D0029E - Message Digest (Lab 1)

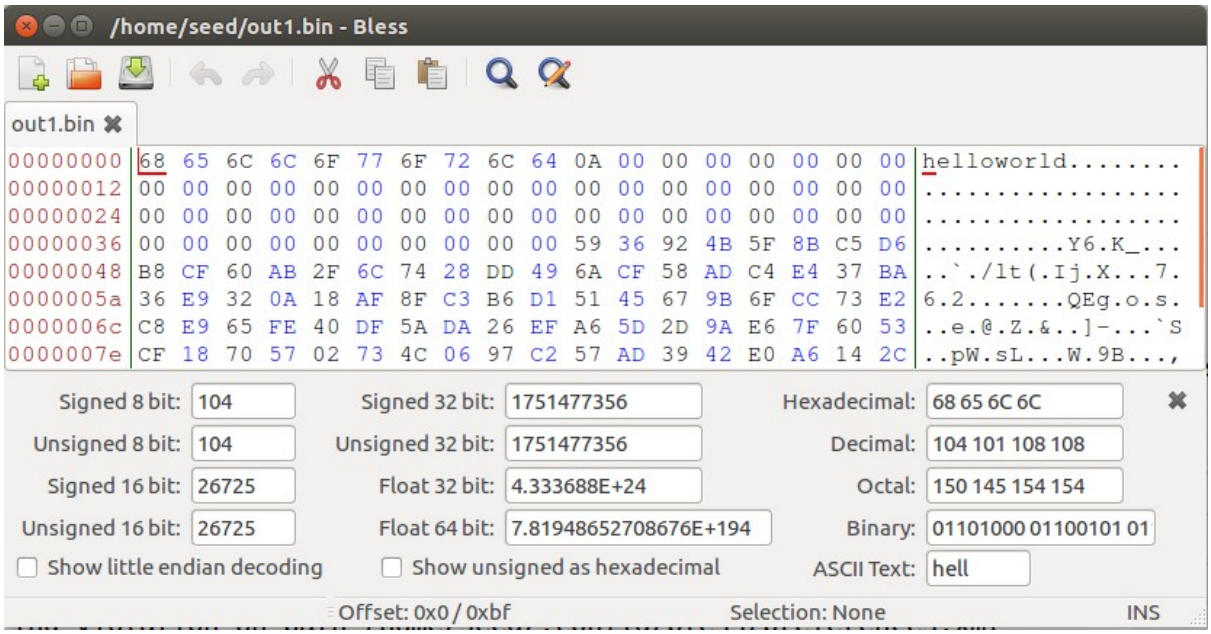
Martin Askolin*

Luleå tekniska universitet
971 87 Luleå, Sverige

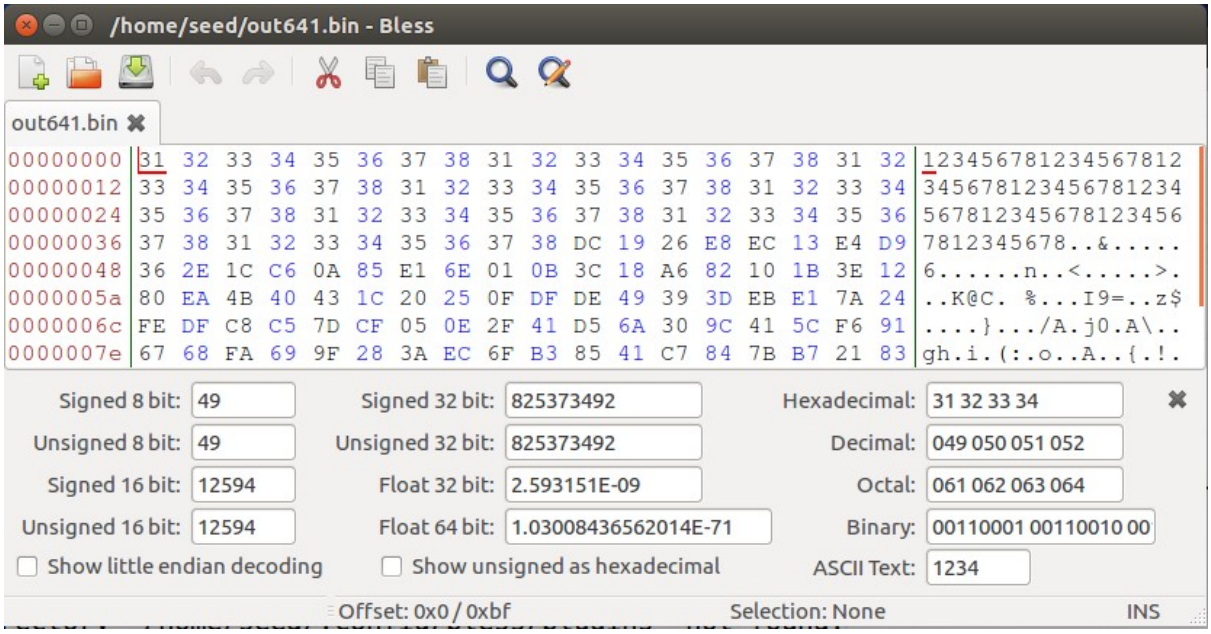
5 september 2021

*email: marsak-8@student.ltu.se

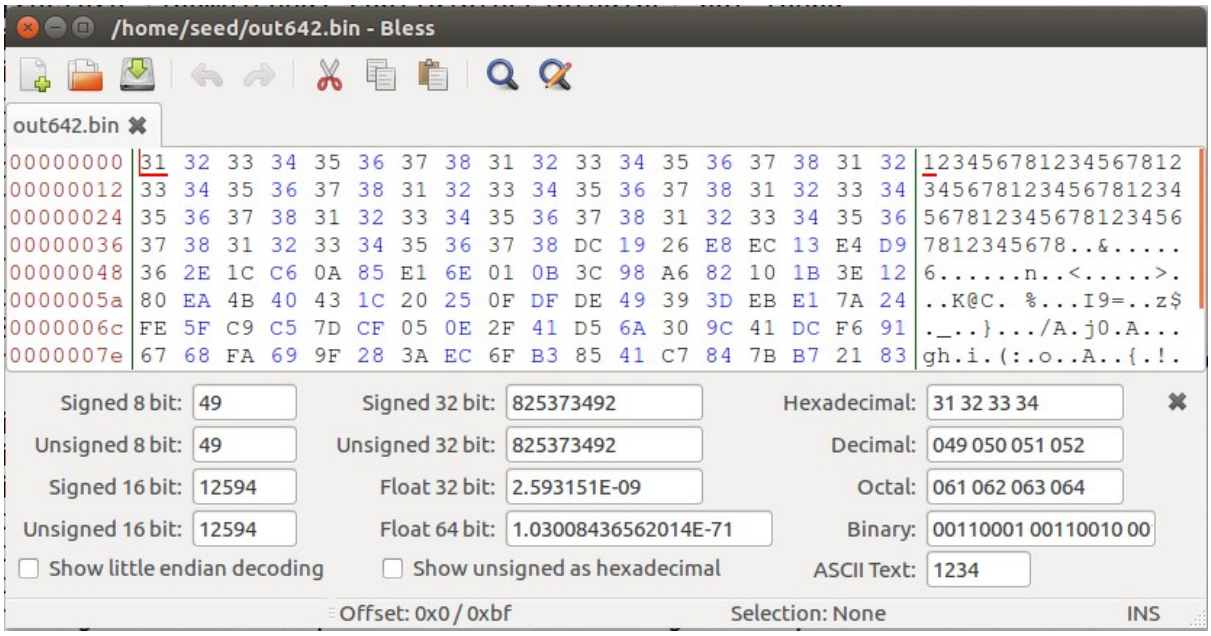
(1) If the length of your prefix file is not multiple of 64, what is going to happen? If the prefix is not a multiple of 64 bytes md5collgen will append x bytes of padding until the prefix + padding is a multiple of 64 bytes

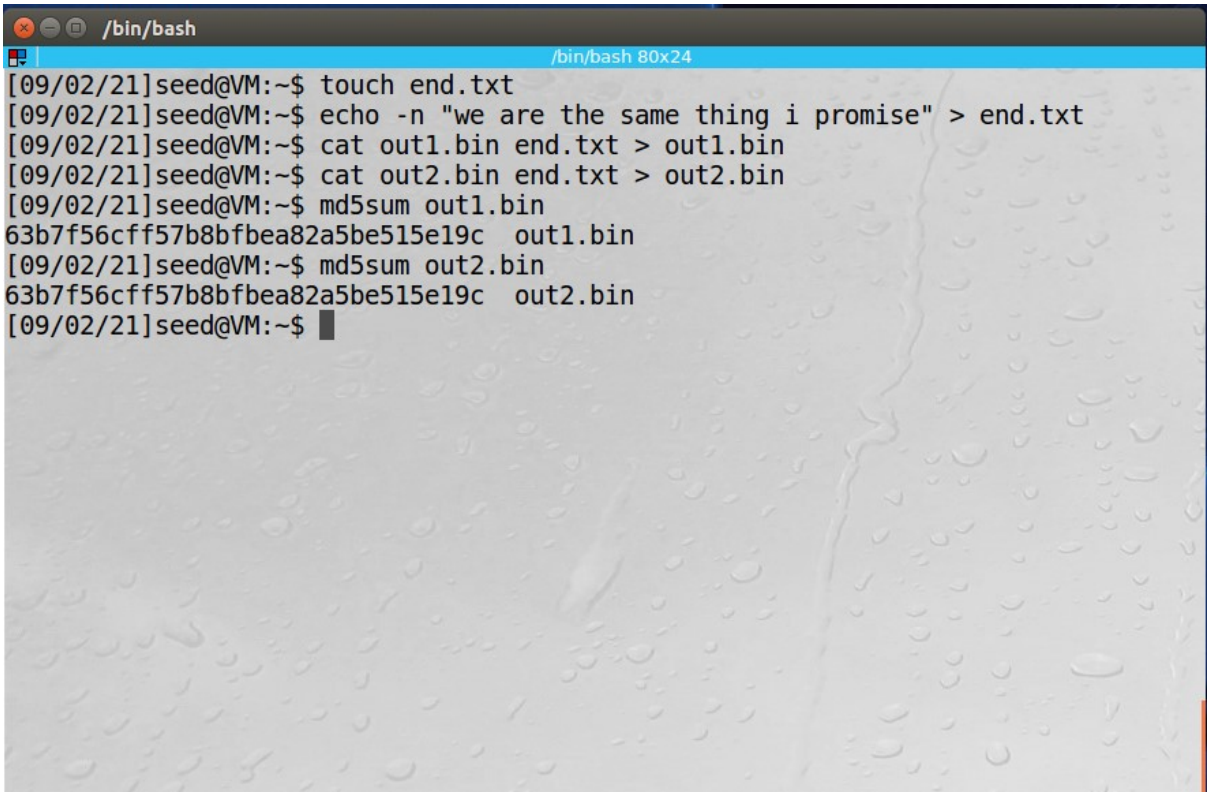


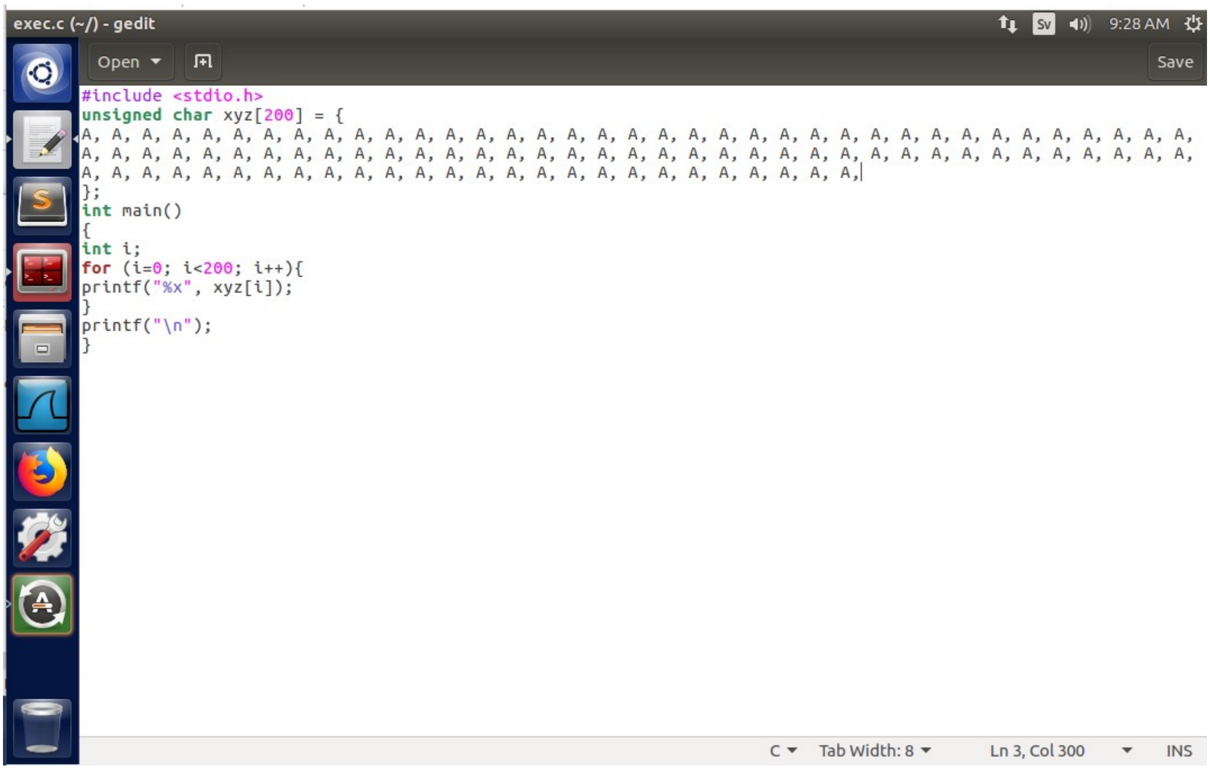
(2) Create a prefix file with exactly 64 bytes, and run the collision tool again, and see what happens. There is no padding added to the prefix this time.

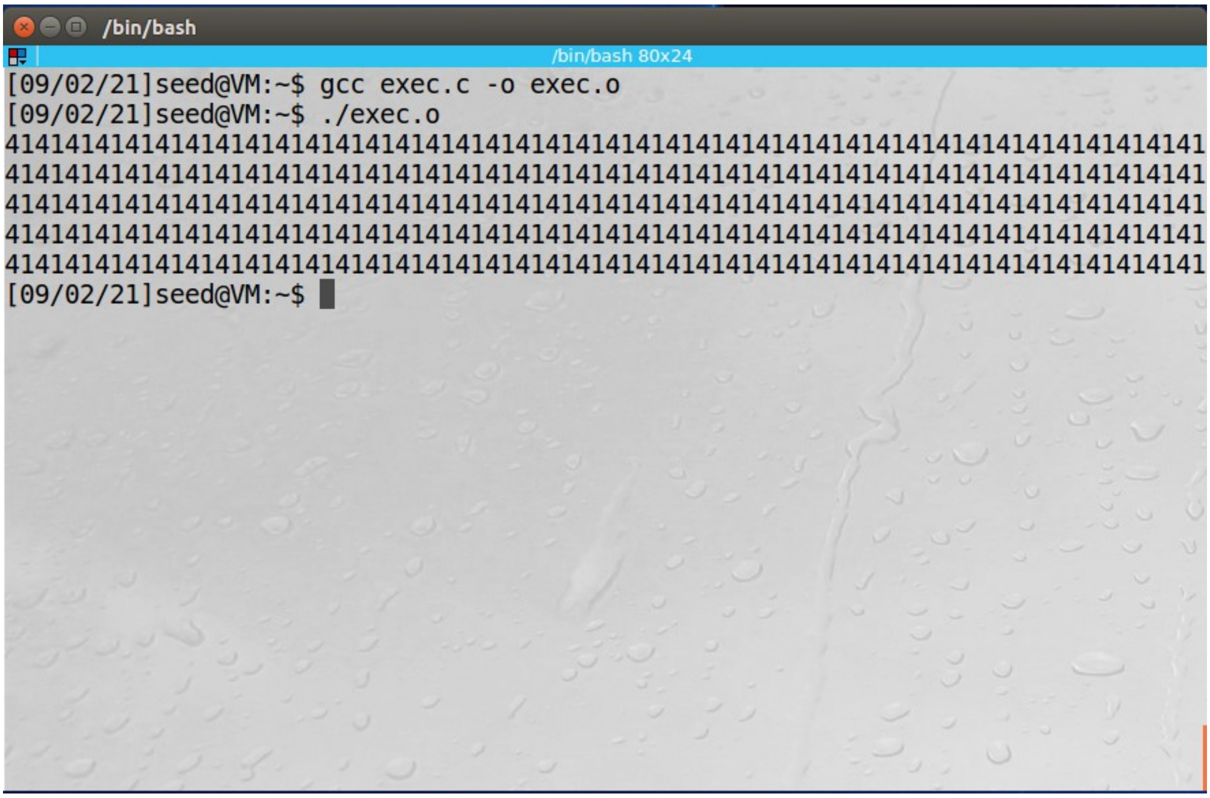


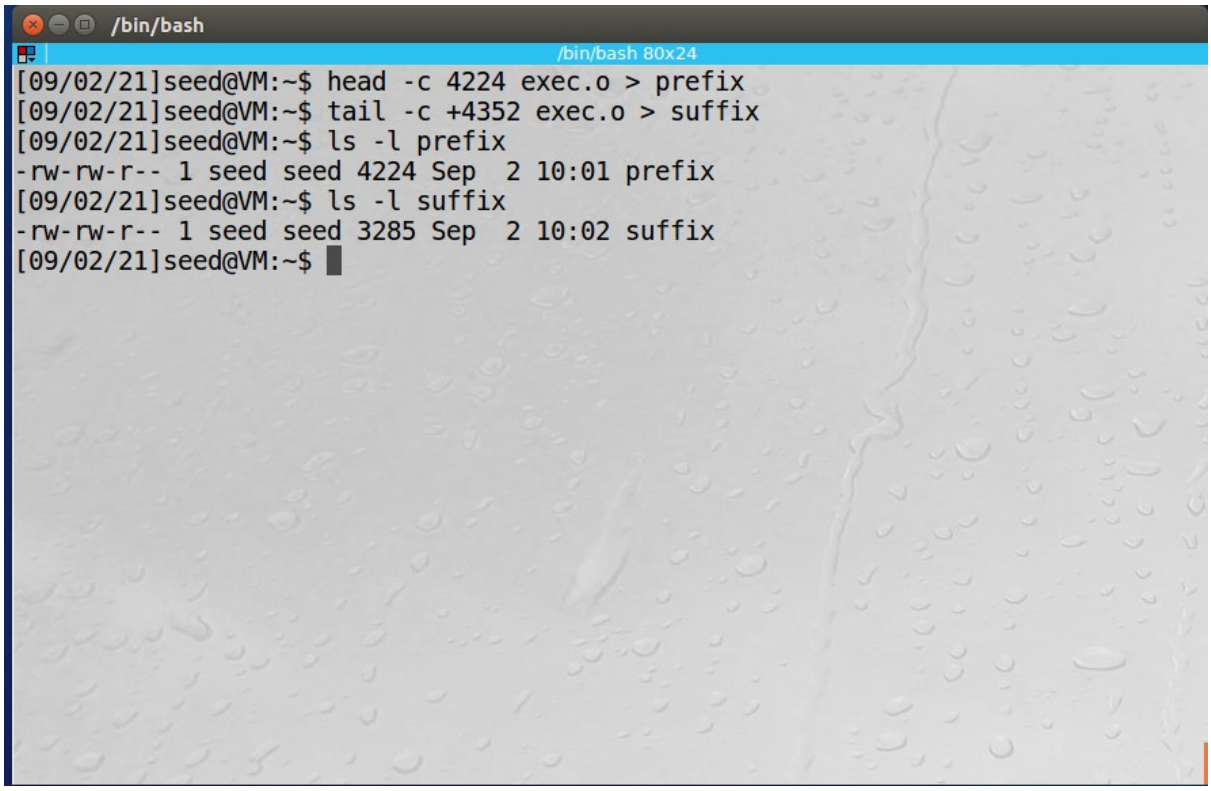
(3) Are the data (128 bytes) generated by md5collgen completely different for the two output files? Please identify all the bytes that are different.


/home/seed/out642.bin - Bless
out642.bin
00000000 31 32 33 34 35 36 37 38 31 32 33 34 35 36 37 38 31 32 1234567812345678
00000012 33 34 35 36 37 38 31 32 33 34 35 36 37 38 31 32 33 34 3456781234567812
00000024 35 36 37 38 31 32 33 34 35 36 37 38 31 32 33 34 35 36 5678123456781234
00000036 37 38 31 32 33 34 35 36 37 38 DC 19 26 E8 EC 13 E4 D9 7812345678..&.....
00000048 36 2E 1C C6 0A 85 E1 6E 01 0B 3C 98 A6 82 10 1B 3E 12 6......n..<.....>.
0000005a 80 EA 4B 40 43 1C 20 25 0F DF DE 49 39 3D EB E1 7A 24 ..K@C. %...I9=..z$
0000006c FE 5F C9 C5 7D CF 05 0E 2F 41 D5 6A 30 9C 41 DC F6 91 ._..}.../A.j0.A...
0000007e 67 68 FA 69 9F 28 3A EC 6F B3 85 41 C7 84 7B B7 21 83 gh.i.(:.o..A..{.!.
Signed 8 bit: 49
Signed 32 bit: 825373492
Hexadecimal: 31 32 33 34
Unsigned 8 bit: 49
Unsigned 32 bit: 825373492
Decimal: 049 050 051 052
Signed 16 bit: 12594
Float 32 bit: 2.593151E-09
Octal: 061 062 063 064
Unsigned 16 bit: 12594
Float 64 bit: 1.03008436562014E-71
Binary: 00110001 00110010 00
Show little endian decoding
Show unsigned as hexadecimal
ASCII Text: 1234
Offset: 0x0 / 0xbf
Selection: None
INS


/bin/bash
/bin/bash 80x24
[09/02/21]seed@VM:~$ touch end.txt
[09/02/21]seed@VM:~$ echo -n "we are the same thing i promise" > end.txt
[09/02/21]seed@VM:~$ cat out1.bin end.txt > out1.bin
[09/02/21]seed@VM:~$ cat out2.bin end.txt > out2.bin
[09/02/21]seed@VM:~$ md5sum out1.bin
63b7f56cff57b8bfbea82a5be515e19c out1.bin
[09/02/21]seed@VM:~$ md5sum out2.bin
63b7f56cff57b8bfbea82a5be515e19c out2.bin
[09/02/21]seed@VM:~$


exec.c (~/) - gedit
9:28 AM
Open
Save
#include <stdio.h>
unsigned char xyz[200] = {
A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A,
A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A,
A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A, A,
};
int main()
{
int i;
for (i=0; i<200; i++){
printf("%x", xyz[i]);
}
printf("\n");
}
C
Tab Width: 8
Ln 3, Col 300
INS


/bin/bash
/bin/bash 80x24
[09/02/21]seed@VM:~$ gcc exec.c -o exec.o
[09/02/21]seed@VM:~$ ./exec.o
41414141414141414141414141414141414141414141414141414141414141414141414141414141
41414141414141414141414141414141414141414141414141414141414141414141414141414141
41414141414141414141414141414141414141414141414141414141414141414141414141414141
41414141414141414141414141414141414141414141414141414141414141414141414141414141
41414141414141414141414141414141414141414141414141414141414141414141414141414141
[09/02/21]seed@VM:~$




```
[09/02/21]seed@VM:~$ md5collgen -p prefix -o p.bin q.bin
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'p.bin' and 'q.bin'
Using prefixfile: 'prefix'
Using initial value: 87d0f8ac71d4d1b0e33287e897409fd3

Generating first block: ................
Generating second block: S00........
Running time: 10.5395 s
[09/02/21]seed@VM:~$
[09/02/21]seed@VM:~$ cat p.bin suffix > harmful.o
[09/02/21]seed@VM:~$ cat q.bin suffix > harmless.o
```

```
[09/02/21]seed@VM:~$ md5sum harmful.o
e56f82d8a4ca4e1b2133e904e38b6b1f  harmful.o
[09/02/21]seed@VM:~$ md5sum harmless.o
e56f82d8a4ca4e1b2133e904e38b6b1f  harmless.o
[09/02/21]seed@VM:~$
[09/02/21]seed@VM:~$
[09/02/21]seed@VM:~$ ls -l harmful.o
-rw-rw-r-- 1 seed seed 7637 Sep  2 10:36 harmful.o
[09/02/21]seed@VM:~$ ls -l harmless.o
-rw-rw-r-- 1 seed seed 7637 Sep  2 10:36 harmless.o
```

```
[09/02/21]seed@VM:~$ chmod u+x harmless.o
[09/02/21]seed@VM:~$ chmod u+x harmful.o
[09/02/21]seed@VM:~$
[09/02/21]seed@VM:~$ ./harmless.o
41414141414141414141414141414141414141414141414141414141414141414141414141414141
41414141414141414141414141414141414141414141414141d0ab6fe5269564c7eebe3916642f1476
43e36366cb157b15dce7bda73fcb0c6242fdc4f982a9b5ebfd6552cfaf3cc6c5b8d86ff74b5ce588
35a3f594fc83527e6518897557f17ab9e14cd839ad533fced541ef17f9e060d1dbf4c8d03079ae4b
6b96fe31eba2e2d170a1fa9ce6e2ae83cd7abc62e636eca55ade137fb73c54141414141414141
[09/02/21]seed@VM:~$ ./harmful.o
41414141414141414141414141414141414141414141414141414141414141414141414141414141
41414141414141414141414141414141414141414141414141d0ab6fe5269564c7eebe3916642f1476
43e36b66cb157b15dce7bda73fcb0c6242fdc4f982a9b5ebfd6552cf2f3cc6c5b8d86ff74b5ce588
35a37594fc83527e6518897557f17ab9e14cd839ad533fced5416f17f9e060d1dbf4c8d03079ae4b
6b96fe31eba2e2d170a1fa94e6f2ae83cd7abc62e636eca55ad6137fb73c54141414141414141
```

```
int isHarmless(){
        int i;
        for (i=0; i<200; i++){
                if (X[i] != Y[i]) { return 0; }
        }

        return 1;
}

void harmful(){
        printf("*Doing harmful stuff* \n");
}

void harmless(){
        printf("*Doing harmless stuff* \n");
}

int main()
{
        if (isHarmless() == 1) {harmless();}
        else {harmful();}
}
```

```
[09/03/21]seed@VM:~$ md5sum out1
54c7ee75bedf75f9919c3f8e31dd00e5  out1
[09/03/21]seed@VM:~$ md5sum out2
54c7ee75bedf75f9919c3f8e31dd00e5  out2
[09/03/21]seed@VM:~$
[09/03/21]seed@VM:~$ tail -c 128 out1 > p
[09/03/21]seed@VM:~$
[09/03/21]seed@VM:~$ cat out1 suffixprefix p suffixsuffix > harmless.o
[09/03/21]seed@VM:~$ cat out2 suffixprefix p suffixsuffix > harmful.o
[09/03/21]seed@VM:~$
[09/03/21]seed@VM:~$ md5sum harmless.o
c69f62a97e03fe3588b73e5584cc6ca7  harmless.o
[09/03/21]seed@VM:~$ md5sum harmful.o
c69f62a97e03fe3588b73e5584cc6ca7  harmful.o
[09/03/21]seed@VM:~$
[09/03/21]seed@VM:~$ chmod u+x harmless.o
[09/03/21]seed@VM:~$ chmod u+x harmful.o
[09/03/21]seed@VM:~$
[09/03/21]seed@VM:~$ ./harmless.o
*Doing harmless stuff*
[09/03/21]seed@VM:~$ ./harmful.o
*Doing harmful stuff*
[09/03/21]seed@VM:~$
```