P134: 18, 19, 20

P154: 2, 3

1. 消息是 $\mathbb{Z}_n$ 中的整数序列，$m = (a_1, a_2, \ldots, a_t)$。

(a) 对于某个预定义好的 n，计算哈希值 $h(m) = \sum_{i=1}^{t} a_i$。这个哈希函数是否满足密码学哈希函数的要求？给出解释。

(b) 对于哈希函数 $h(m) = \sum_{i=1}^{t} a_i^2 \bmod n$，这个哈希函数是否满足密码学哈希函数的要求？给出解释。

(c) 当 $m = (198, 632, 900, 722, 349), n = 989$ 时，计算 (b) 中的哈希值。

2. 如何利用哈希函数构造类似 DES 结构的分组密码？

2025 年 4 月 2 日