

0xcce

m[0x20] = 0x17

m[0x0] = c[0x4]

\$s2 = ad_mask & s[sha3(0x0, 0x40)]

m[\$m] = ad_mask & \$s2

return(\$m, 0x20)