CS326 – Systems Security

Lecture 4

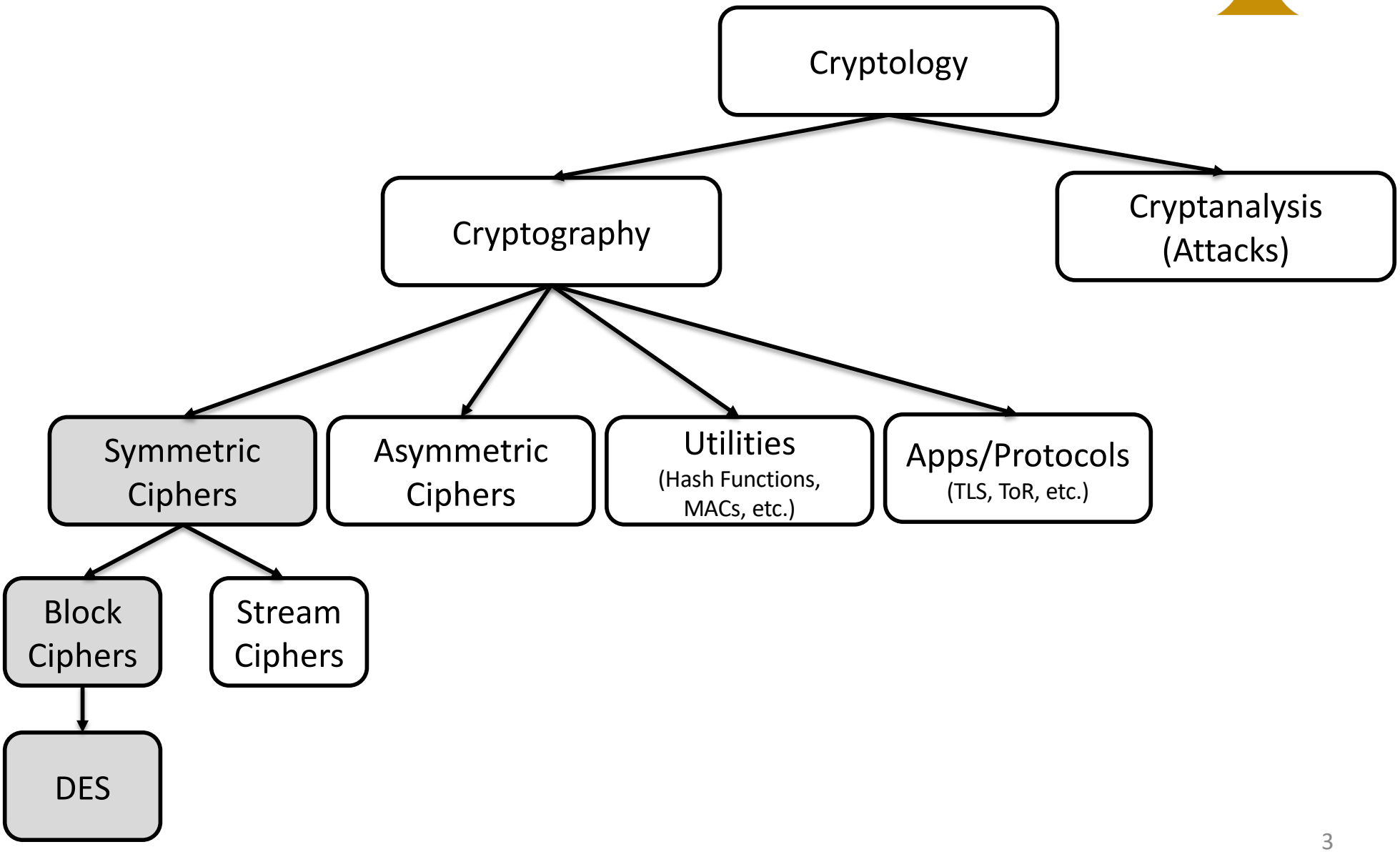
DES Key Scheduling

Elias Athanasopoulos
athanasopoulos.elias@ucy.ac.cy

Sections of this Lecture

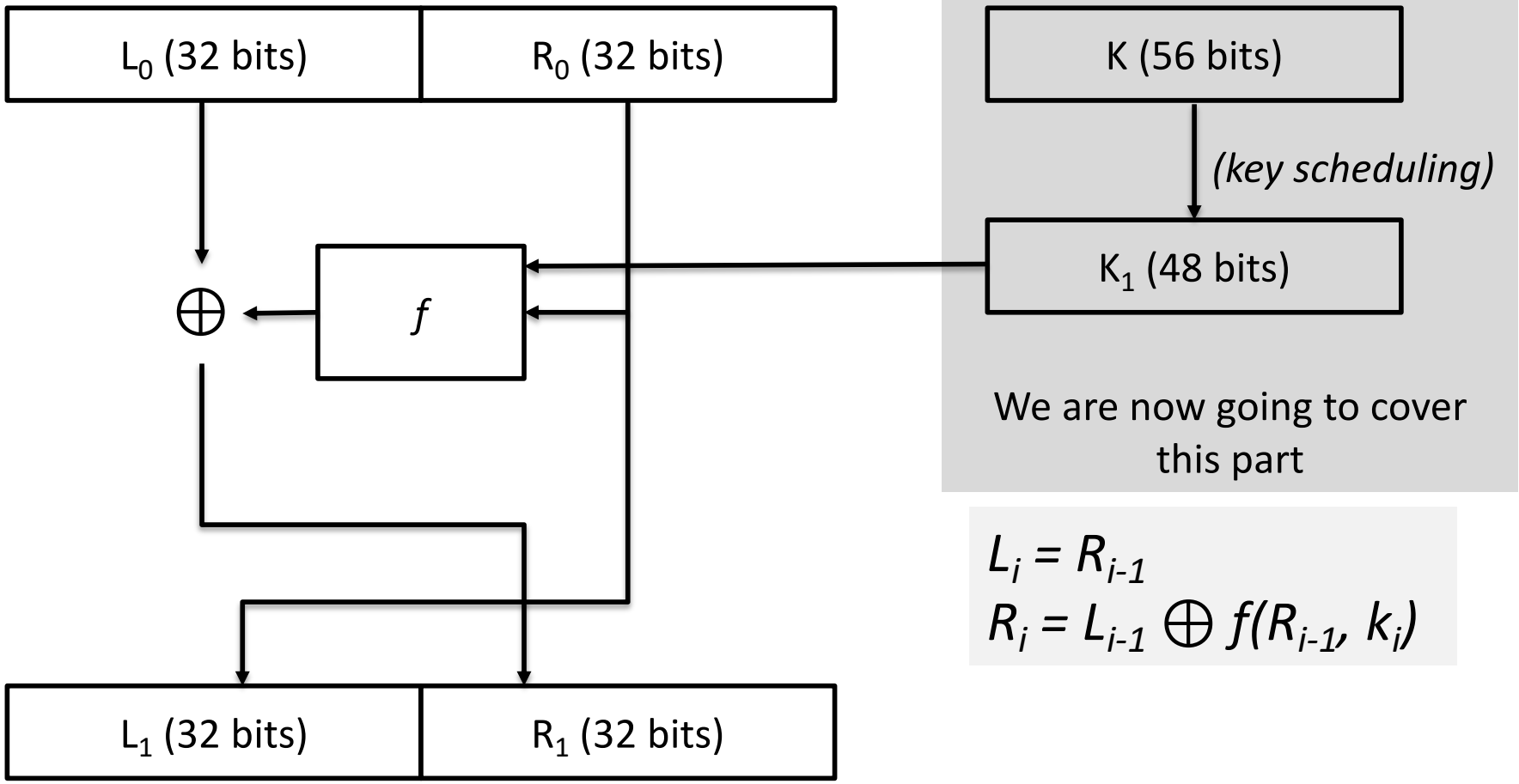
- DES Key Scheduling
- DES Decryption
- DES Security Analysis
- Alternatives

Cryptography Roadmap



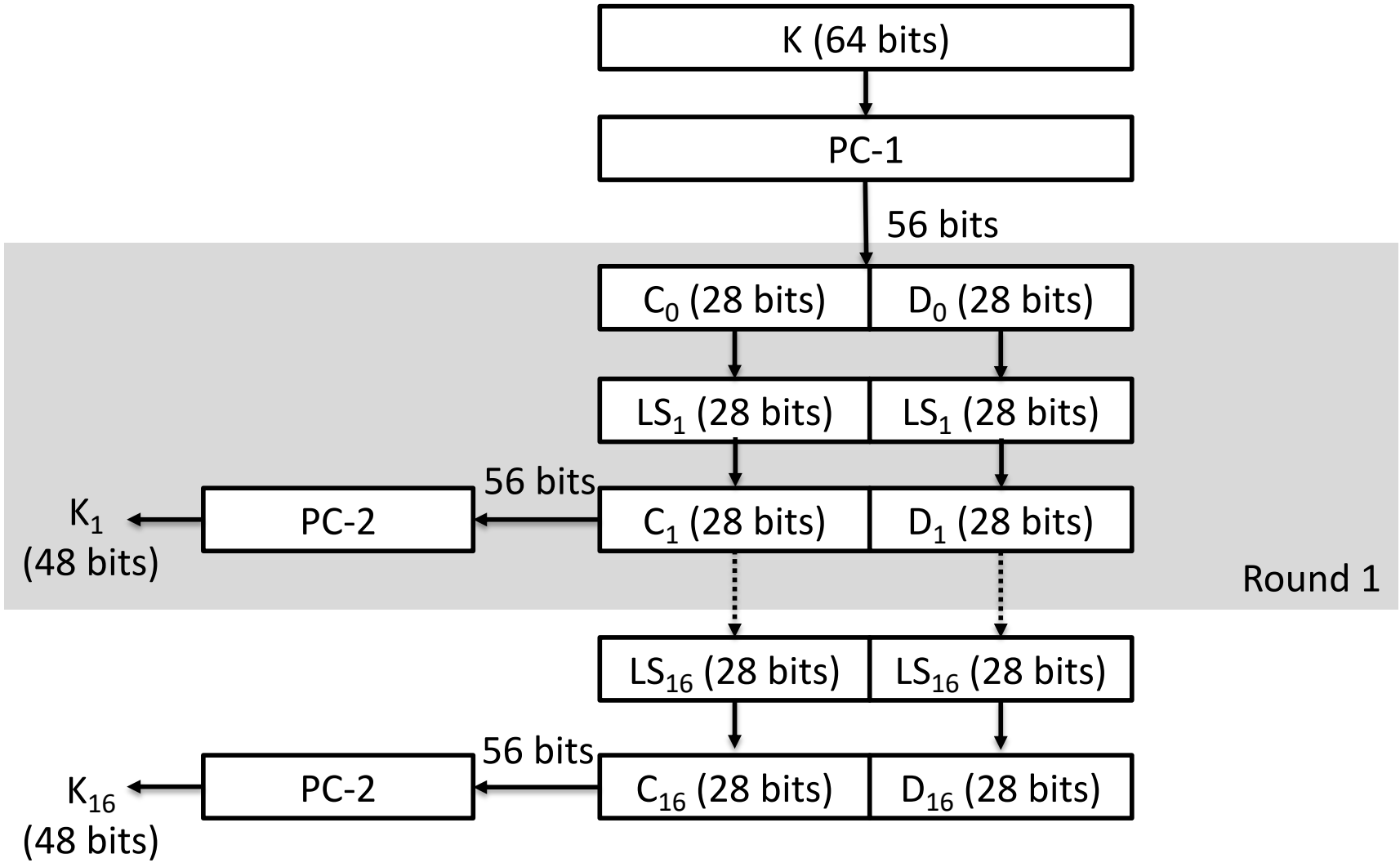
DES KEY SCHEDULING

DES Feistel Network



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

Key Schedule Overview



Key Permutations

- PC-1 and PC-2 are *permuted choice 1* and *permuted choice 2*
  - PC-1 takes 64 bits and drops the 8, output is 56 bits (effective key size)
  - PC-2 takes 56 bits and outputs 48
- LS_1 and LS_2 perform a *left shift* of the bits
  - For rounds 1, 2, 9, and 16 the shift involves 1 bit
  - For all other rounds the shift involves 2 bits
  - Final Round: 4x1 + 12x2 = 28 bits (C_0 and D_0 are equal to C_{16} and D_{16} – very important for the decryption process, since it is easy to derive K_{16} as easy it is to derive K_1)

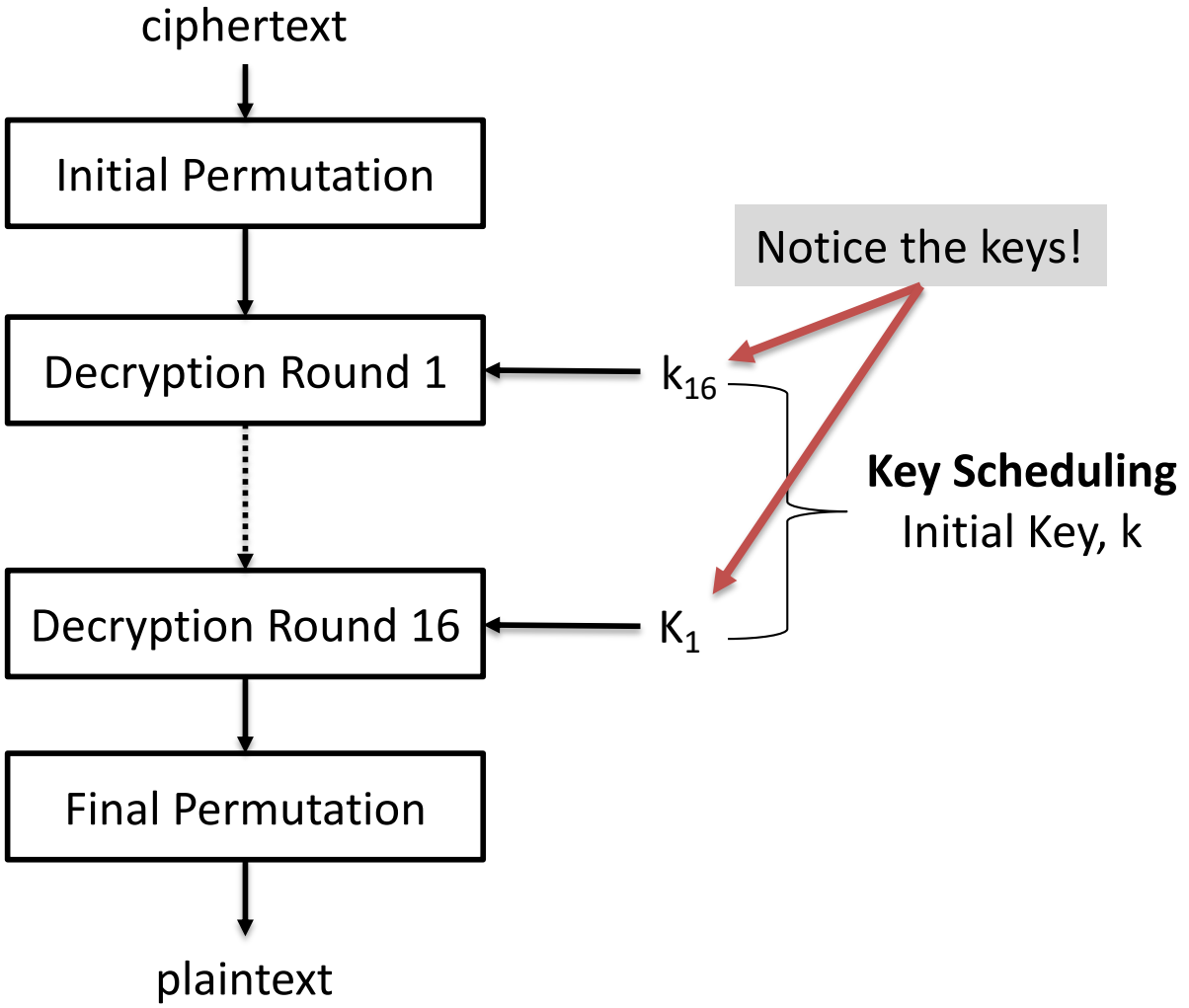
PC-1 and PC-2

PC-1							
57	49	41	33	25	17	9	1
58	50	42	34	26	18	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	14	6	61	53	45	37
29	21	13	5	28	20	12	4

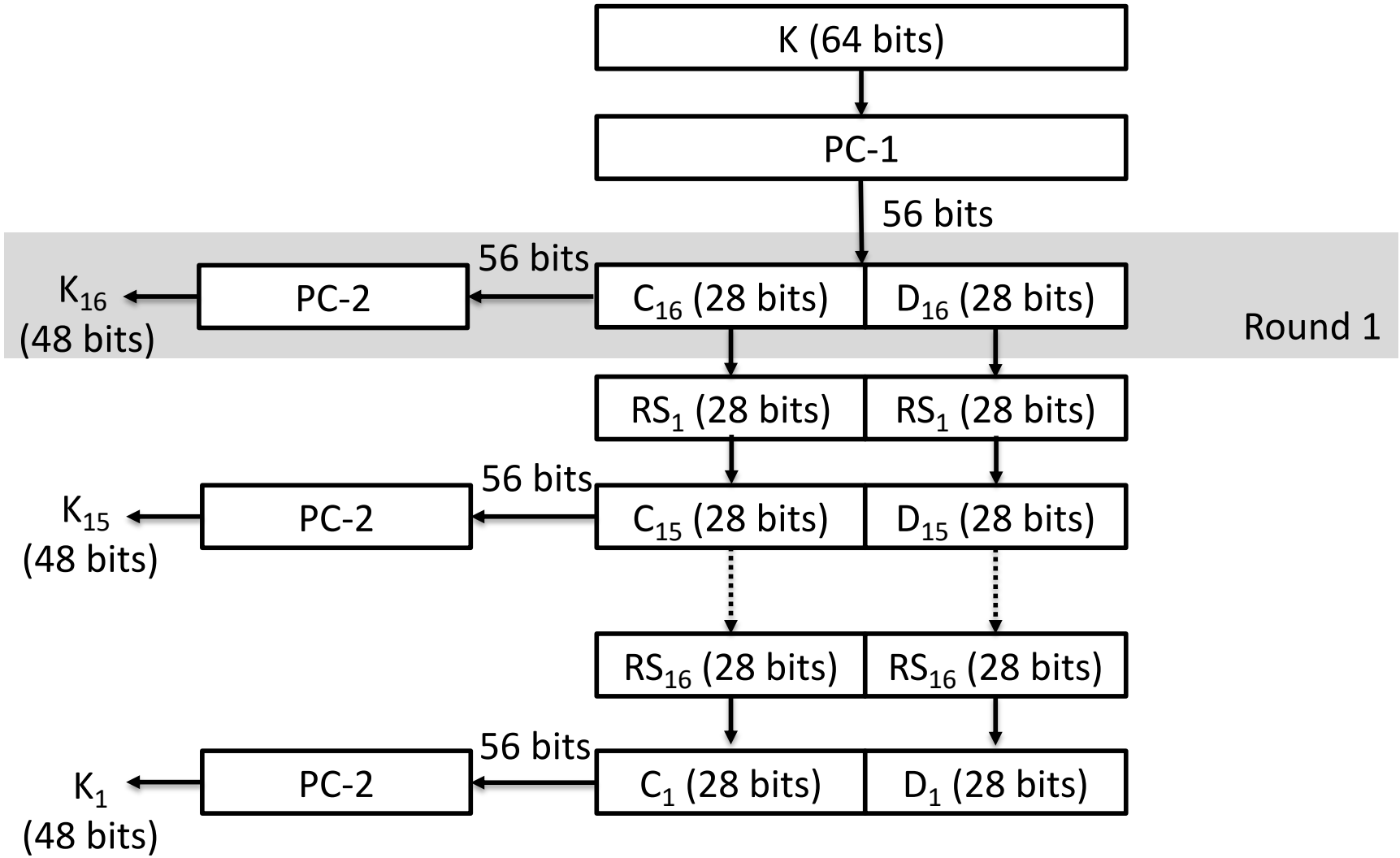
PC-2							
14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

DES DECRYPTION

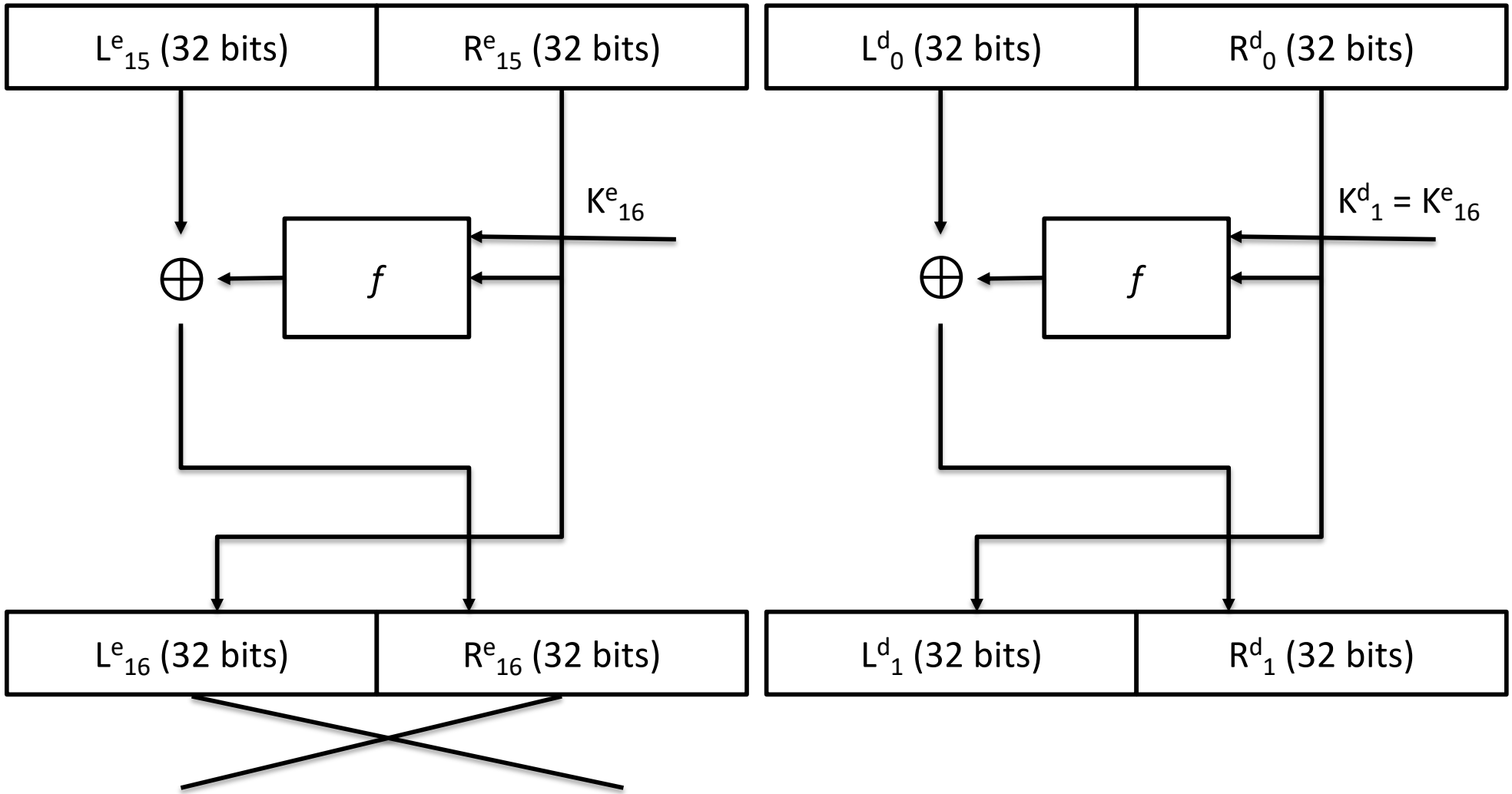
Decryption


ciphertext
Initial Permutation
Decryption Round 1
Decryption Round 16
Final Permutation
plaintext
Notice the keys!
k_{16}
K_1
Key Scheduling
Initial Key, k

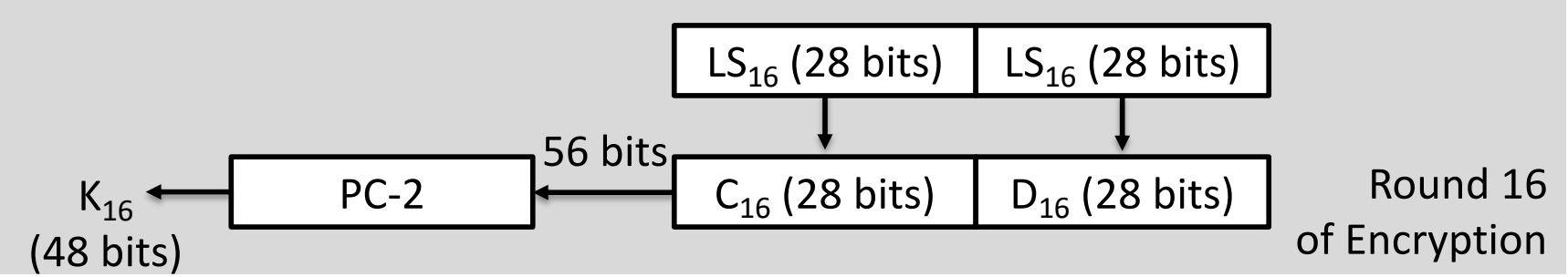
Reverse Key Schedule

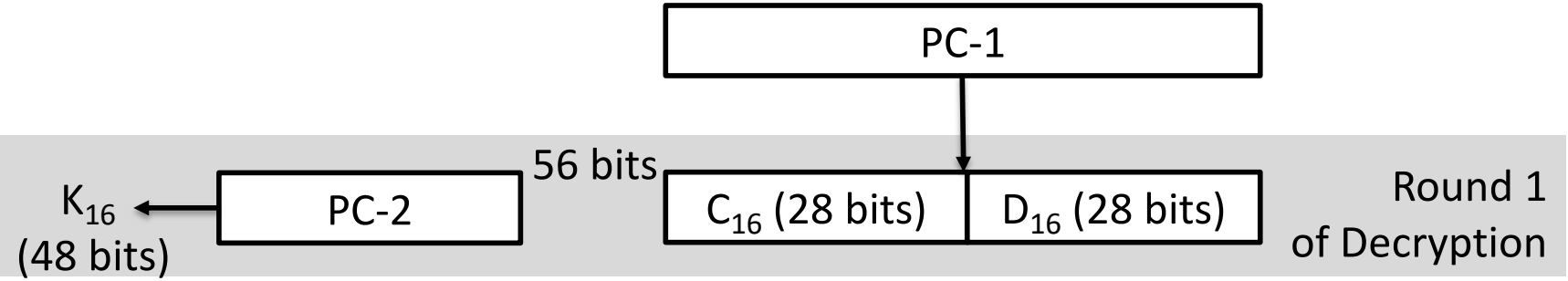


Decrypting the Feistel Network



Key Relationship





C_0 and D_0 are equal to C_{16} and D_{16} – very important for the decryption process, since it is easy to derive K_{16} as easy it is to derive K_1

Does it work?

Does it work?

- $L^d_1 = R^d_0 = L^e_{16} = R^e_{15}$

- $R^d_1 = L^d_0 \oplus f(R^d_0, K_{16}) = R^e_{16} \oplus f(L^e_{16}, K_{16})$
  $R^d_1 = (L^e_{15} \oplus f(R^e_{15}, K_{16})) \oplus f(R^e_{15}, K_{16})$
  $R^d_1 = L^e_{15} \oplus (f(R^e_{15}, K_{16}) \oplus f(R^e_{15}, K_{16})) = L^e_{15}$

DES SECURITY ANALYSIS

Brute-force the Key Space

- DES effective key size is 56 bits
- 1998
  - EFF constructed Deep Crack with a cost of less than $250K and cracked a DES key in 56 hours (see https://crack.sh)
- 2006
  - COPACOBANA based on FPGAs, can break a DES key in 7 days with a cost of less than $10K
- 2012
  - Cloud infrastructures can break a DES key in less than a day

Analytical Attacks

- Differential Cryptanalysis
  - A set of techniques for identifying how differences in information input can affect the resultant difference at the output
- Linear Cryptanalysis
  - Construct linear equations relating plaintext, ciphertext and key bits
  - Use these linear equations in conjunction with known plaintext-ciphertext pairs to derive key bits

Analytical Attacks

- S-box structure of DES is resistant in differential and linear cryptanalysis
  - A slight change of the numbers of an S-box can make DES very weak
- Differential Cryptanalysis
  - 2^{55} random plaintext-ciphertext pairs
  - 2^{47} particularly chosen plaintext-ciphertext pairs
- Linear Cryptanalysis
  - 2^{43} random plaintext-ciphertext pairs

ALTERNATIVES

Cipher	Key **Length**	**Remarks**
AES (Rinjndael)	128/192/256	DES replacement
3DES (*Triple DES)*	112 (effective)	DES hardened
Mars	128/192/256	AES finalist
RC6	128/192/256	AES finalist
Serpent	128/192/256	AES finalist
Twofish	128/192/256	AES finalist

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