

# Homework

1. What are two desirable properties of a hash function?

Nếu dùng cho hash table, database indexing, data structure:

- **Tính toán nhanh.**
- **Giảm thiểu xung đột giá trị.**

Nếu dùng cho bảo mật, mã hóa:

- **Không va chạm (Collision Resistance):** đảm bảo rằng hàm băm không dễ bị collision, tức là hai dữ liệu khác nhau không thể tạo ra cùng một giá trị băm.
  - **Chống nghịch ảnh (Pre-image Resistance):** không thể “khôi phục” hàm băm (không thể xác định được dữ liệu đầu vào dựa trên kết quả đầu ra).
2. Draw the 11-entry hash that results from using the hash function  $h(i) = (2i+5) \bmod 11$  to hash keys 12, 44, 13, 88, 23, 94, 11, 39, 20, 16, 5.

Key	12	44	13	88	23	94	11	39	20	16	5
$h(\text{key})$	7	5	9	5	7	6	5	6	1	4	4

a. Assume collisions are handled by chaining.

index	0	1	2	3	4	5	6	7	8	9	10
key		20			16	44	94	12		13	
					5	88	39	23			
						11					

b. Assume collisions are handled by linear probing.

index	0	1	2	3	4	5	6	7	8	9	10
key	11	39	20	5	16	44	88	12	23	13	94

3. Draw the 17-entry hash that results from using the hash function  $h(i) = (i+3) \bmod 17$  to hash keys 1, 3, 18, 8, 23, 35, 11, 36, 20, 16.

Key	1	3	18	8	23	35	11	36	20	16
$h(\text{key})$	4	6	4	11	9	4	14	5	6	2

- a. Assume collisions are handled by chaining
- b. Assume collisions are handled by linear probing

index	key		
0			
1			
2	16		
3			
4	1	18	35
5	36		
6	3	20	
7			
8			
9	23		
10			
11	8		
12			
13			
14	11		
15			
16			

index	key
0	
1	
2	16
3	
4	1
5	18
6	3
7	35
8	36
9	23
10	20
11	8
12	
13	
14	11
15	
16	