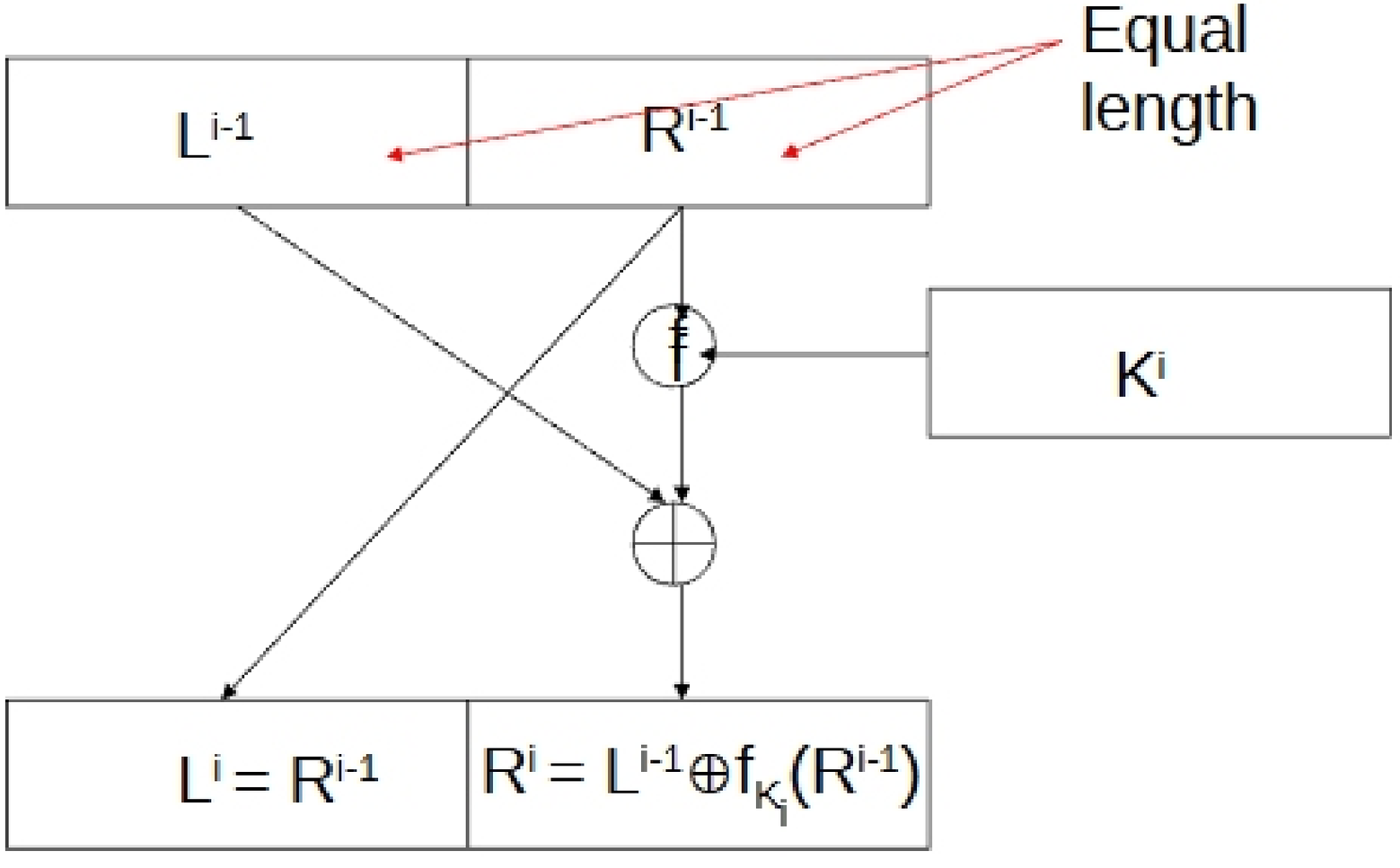
Block Ciphers: DES, SPNs, AES

CSCI283/172 Fall 2006

GWU

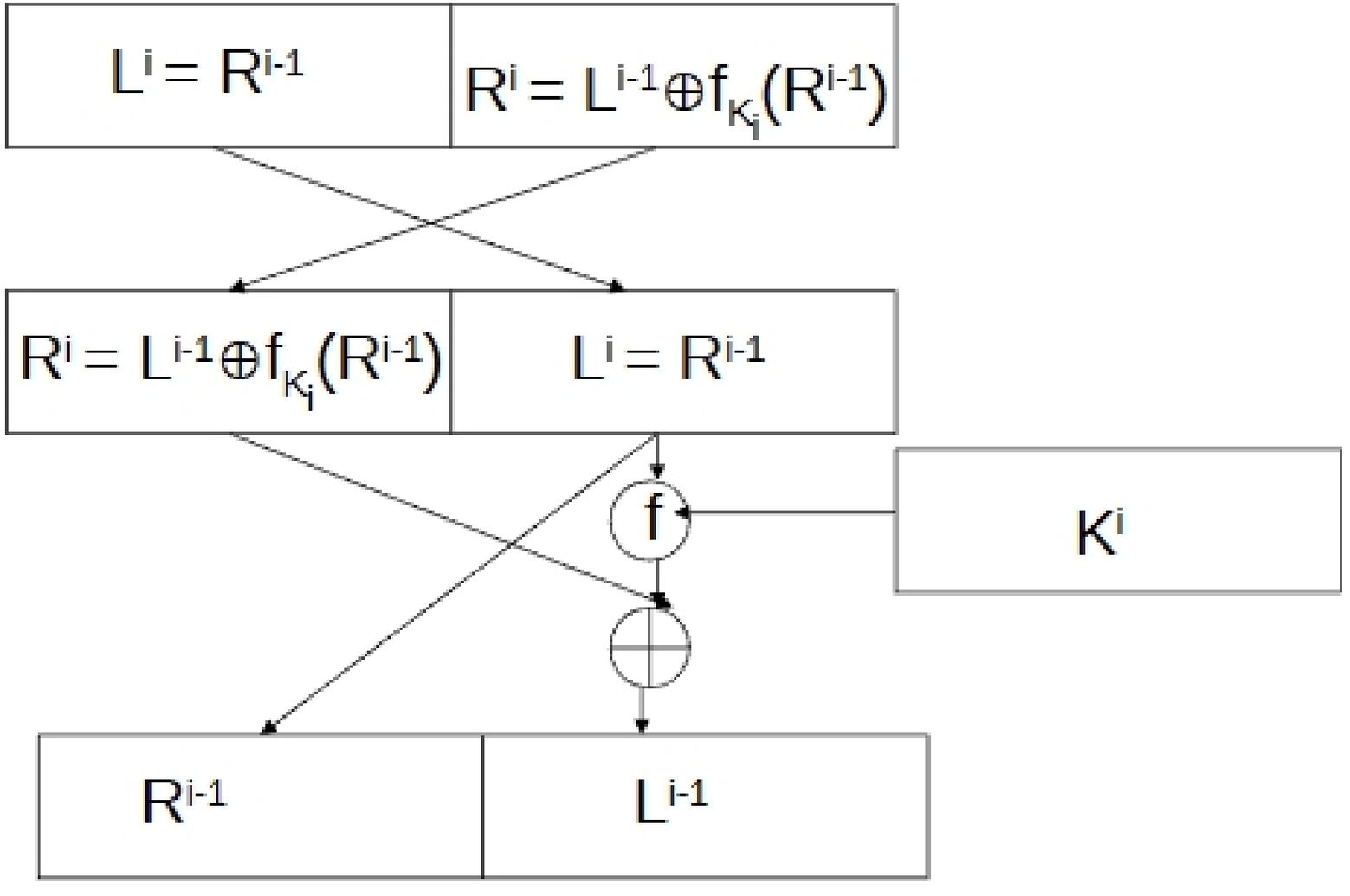
Some of this slide set is from: H. M. Heys, "A Tutorial on Linear and Differential Cryptanalysis", Technical Report CORR 2001-17, Centre for Applied Cryptographic Research, Department of Combinatorics and Optimization, University of Waterloo, Mar. 2001. (Also appears in Cryptologia, vol. XXVI, no. 3, pp. 189-221, 2002.)

One round of DES: Feistel Cipher



Some figures and accompanying text from Heys

Feistel Cipher Inverse



Some figures and accompanying text from Heys