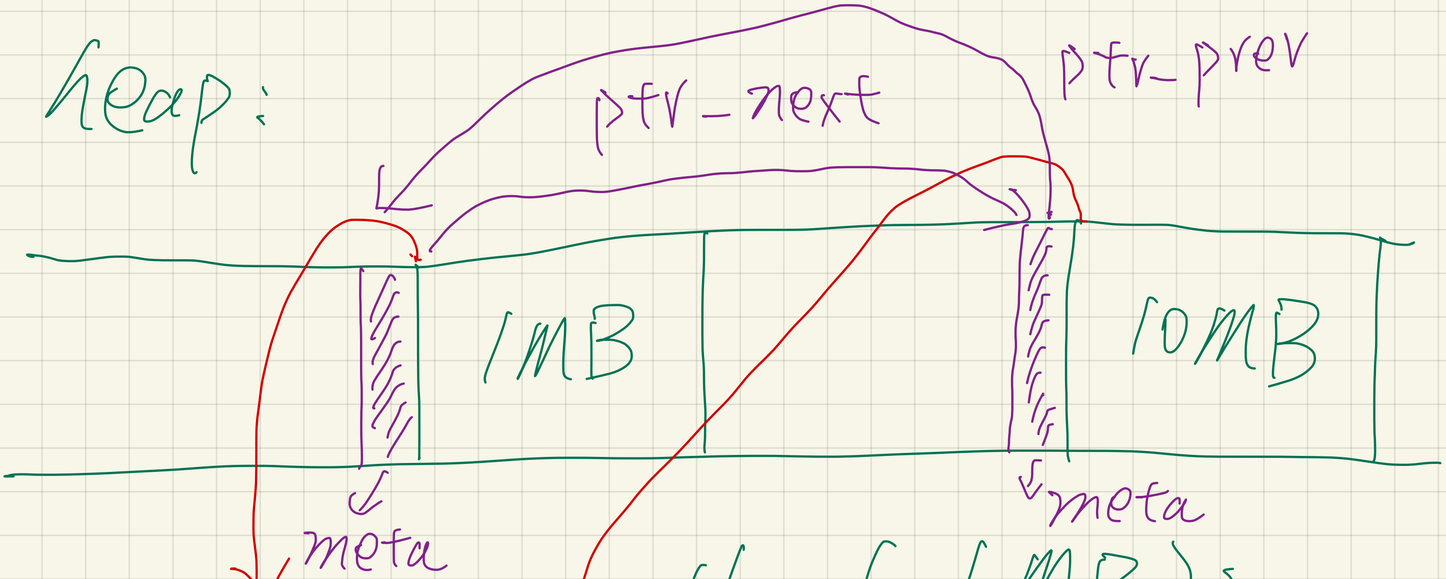
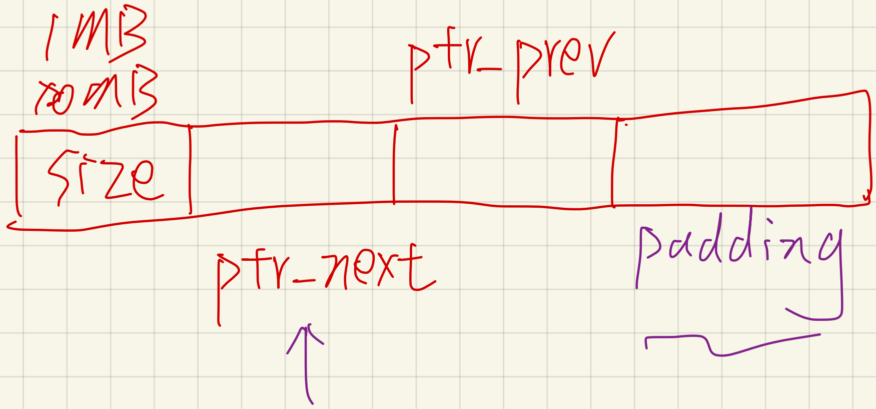
heap :



```
ptr1 = malloc(1MB);

ptr2 = malloc(10MB);
```

meta :

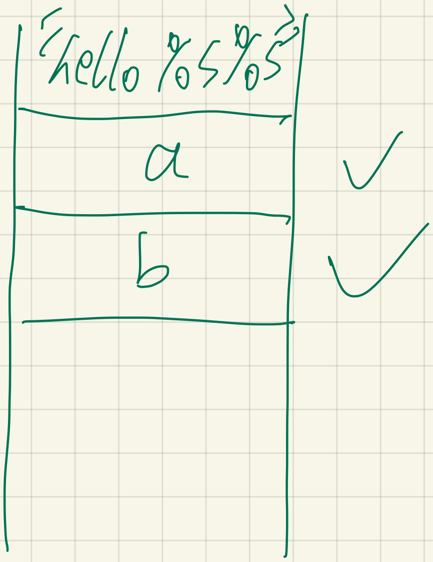


linked list
- chain of allocated block
- chain of freed block

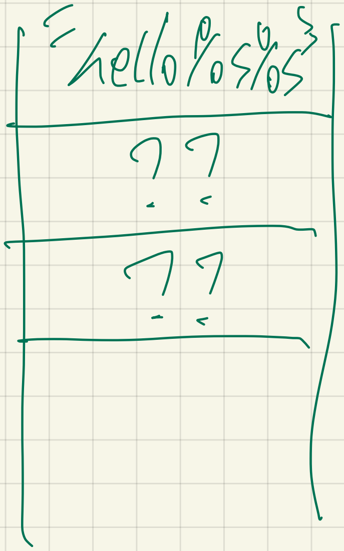
```
free(ptr1);

ptr3 = malloc(1MB);
```

format string:

printf("hello %s %s", a, b);



printf("hello %s %s");



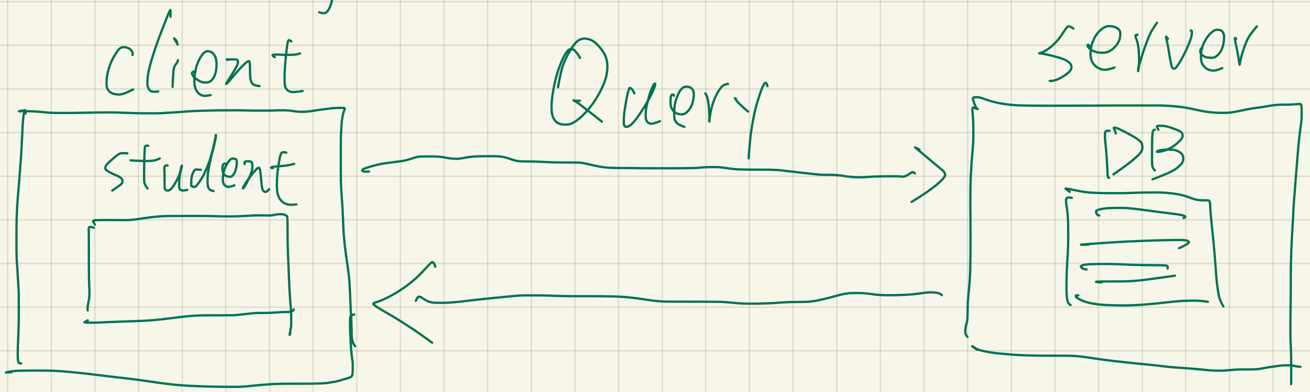
① legit

② ??

overread

attacker $\xrightarrow{\text{taint}}$ format string

SQL Injection:



“Alice” $\xrightarrow{\text{template}}$ Query → SQL

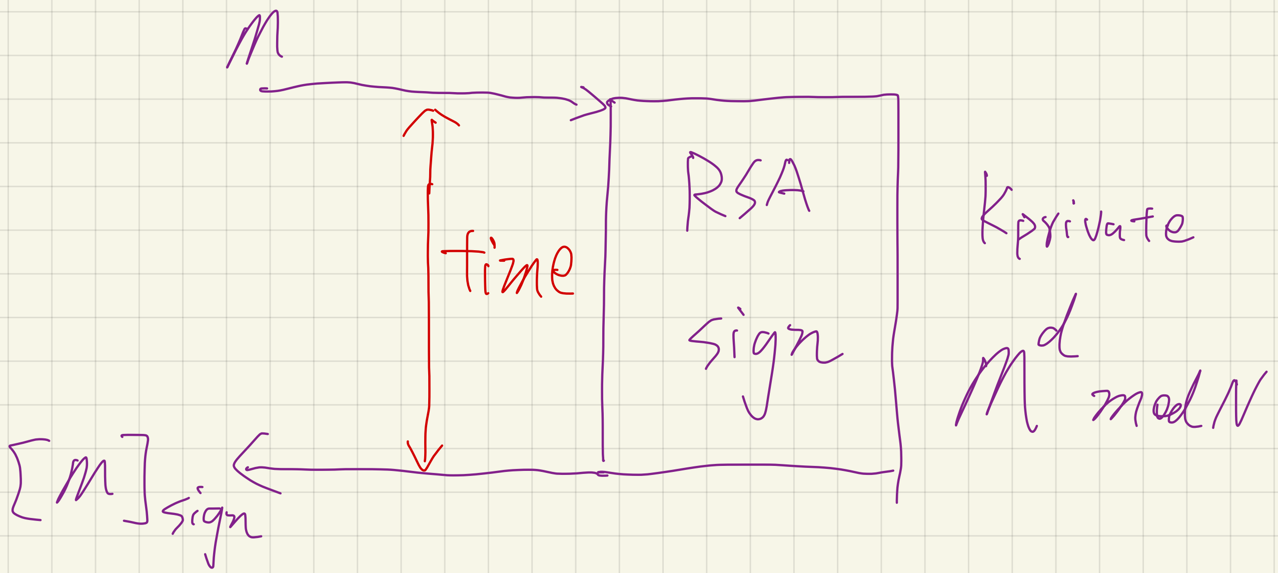
SELECT * FROM STUDENT WHERE $\underbrace{\text{NAME = “Alice”}}_{\text{true}}$;

“Alice” OR 1 = 1 ;

always true !!

SQL Injection:

Root cause → data
→ code



Math Induction: ✓

$i=0$ $\quad$ $i=N \Rightarrow i=N+1$

K_0 $\quad$ K_1 $\quad$ K_2 - - - - - $K_{n-1} \Rightarrow K_n$

↑ bit $\quad$ ↑ bit $\quad$ ↑ bit $\quad$ ↑ bit $\quad$ ↑ bit

m_1

m_2

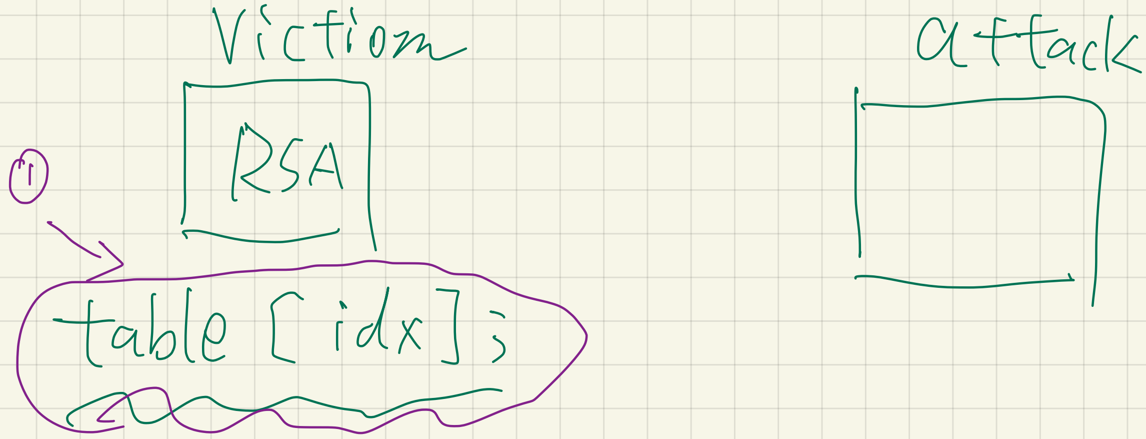
```
if ( $K_n == 1$ )
{ $T(m_1) \gg T(m_2)$
}
else
{ $T(m_1) = T(m_2)$
}
```

Square & multiply

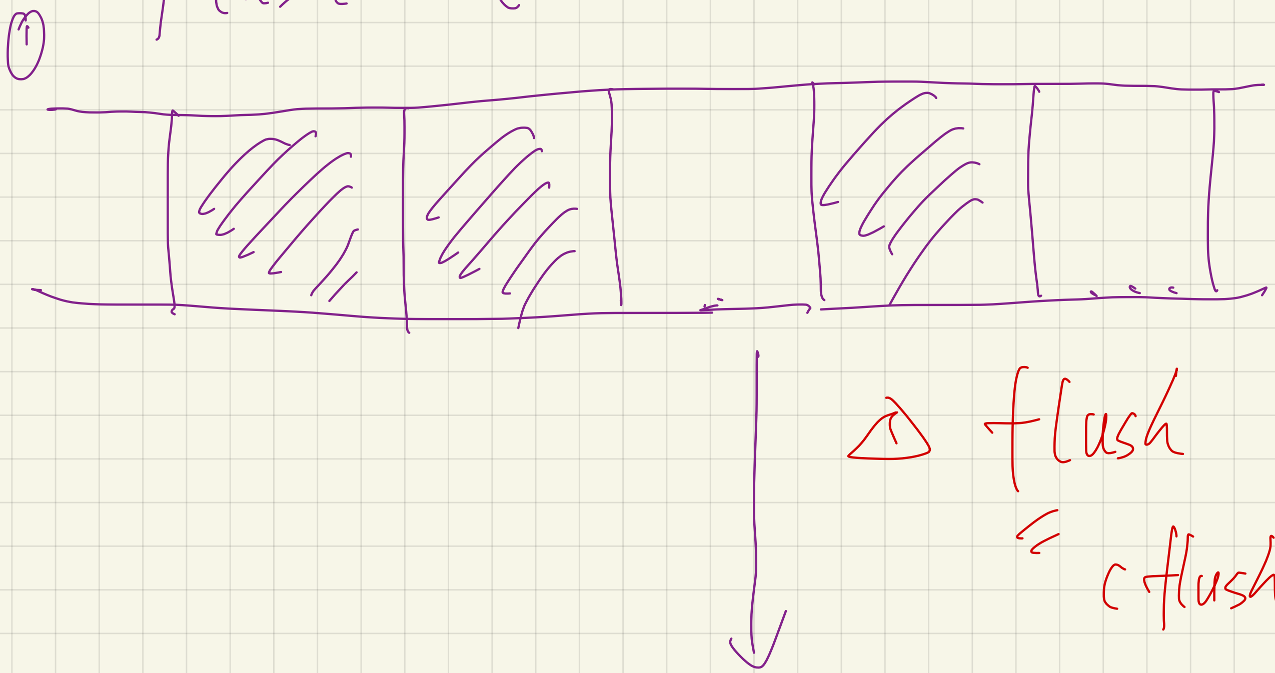
$x \cdot M_1 > N \implies \mathrm{mod}(x \cdot M_1, N)$

$\updownarrow$ timing diff

$x \cdot M_2 < N \implies \mathrm{mod}(x \cdot M_2, N)$

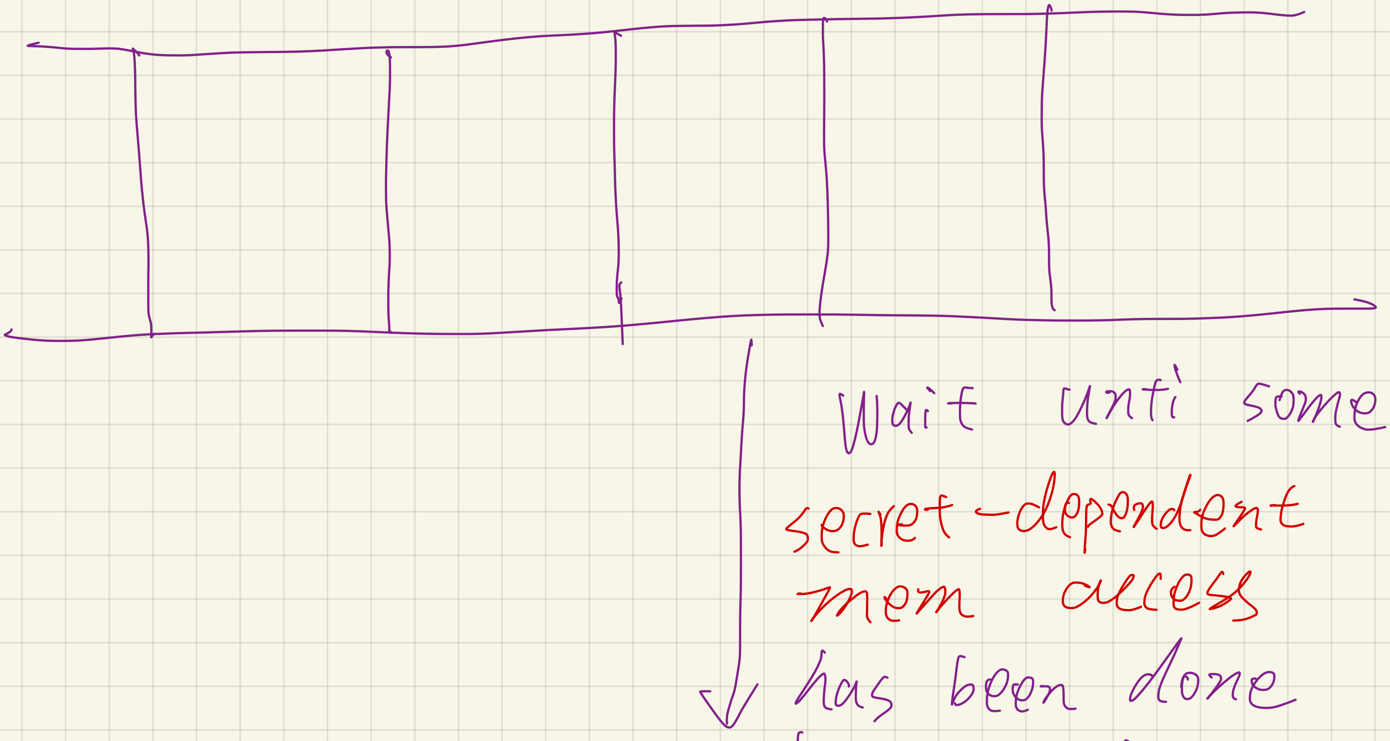


flush & Reload:

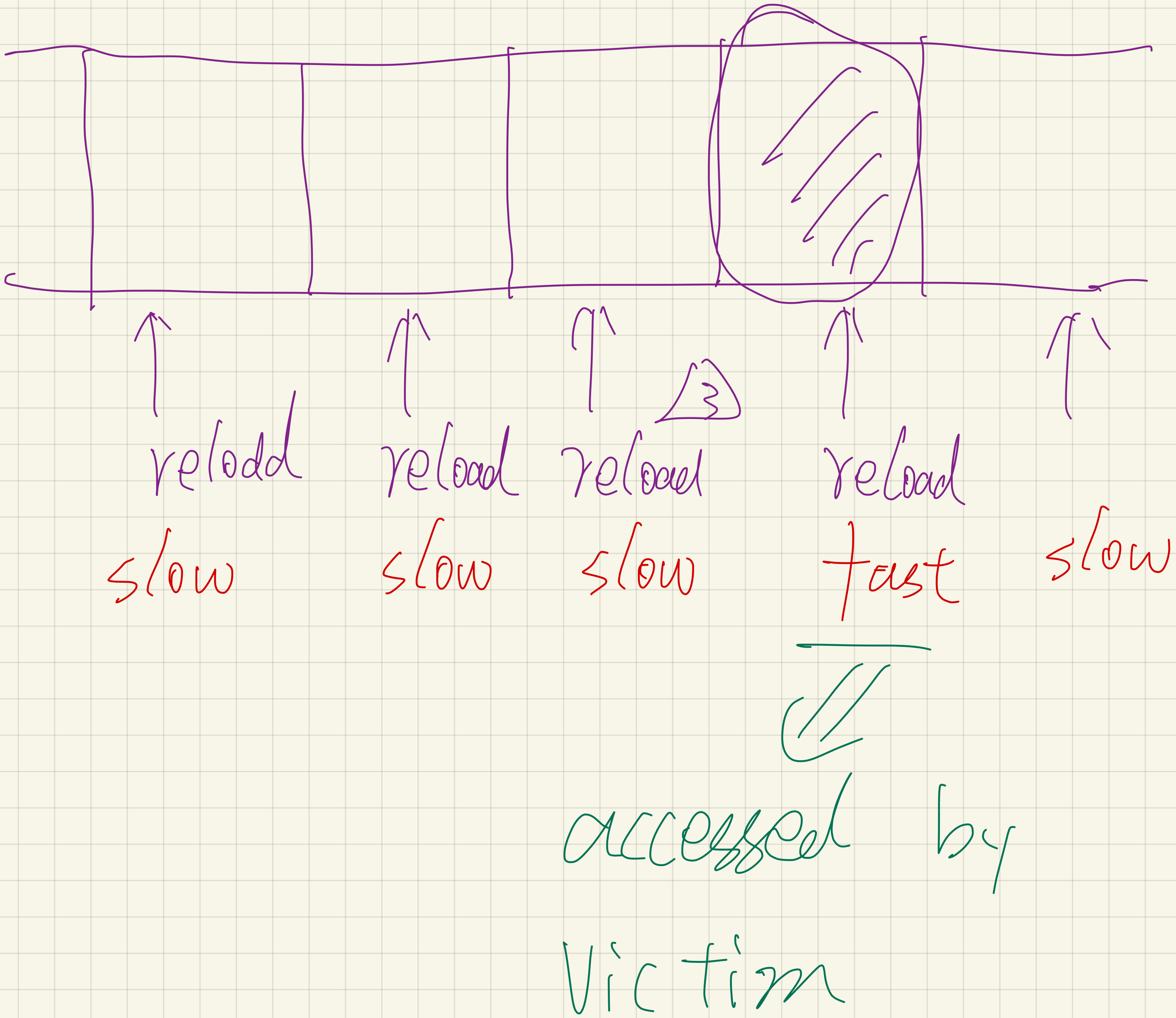


⚠ flush

= clflush



wait unti some secret-dependent mem access has been done by victim


reload
reload
reload
reload
slow
slow
slow
fast
slow
accessed by
Victim