哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY
立足航天，服务国防，面向国民经济主战场

计算机网络之危机四伏

主讲人：李全龙

本讲主题

密码学基础（4）

数据加密标准: DES

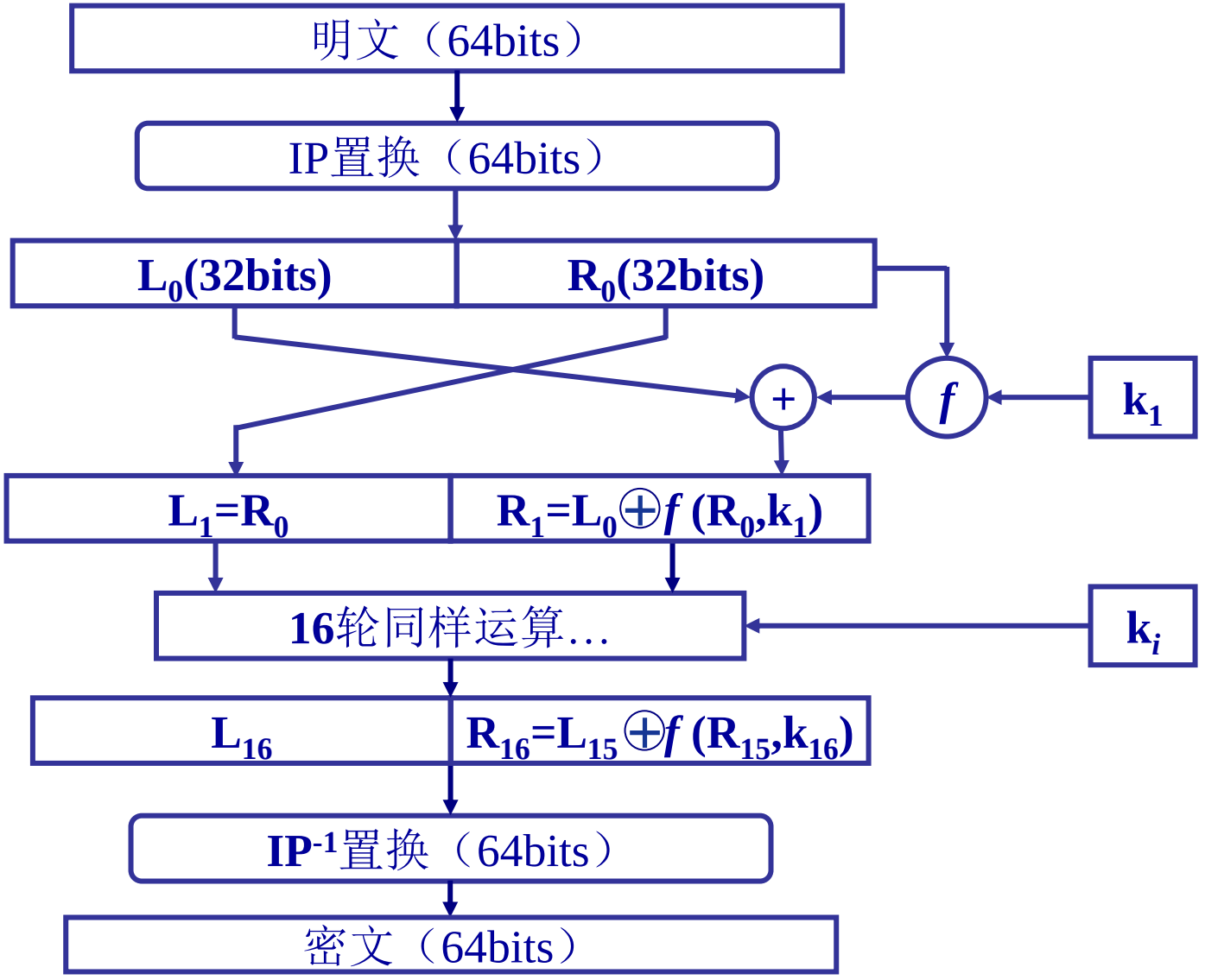
DES: Data Encryption Standard

- IBM公司研制
- 1972年，美国国家标准局NBS (National Bureau of Standards)开始实施计算机数据保护标准的开发计划。
- 1973年5月13日，NBS征集在传输和存贮数据中保护计算机数据的密码算法。
- 1975年3月17日，首次公布DES算法描述。
- 1977年1月15日，正式批准为加密标准(FIPS-46)，当年7月1日正式生效。
- 1994年1月的评估后决定1998年12月以后不再将DES作为数据加密标准。

数据加密标准：DES

- DES是16轮的Feistel结构密码
- DES是一个包含16个阶段的“替代--置换”的分组加密算法
- DES的分组长度是64位
  - 64位的分组明文序列作为加密算法的输入，经过16轮加密得到64位的密文序列
- DES使用56位的密钥
- DES的每一轮使用48位的子密钥
  - 每个子密钥是56位密钥的子集构成

DES算法结构


明文（64bits）
IP置换（64bits）
L_0(32bits)
R_0(32bits)
+
f
k_1
$L_1=R_0$
$R_1=L_0 \oplus f(R_0,k_1)$
16轮同样运算…
k_i
L_{16}
$R_{16}=L_{15} \oplus f(R_{15},k_{16})$
IP^{-1}置换（64bits）
密文（64bits）

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

立足航天，服务国防，面向国民经济主战场

谢 谢！