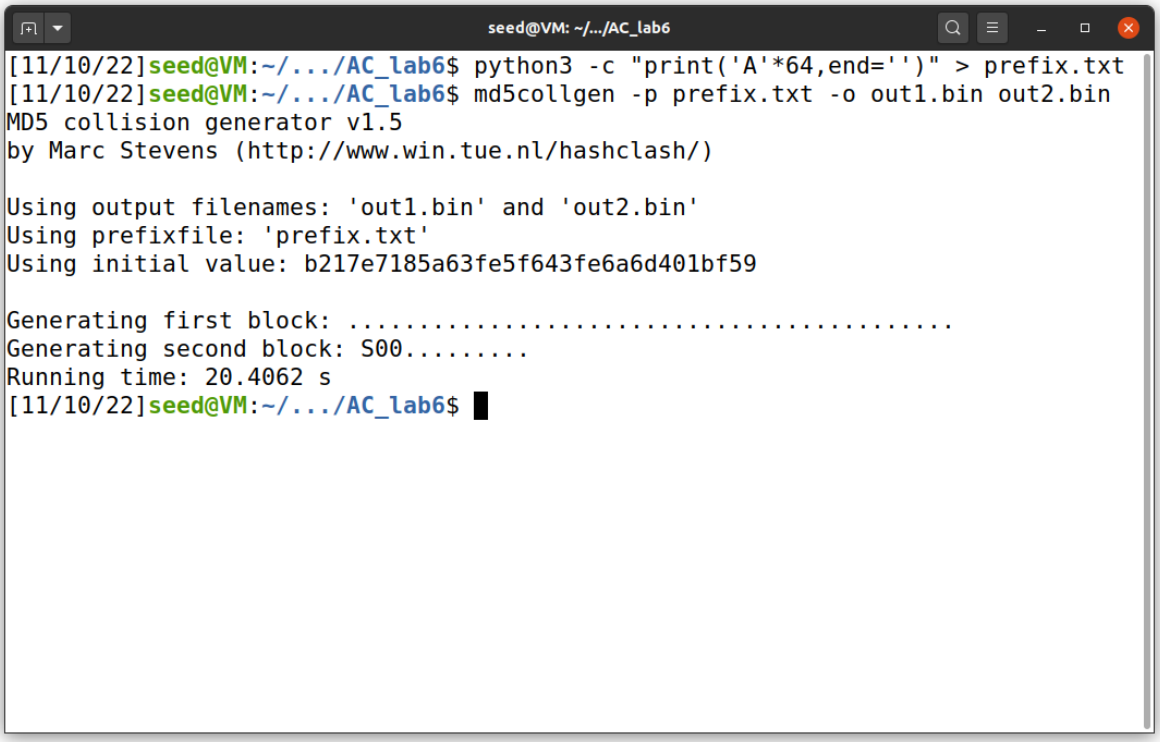
APPLIED CRYPTOGRAPHY

NAME: VISHWAS M

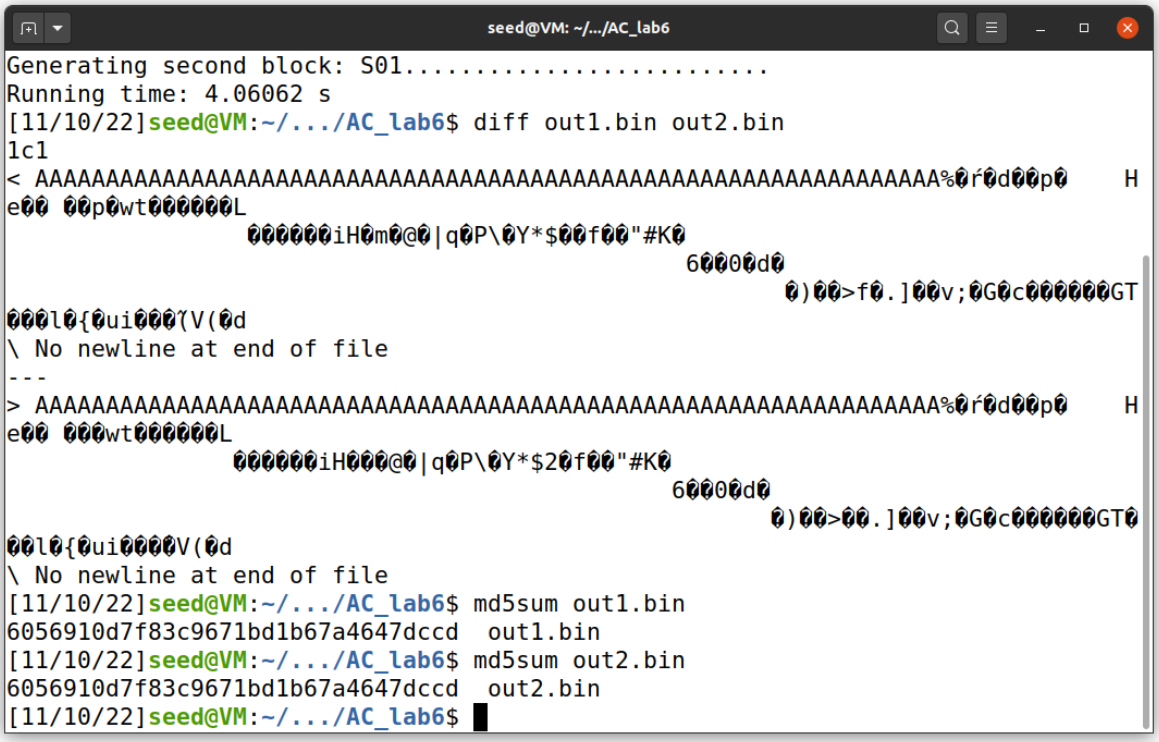
CLASS:F

SEC:F

SRN:PES2UG20CS390



```
seed@VM: ~/.../AC_lab6
[11/10/22]seed@VM:~/.../AC_lab6$ python3 -c "print('A'*64,end='')" > prefix.txt
[11/10/22]seed@VM:~/.../AC_lab6$ md5collgen -p prefix.txt -o out1.bin out2.bin
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'out1.bin' and 'out2.bin'
Using prefixfile: 'prefix.txt'
Using initial value: b217e7185a63fe5f643fe6a6d401bf59

Generating first block: ........................................
Generating second block: S00.........
Running time: 20.4062 s
[11/10/22]seed@VM:~/.../AC_lab6$
```



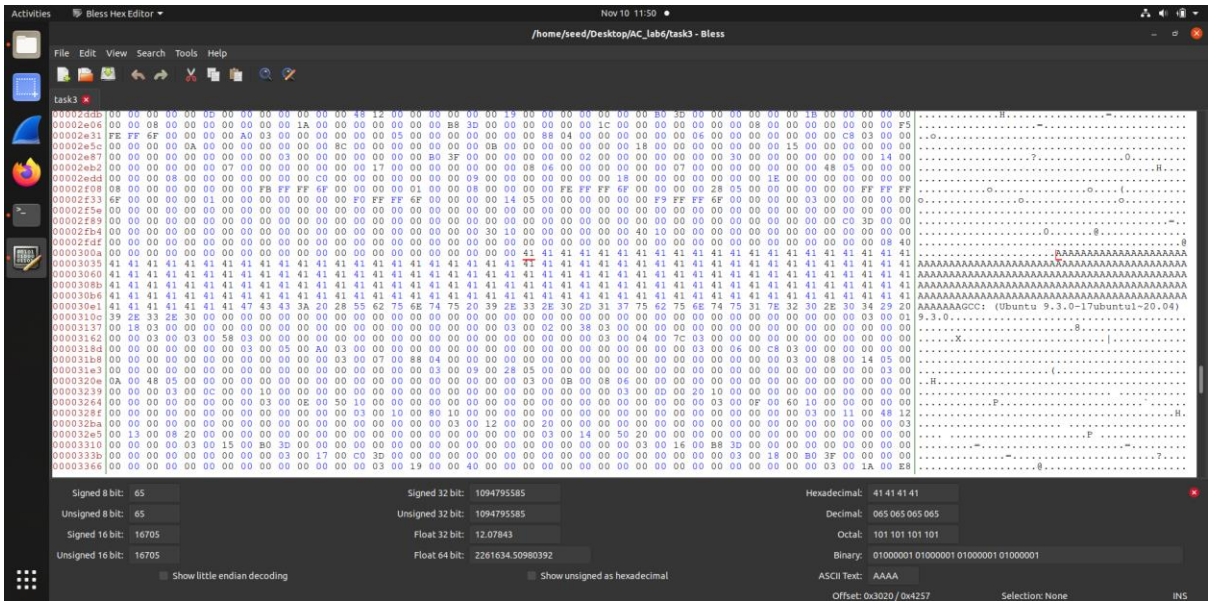
```
seed@VM: ~/.../AC_lab6
Generating second block: S01.........................
Running time: 4.06062 s
[11/10/22]seed@VM:~/.../AC_lab6$ diff out1.bin out2.bin
1c1
< AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA%́d́dṕ    H
é́ ́́ṕwt́́́́́́L
                ́́́́́́iH́ḿ́́|q́P\́Y*$́́f́́"#Ḱ
                                                6́́́́d́
                                                        ́)́́>f́.]́́v;́Ǵć́́́́́GT
́́́ĺ{́uí́́(V(́d
\ No newline at end of file
---
> AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA%́d́dṕ    H
é́ ́́́wt́́́́́́L
               ́́́́́́iH́́́́|q́P\́Y*$2́f́́"#Ḱ
                                               6́́́́d́
                                                       ́)́́>́́.]́́v;́Ǵć́́́́́GT́
́́ĺ{́uí́́́V(́d
\ No newline at end of file
[11/10/22]seed@VM:~/.../AC_lab6$ md5sum out1.bin
6056910d7f83c9671bd1b67a4647dccd  out1.bin
[11/10/22]seed@VM:~/.../AC_lab6$ md5sum out2.bin
6056910d7f83c9671bd1b67a4647dccd  out2.bin
[11/10/22]seed@VM:~/.../AC_lab6$
```

Task 2: Understanding MD5's Property

```
seed@VM: ~/.../AC_lab6
[11/10/22]seed@VM:~/.../AC_lab6$ tail -c 128 out1.bin > P
[11/10/22]seed@VM:~/.../AC_lab6$ tail -c 128 out2.bin > Q
[11/10/22]seed@VM:~/.../AC_lab6$ md5sum P
7af06f0f5aab95664cc81fe6e4c383a6  P
[11/10/22]seed@VM:~/.../AC_lab6$ md5sum Q
30483d20ae92c27401ded0d4ebb47c16  Q
[11/10/22]seed@VM:~/.../AC_lab6$
```

```
seed@VM: ~/.../AC_lab6
[11/10/22]seed@VM:~/.../AC_lab6$ python3 -c "print('114514'*10,end='')" > suffix
[11/10/22]seed@VM:~/.../AC_lab6$ cat out1.bin suffix > f1
[11/10/22]seed@VM:~/.../AC_lab6$ cat out2.bin suffix > f2
[11/10/22]seed@VM:~/.../AC_lab6$ md5sum f1
70b5df37160501e4e2d37260ac51b268  f1
[11/10/22]seed@VM:~/.../AC_lab6$ md5sum f2
70b5df37160501e4e2d37260ac51b268  f2
[11/10/22]seed@VM:~/.../AC_lab6$
```

Task 3: Generating Two Executable Files with the Same MD5 Hash



Step1:

```
seed@VM: ~/.../AC_lab6
seed@VM: ~/.../AC_lab6    seed@VM: ~/.../AC_lab6
[11/10/22]seed@VM:~/.../AC_lab6$ head -c <12352> task3 > prefi
x
bash: syntax error near unexpected token `12352'
[11/10/22]seed@VM:~/.../AC_lab6$ head -c 12352 task3 > prefix
[11/10/22]seed@VM:~/.../AC_lab6$ tail -c +12480 task3 > suffix
[11/10/22]seed@VM:~/.../AC_lab6$
```

Step2:

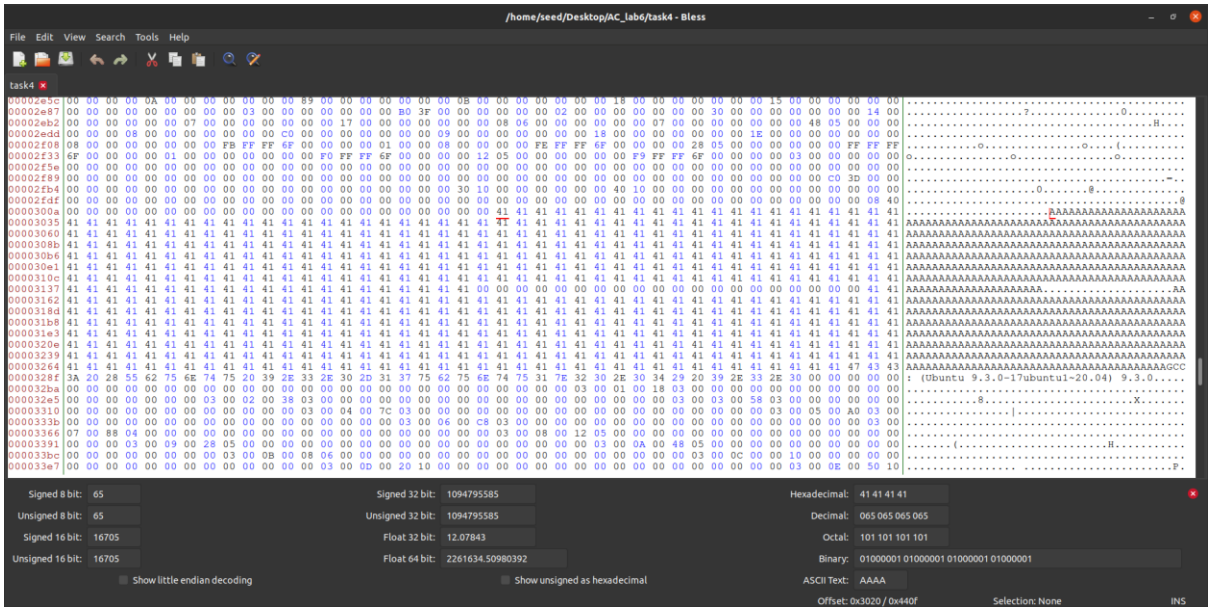
```
[11/10/22]seed@VM:~/.../AC_lab6$ md5collgen -p prefix -o P Q
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'P' and 'Q'
Using prefixfile: 'prefix'
Using initial value: aefe77439646539fe6db56554d46ae83

Generating first block: ....................
Generating second block: S11..................................
.........
Running time: 16.758 s
[11/10/22]seed@VM:~/.../AC_lab6$ cat P suffix > arr1.out
[11/10/22]seed@VM:~/.../AC_lab6$ cat Q suffix > arr2.out
[11/10/22]seed@VM:~/.../AC_lab6$ sudo chmod +x arr1.out arr2.o
ut
[11/10/22]seed@VM:~/.../AC_lab6$
```

Step3:

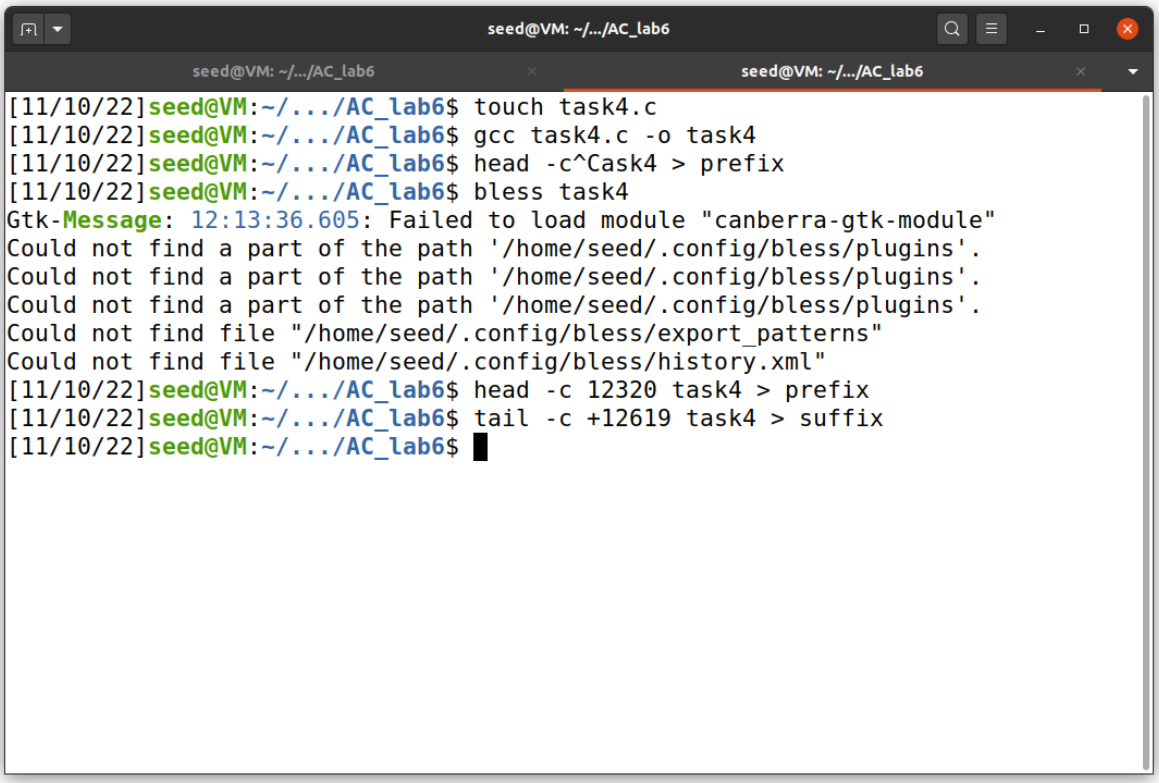
```
seed@VM: ~/.../AC_lab6
seed@VM: ~/.../AC_lab6    seed@VM: ~/.../AC_lab6
[11/10/22]seed@VM:~/.../AC_lab6$ ./arr1.out > f1
[11/10/22]seed@VM:~/.../AC_lab6$ ./arr2.out > f2
[11/10/22]seed@VM:~/.../AC_lab6$ md5sum arr1.out
9d5702377911d15cd906a06fa246b554  arr1.out
[11/10/22]seed@VM:~/.../AC_lab6$ md5sum arr2.out
9d5702377911d15cd906a06fa246b554  arr2.out
[11/10/22]seed@VM:~/.../AC_lab6$ diff f1 f2
1c1
< 41414141414141414141414141414141414141414141414141414141414141
41417ce6a55b4399635295504c354a3d61c5a0fb763ddf26cc312f3a84e24b
92c51deafa12e03ebfb6cc7da6b64ebcf743583d8c2ed779f34bb9424b5aa3
2e6b35f5736faf152244e102e87b1386e812a717fa04250f4f192e7ed79bdf
5b5cc541b13cbd6a826a39f97986751bbf56c4bfc5ad5ccbd96911cff422c3
a6da8a4d41414141414141414141414141414141414141414141414141414141
41414141414141414141414141
---
> 41414141414141414141414141414141414141414141414141414141414141
41417ce6a55b4399635295504c354a3d61c5a0fb76bddf26cc312f3a84e24b
92c51deafa12e03ebfb6cc7da6b64eb4f753583d8c2ed779f34bb9424b52a3
2e6b35f5736faf152244e102e87b1386e812a717fa042d0f4f192e7ed79bdf
5b5cc541b13cbd6a826a39f97986751bb756c4bfc5ad5ccbd96911cff422cb
a6da8a4d41414141414141414141414141414141414141414141414141414141
41414141414141414141414141
[11/10/22]seed@VM:~/.../AC_lab6$
```

Task 4: Making the Two Programs Behave Differently

Step1:


/home/seed/Desktop/AC_lab6/task4 - Bless
File Edit View Search Tools Help
task4
Signed 8 bit: 65
Unsigned 8 bit: 65
Signed 16 bit: 16705
Unsigned 16 bit: 16705
Signed 32 bit: 1094795585
Unsigned 32 bit: 1094795585
Float 32 bit: 12.07843
Float 64 bit: 2261634.50980392
Hexadecimal: 41 41 41 41
Decimal: 065 065 065 065
Octal: 101 101 101 101
Binary: 01000001 01000001 01000001 01000001
ASCII Text: AAAA
Show little endian decoding
Show unsigned as hexadecimal
Offset: 0x3020 / 0x440f
Selection: None
INS

Step2:


seed@VM: ~/.../AC_lab6
seed@VM: ~/.../AC_lab6
seed@VM: ~/.../AC_lab6
[11/10/22]seed@VM:~/.../AC_lab6$ touch task4.c
[11/10/22]seed@VM:~/.../AC_lab6$ gcc task4.c -o task4
[11/10/22]seed@VM:~/.../AC_lab6$ head -c^Cask4 > prefix
[11/10/22]seed@VM:~/.../AC_lab6$ bless task4
Gtk-Message: 12:13:36.605: Failed to load module "canberra-gtk-module"
Could not find a part of the path '/home/seed/.config/bless/plugins'.
Could not find a part of the path '/home/seed/.config/bless/plugins'.
Could not find a part of the path '/home/seed/.config/bless/plugins'.
Could not find file "/home/seed/.config/bless/export_patterns"
Could not find file "/home/seed/.config/bless/history.xml"
[11/10/22]seed@VM:~/.../AC_lab6$ head -c 12320 task4 > prefix
[11/10/22]seed@VM:~/.../AC_lab6$ tail -c +12619 task4 > suffix
[11/10/22]seed@VM:~/.../AC_lab6$

Step3:

```
[11/10/22]seed@VM:~/.../AC_lab6$ md5collgen -p prefix -o s1 s2
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 's1' and 's2'
Using prefixfile: 'prefix'
Using initial value: 65f42c5c575af28928ab39f2a1b35942

Generating first block: ..............................................
Generating second block: S10....................
Running time: 36.787 s
[11/10/22]seed@VM:~/.../AC_lab6$ tail -c 128 s1 > P
[11/10/22]seed@VM:~/.../AC_lab6$ tail -c 128 s2 > Q
[11/10/22]seed@VM:~/.../AC_lab6$ head -c 22 suffix > suffix_pre
[11/10/22]seed@VM:~/.../AC_lab6$  tail -c +321 suffix > suffix_post
[11/10/22]seed@VM:~/.../AC_lab6$
```

Step4:

```
[11/10/22]seed@VM:~/.../AC_lab6$ cat s1 suffix_pre P suffix_post > benign
[11/10/22]seed@VM:~/.../AC_lab6$ cat s2 suffix_pre P suffix_post > evil
[11/10/22]seed@VM:~/.../AC_lab6$ chmod u+x benign evil
[11/10/22]seed@VM:~/.../AC_lab6$ ./evil
i = 0, X[i] = 00, Y[i] = 75
Malicious
[11/10/22]seed@VM:~/.../AC_lab6$ ./task4
Benign
[11/10/22]seed@VM:~/.../AC_lab6$
```