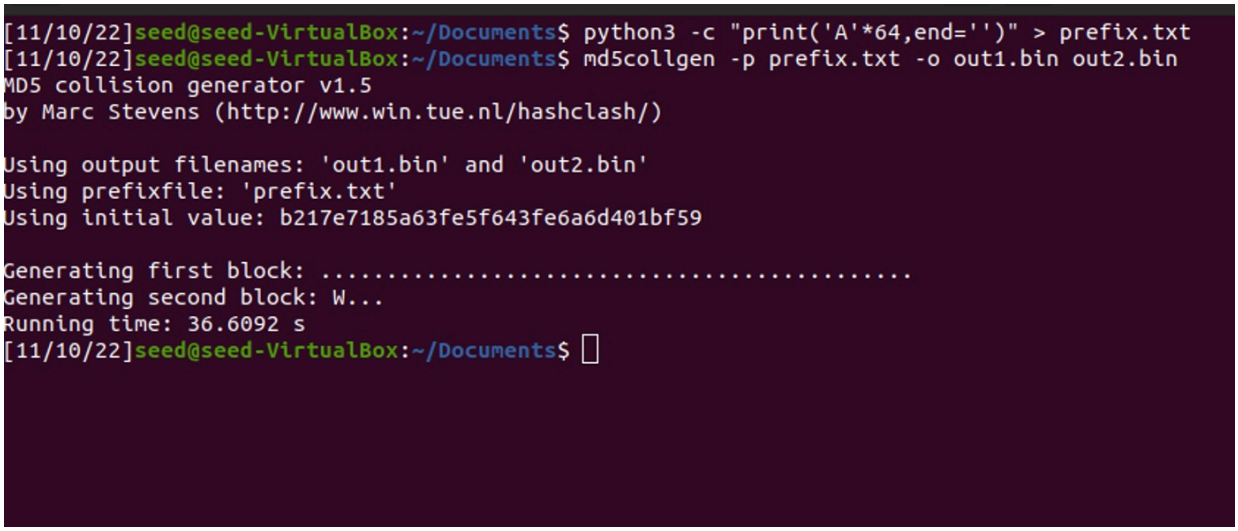
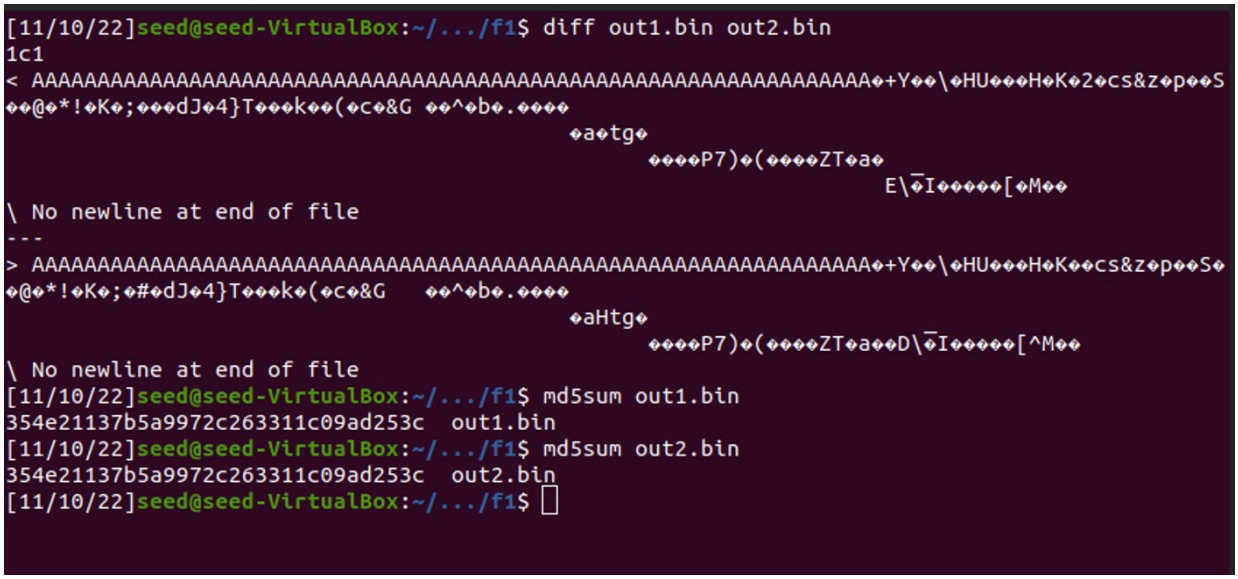
Applied Cryptography

Name	Naman Choudhary
SRN	PES2UG20CS209
Section	D

MD5

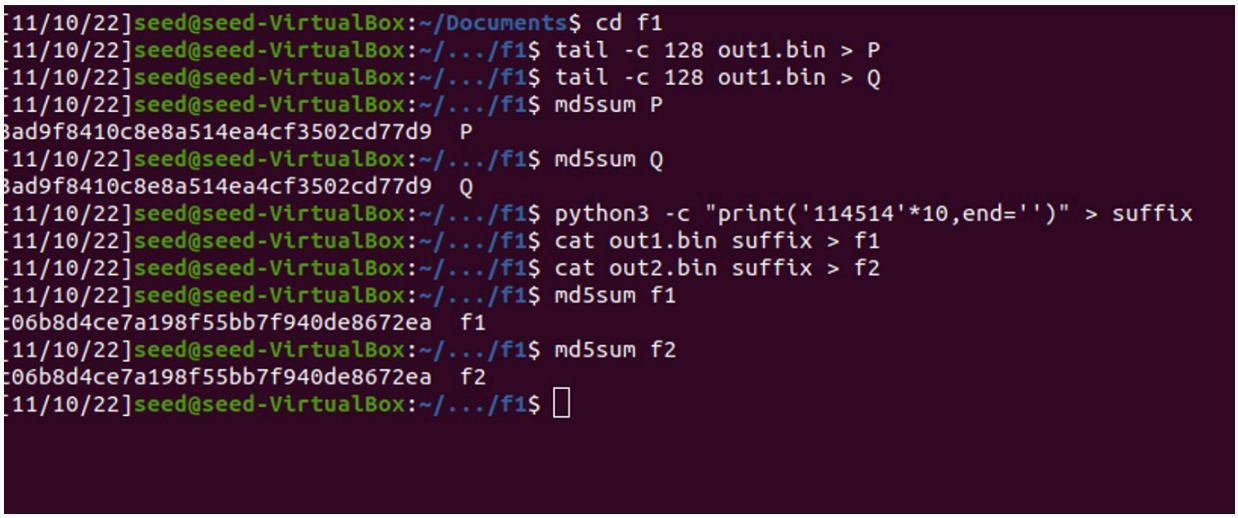
Task 1



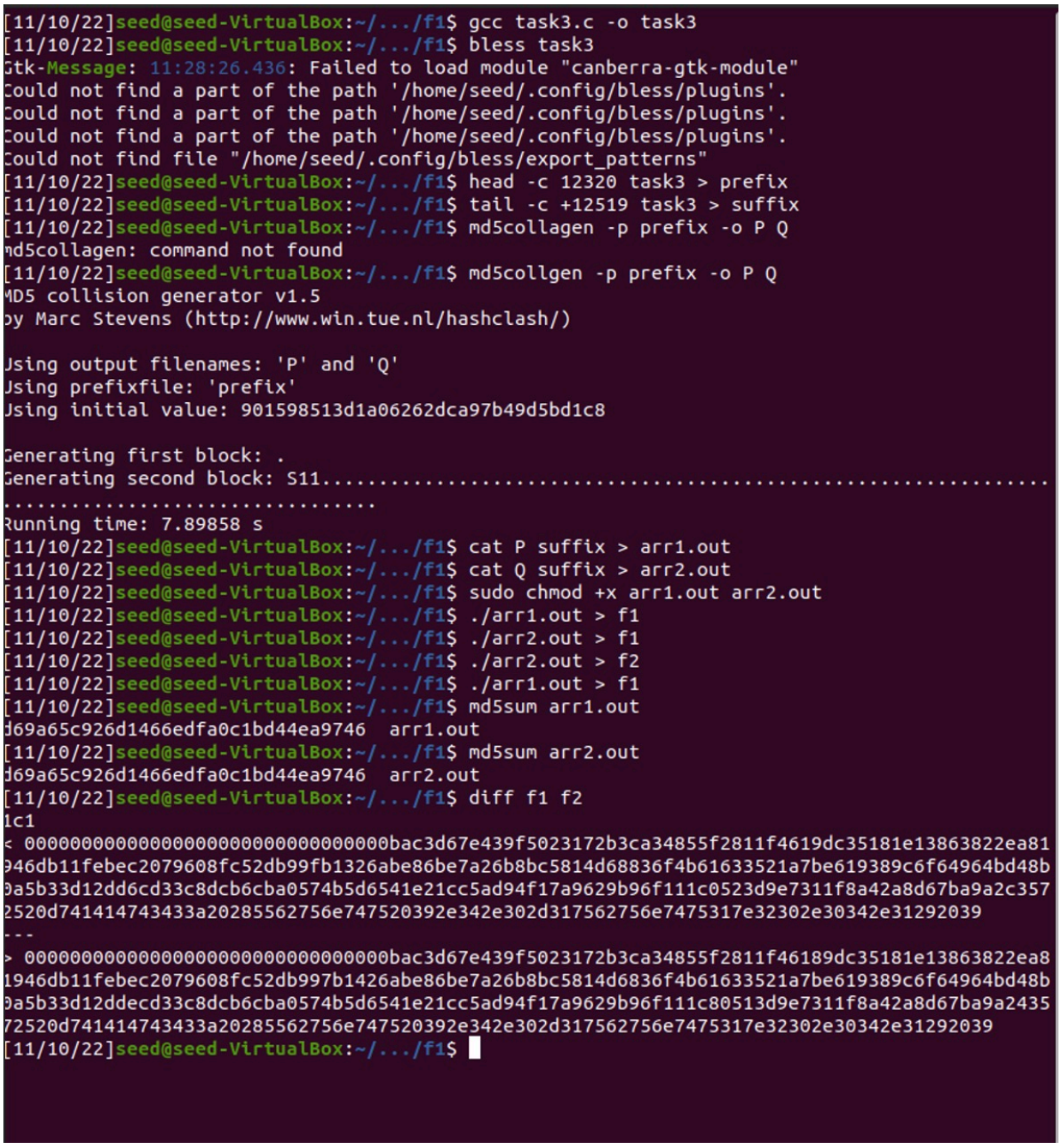


Observation: if the length of prefix is not multiple of 64, it will be padded with zeros

Task 2



Task 3


[11/10/22]seed@seed-VirtualBox:~/.../f1$ gcc task3.c -o task3
[11/10/22]seed@seed-VirtualBox:~/.../f1$ bless task3
Gtk-Message: 11:28:26.436: 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"
[11/10/22]seed@seed-VirtualBox:~/.../f1$ head -c 12320 task3 > prefix
[11/10/22]seed@seed-VirtualBox:~/.../f1$ tail -c +12519 task3 > suffix
[11/10/22]seed@seed-VirtualBox:~/.../f1$ md5collagen -p prefix -o P Q
md5collagen: command not found
[11/10/22]seed@seed-VirtualBox:~/.../f1$ 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: 901598513d1a06262dca97b49d5bd1c8
Generating first block: .
Generating second block: S11.....
.....
Running time: 7.89858 s
[11/10/22]seed@seed-VirtualBox:~/.../f1$ cat P suffix > arr1.out
[11/10/22]seed@seed-VirtualBox:~/.../f1$ cat Q suffix > arr2.out
[11/10/22]seed@seed-VirtualBox:~/.../f1$ sudo chmod +x arr1.out arr2.out
[11/10/22]seed@seed-VirtualBox:~/.../f1$ ./arr1.out > f1
[11/10/22]seed@seed-VirtualBox:~/.../f1$ ./arr2.out > f1
[11/10/22]seed@seed-VirtualBox:~/.../f1$ ./arr2.out > f2
[11/10/22]seed@seed-VirtualBox:~/.../f1$ ./arr1.out > f1
[11/10/22]seed@seed-VirtualBox:~/.../f1$ md5sum arr1.out
d69a65c926d1466edfa0c1bd44ea9746 arr1.out
[11/10/22]seed@seed-VirtualBox:~/.../f1$ md5sum arr2.out
d69a65c926d1466edfa0c1bd44ea9746 arr2.out
[11/10/22]seed@seed-VirtualBox:~/.../f1$ diff f1 f2
1c1
< 00000000000000000000000000000000bac3d67e439f5023172b3ca34855f2811f4619dc35181e13863822ea81
946db11febec2079608fc52db99fb1326abe86be7a26b8bc5814d68836f4b61633521a7be619389c6f64964bd48b
0a5b33d12dd6cd33c8dcb6cba0574b5d6541e21cc5ad94f17a9629b96f111c0523d9e7311f8a42a8d67ba9a2c357
2520d741414743433a20285562756e747520392e342e302d317562756e7475317e32302e30342e31292039

> 00000000000000000000000000000000bac3d67e439f5023172b3ca34855f2811f46189dc35181e13863822ea8
1946db11febec2079608fc52db997b1426abe86be7a26b8bc5814d6836f4b61633521a7be619389c6f64964bd48b
0a5b33d12ddecd33c8dcb6cba0574b5d6541e21cc5ad94f17a9629b96f111c80513d9e7311f8a42a8d67ba9a2435
72520d741414743433a20285562756e747520392e342e302d317562756e7475317e32302e30342e31292039
[11/10/22]seed@seed-VirtualBox:~/.../f1$

Task 4

```
[11/10/22]seed@seed-VirtualBox:~/.../f1$ gcc task4.c -o task4
[11/10/22]seed@seed-VirtualBox:~/.../f1$ bless task4
Gtk-Message: 11:38:05.981: 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"
^C
[11/10/22]seed@seed-VirtualBox:~/.../f1$ head -c 12320 task4 > prefix
[11/10/22]seed@seed-VirtualBox:~/.../f1$ tail -c +12619 task4 > suffix
[11/10/22]seed@seed-VirtualBox:~/.../f1$ 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: 28a2c115c9e2c479dffc847e9d68c6c3

Generating first block: ......................
Generating second block: W..............................................
Running time: 30.6543 s
[11/10/22]seed@seed-VirtualBox:~/.../f1$ tail -c 128 s1 > P
[11/10/22]seed@seed-VirtualBox:~/.../f1$ tail -c 128 s2 > Q
[11/10/22]seed@seed-VirtualBox:~/.../f1$ head -c 12640 suffix > suffix_ore
[11/10/22]seed@seed-VirtualBox:~/.../f1$ head -c 12640 suffix > suffix_pre
[11/10/22]seed@seed-VirtualBox:~/.../f1$ tail -c +12939 suffix > suffix_post
[11/10/22]seed@seed-VirtualBox:~/.../f1$ cat s1 suffix_pre P suffix_post > benign
[11/10/22]seed@seed-VirtualBox:~/.../f1$ cat s2 suffix_pre P suffix_post > evil
[11/10/22]seed@seed-VirtualBox:~/.../f1$ chmod u+x benign evil
[11/10/22]seed@seed-VirtualBox:~/.../f1$ ./benign
i = 0, X[i] = 00, Y[i] = 41
Malicious
[11/10/22]seed@seed-VirtualBox:~/.../f1$ ./evil
i = 0, X[i] = 00, Y[i] = 41
Malicious
[11/10/22]seed@seed-VirtualBox:~/.../f1$
```