phase-1

rax	return value
rsp	stack pointer
rdi	1
rsi	2
rdx	3
rcx	4
r8	5
r9	6

strings_not_equal(mystring, ans)

%rbx = mystring

%rbp = ans

%r12d = len(mystring)

0: %rdi = 0x603780

%rsi = 0x402400

%r12d = 1

%rdi = rbp = 0x402400 ⟶ 52

%rdx = %rdi

%rdx = %rdx + 1

%eax = %edx

%eax = %eax - %edi

为什么%rdi = 52? b * 0x4013d4

可知 phase1 52个字符.

6	0	3	7	8	0
8 4 2 1					
0 1 1 0	0 0 0 0	0 0 1 1	0 1 1 1	1 0 0 0	0 0 0 0

13	
8	

③ ②

%rdx = %rsi

%rcx = %rsi + 4

%rax = %rsi + 0x14

~~%rax~~

(%rsp + 8) = %rax