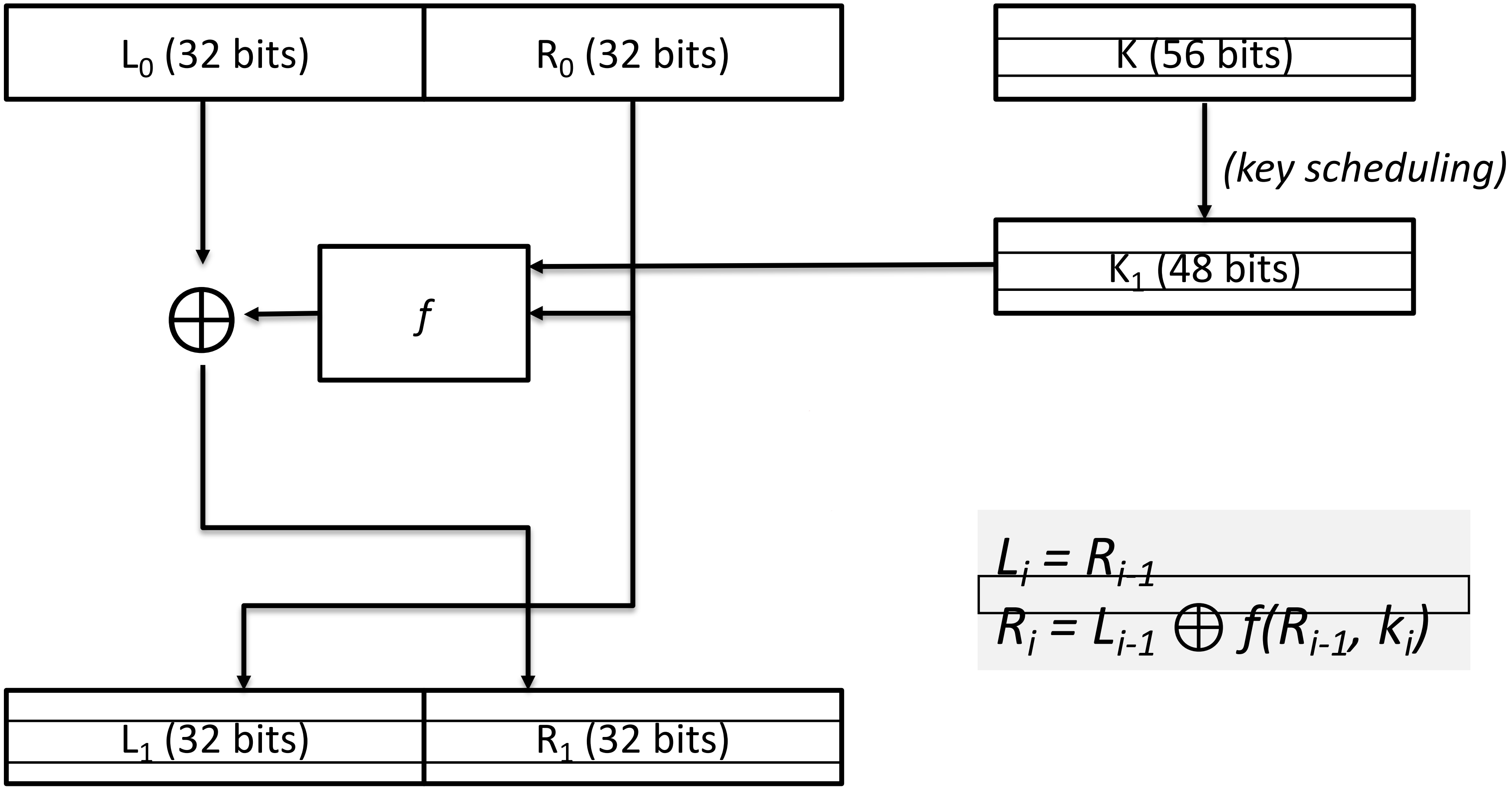


We are now going to analyze this part

DETAILS OF A DES ROUND

DES Feistel Network

DES Feistel Network



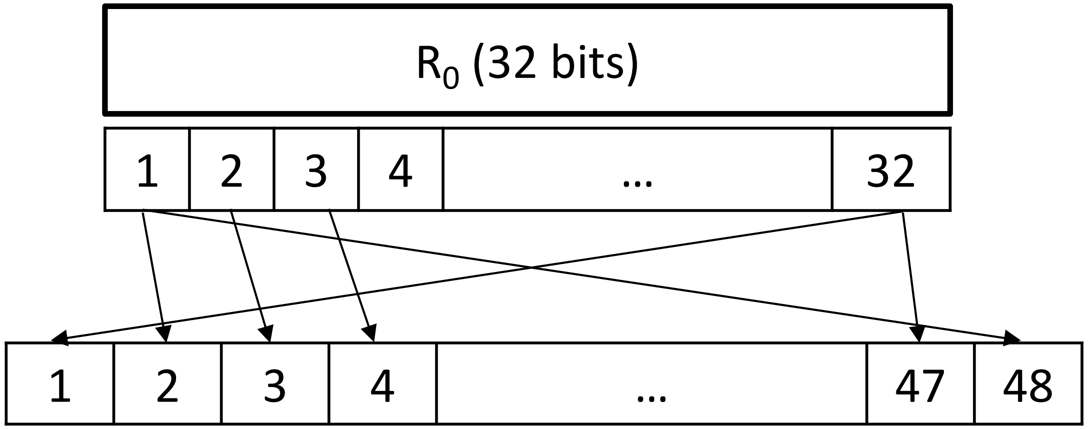
$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

DES function *f*

- Input is R_{i-1} (32 bits) and k_i (48 bits)
- 4 steps
  1. Expansion *E*
  2. XOR with key k_i
  3. S-box substitution
  4. Permutation *P*

Step 1: Expansion *E*



R_0 (32 bits)

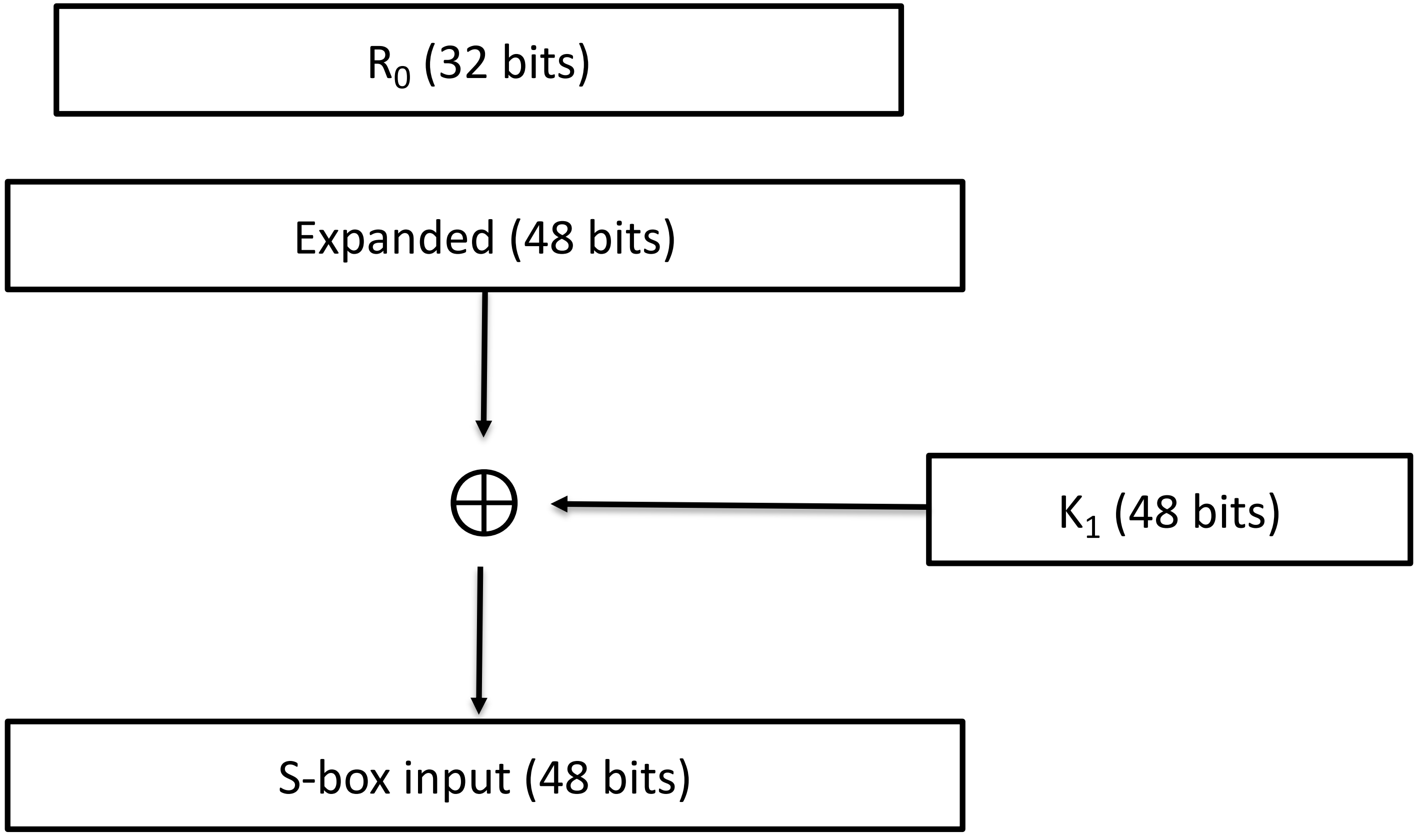
1 2 3 4 … 32

1 2 3 4 … 47 48

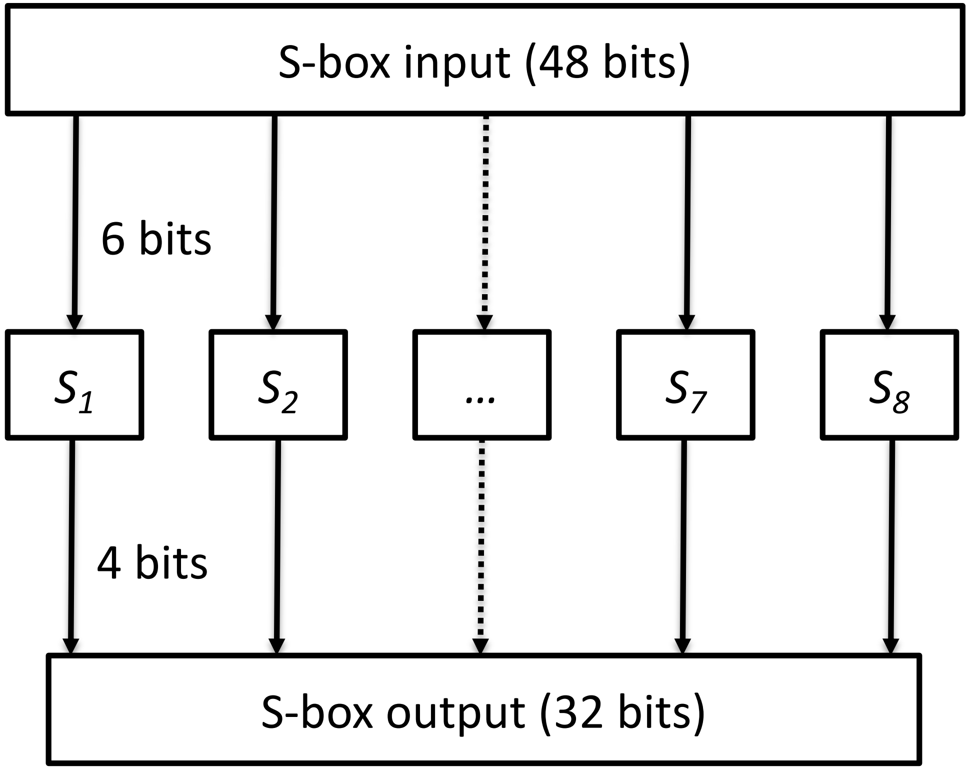
E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Transform 32 bits to 48 bits
Increase diffusion

Step 2: XOR with round key



Step 3: S-box Substitution



Inside an S-box

- There are 8 S-boxes
- Each one takes 6 bits and outputs 4 bits
- Selection: $X_1Y_2Y_3Y_4Y_5X_6$
  - Xs manage row, Ys manage column
  - Eg: 100101, 11 fourth row, 0010 third column

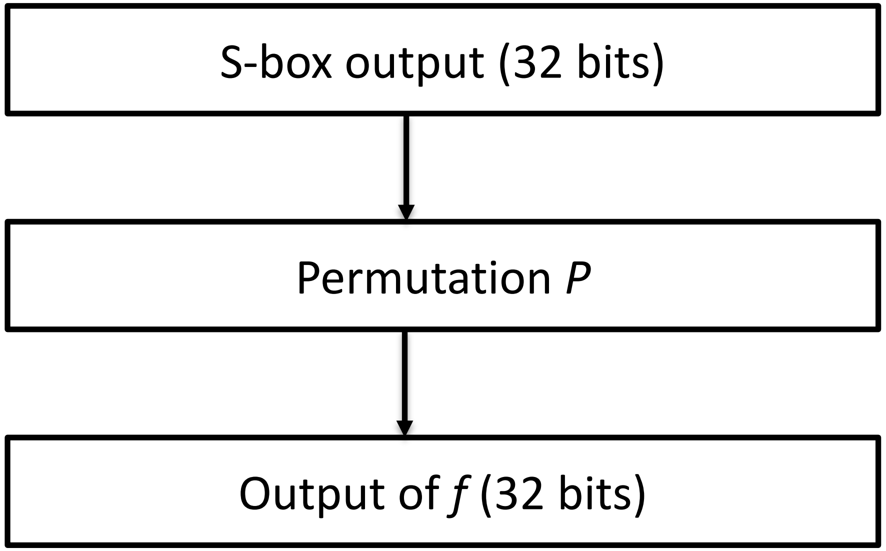
S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Inside an S-box

- There are 8 S-boxes
- Each one takes 6 bits and outputs 4 bits
- Selection: $X_1Y_2Y_3Y_4Y_5X_6$
  - Xs manage row, Ys manage column
  - Eg: 100101, 11 fourth row, 0010 third column, (**8**)

S_1	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

Step 4: Permutation *P*



S-box output (32 bits)

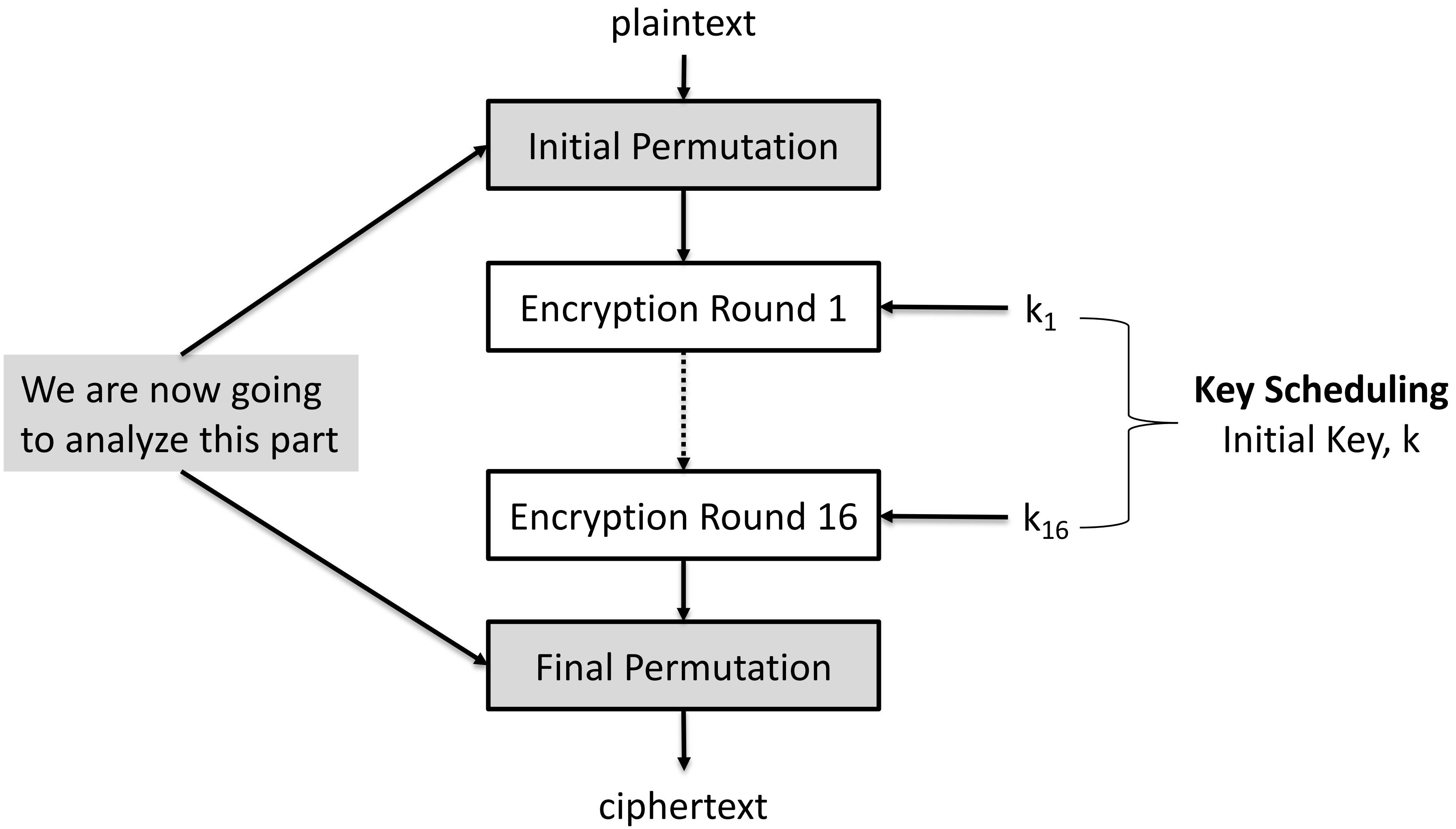
Permutation *P*

Output of *f* (32 bits)

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

First bit comes from bit 16,
second bit from bit 7, third from bit 20, etc.
Another diffusion element

DES Initial/Final Permutation



We are now going to analyze this part

The Permutations

IP							
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

IP^{-1}							
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

Initial and Final Permutation

- Do not offer any security
- Easy to implement in hardware by crosswiring
- It is *believed* that they were used to re-arrange the plaintext for faster and easier data fetches in 8-bit buses

Resources

- This lecture was built using material that can be found at
  - Chapter 7, Handbook of Applied Cryptography, http://cacr.uwaterloo.ca/hac/
  - Chapter 3, Understanding Cryptography, http://www.crypto-textbook.com