

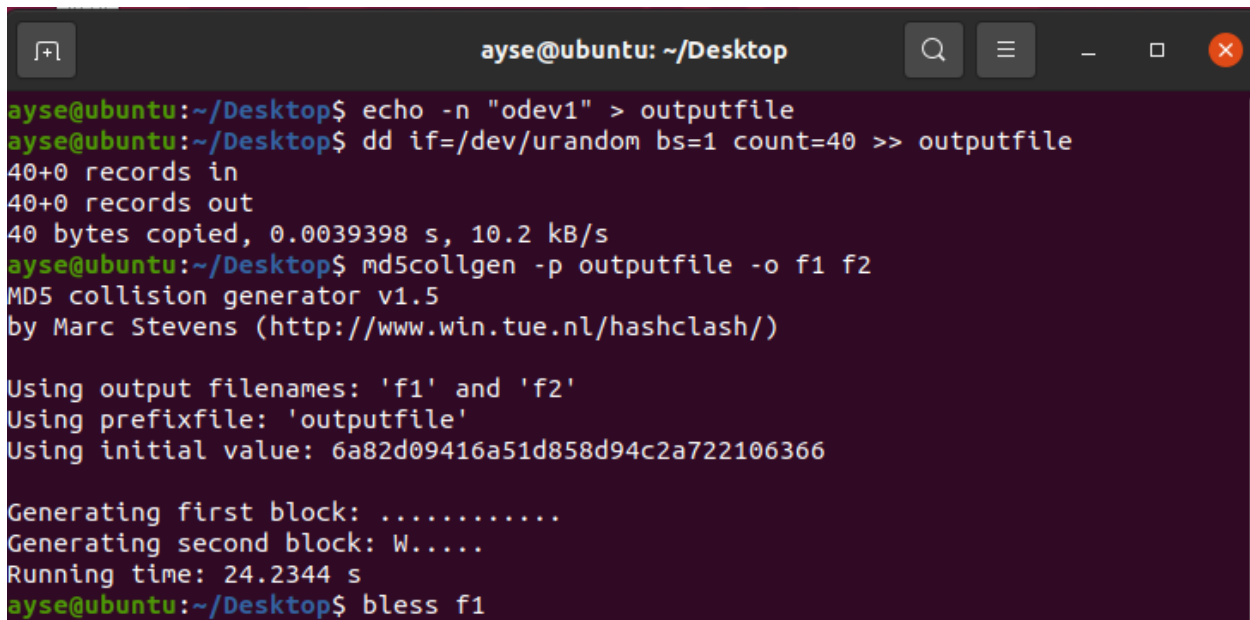
# MD5 Collision Attack Lab

Ayşe Sadioğlu 191101077

## Task 1: Generating Two Different Files with the Same MD5 Hash

**Question 1.** If the length of your prefix file is not multiple of 64, what is going to happen?

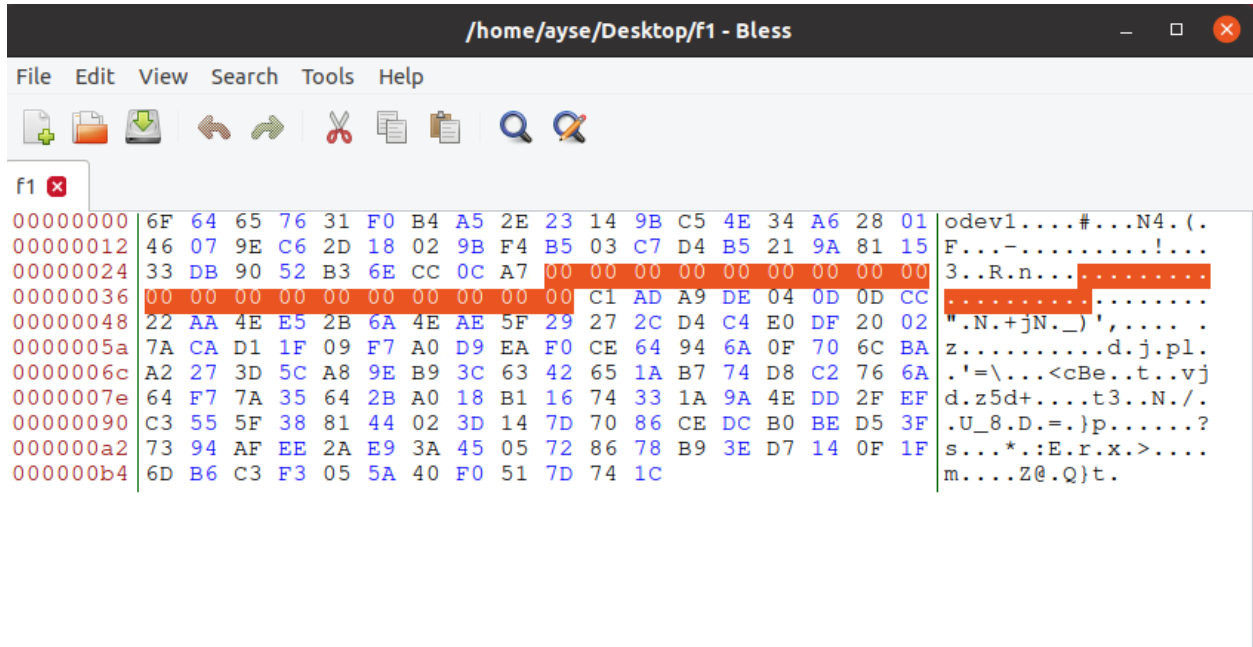
İlk olarak “odev1” ile başlayan ve zero paddingi görebilmemiz için random bir şekilde doldurulan bir prefix dosyası oluşturdum. Bu dosyanın boyutunu 45 olarak ayarladım. md5collgen kullandıktan sonra dosyaları bless yardımıyla görüntüledim ve boşlukların 0’lar ile doldurulduğunu gördüm. (zero padding)



```
ayse@ubuntu: ~/Desktop
ayse@ubuntu:~/Desktop$ echo -n "odev1" > outputfile
ayse@ubuntu:~/Desktop$ dd if=/dev/urandom bs=1 count=40 >> outputfile
40+0 records in
40+0 records out
40 bytes copied, 0.0039398 s, 10.2 kB/s
ayse@ubuntu:~/Desktop$ md5collgen -p outputfile -o f1 f2
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'f1' and 'f2'
Using prefixfile: 'outputfile'
Using initial value: 6a82d09416a51d858d94c2a722106366

Generating first block: .....
Generating second block: W....
Running time: 24.2344 s
ayse@ubuntu:~/Desktop$ bless f1
```



**Question 2.** Create a prefix file with exactly 64 bytes, and run the collision tool again, and see what happens.

Bu soru için 64 byte uzunluğunda olan ve `odev` ile başlayan bir dosya oluşturdum. Daha sonra bu prefix dosyası ve md5collgeni kullandım. Dosyayı görüntülediğimde zero padding olmadığını gördüm.

```
ayse@ubuntu: ~/Desktop
ayse@ubuntu: ~/Desktop
ayse@ubuntu:~/Desktop$ echo -n "odev" > outputfile
ayse@ubuntu:~/Desktop$ dd if=/dev/urandom bs=1 count=60 >> outputfile
60+0 records in
60+0 records out
60 bytes copied, 0.00206259 s, 29.1 kB/s
ayse@ubuntu:~/Desktop$ md5collgen -p outputfile -o f1 f2
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)

Using output filenames: 'f1' and 'f2'
Using prefixfile: 'outputfile'
Using initial value: 5cc2237cef2042d381f0886a14a05237

Generating first block: .....
Generating second block: W.....
Running time: 31.5401 s
```

```

/home/ayse/Desktop/f2 - Bless
File Edit View Search Tools Help
[Icons]

f2 x
00000000 6F 64 65 76 D9 E4 3C A2 D8 14 A0 C1 F6 EF B8 87 B5 1D B3 odev..<.....
00000013 3B C2 76 C4 38 7A 5C 06 76 61 F5 A5 15 D8 87 A8 04 82 36 ;.v.8z\..va.....6
00000026 90 CC 4D 35 62 88 34 68 61 37 E9 AC F5 56 D1 2F 2C EA 7F ..M5b.4ha7...V./,..
00000039 62 79 54 ED F1 27 0A F2 37 0B FC 15 6F 6E 2E CF 3E 0D E1 byT...'..7...on..>..
0000004c 80 18 2D D0 4C 28 1E 00 CB 61 F2 5A 3A F2 77 8D D4 27 A7 ..-.L(...a.Z:w...'
0000005f FA CF DD EE E8 38 25 04 A1 EB 07 BD FA 9B 31 9B 5A 6B 10 .....8%.....1.Zk.
00000072 F5 B7 C2 24 75 66 C2 F9 4E E6 5D 04 10 F1 2A 90 E6 CF 44 ...$uf..N.]...*...D
00000085 43 E5 76 51 D5 55 9A 6E 68 24 2E D2 91 06 C7 07 F2 26 4D C.vQ.U.nh$......&M
00000098 1E 99 2D 16 4D D7 FC AD A5 A7 36 59 E8 90 8B A7 BE 6E B9 ..-.M.....6Y.....n.
000000ab 89 86 EC 61 FF BB 54 AC DB 6E C0 33 85 83 1B 04 6B A8 19 ...a..T..n.3....k..
000000be 34 7C 4|

```

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

Şekillerden görüldüğü üzere tüm bytler farklı değil sadece birkaçı farklıdır.

Bunlar : 84, 110, 111,124, 148,174,175,188 numaralı bitler.

```

f1 x
00000000 6F 64 65 76 D9 E4 3C A2 D8 14 A0 C1 F6 EF B8 87 B5 1D odev..<.....
00000012 B3 3B C2 76 C4 38 7A 5C 06 76 61 F5 A5 15 D8 87 A8 04 ;.v.8z\..va.....6
00000024 82 36 90 CC 4D 35 62 88 34 68 61 37 E9 AC F5 56 D1 2F .6..M5b.4ha7...V./
00000036 2C EA 7F 62 79 54 ED F1 27 0A F2 37 0B FC 15 6F 6E 2E ,...byT...'..7...on.
00000048 CF 3E 0D E1 80 18 2D D0 4C 28 1E 80 CB 61 F2 5A 3A F2 .>....-.L(...a.Z:.
0000005a 77 8D D4 27 A7 FA CF DD EE E8 38 25 04 A1 EB 07 BD FA w...'.....8%.....
0000006c 9B B1 9A 5A 6B 10 F5 B7 C2 24 75 66 C2 F9 4E 66 5D 04 ...Zk....$uf..Nf].
0000007e 10 F1 2A 90 E6 CF 44 43 E5 76 51 D5 55 9A 6E 68 24 2E .*....DC.vQ.U.nh$.
00000090 D2 91 06 47 07 F2 26 4D 1E 99 2D 16 4D D7 FC AD A5 A7 ...G..&M.-.M.....
000000a2 36 59 E8 90 8B A7 BE 6E B9 89 86 6C 62 FF BB 54 AC DB 6Y.....n...lb..T..
000000b4 6E C0 33 85 83 1B 04 EB A8 19 34 7C n.3.....4|

```

**F1**

```

/home/ayse/Desktop/f2 - Bless
File Edit View Search Tools Help
[Icons]

f2 x
00000000 6F 64 65 76 D9 E4 3C A2 D8 14 A0 C1 F6 EF B8 87 B5 1D B3 odev..<.....
00000013 3B C2 76 C4 38 7A 5C 06 76 61 F5 A5 15 D8 87 A8 04 82 36 ;.v.8z\..va.....6
00000026 90 CC 4D 35 62 88 34 68 61 37 E9 AC F5 56 D1 2F 2C EA 7F ..M5b.4ha7...V./,..
00000039 62 79 54 ED F1 27 0A F2 37 0B FC 15 6F 6E 2E CF 3E 0D E1 byT...'..7...on..>..
0000004c 80 18 2D D0 4C 28 1E 00 CB 61 F2 5A 3A F2 77 8D D4 27 A7 ..-.L(...a.Z:w...'
0000005f FA CF DD EE E8 38 25 04 A1 EB 07 BD FA 9B 31 9B 5A 6B 10 .....8%.....1.Zk.
00000072 F5 B7 C2 24 75 66 C2 F9 4E E6 5D 04 10 F1 2A 90 E6 CF 44 ...$uf..N.]...*...D
00000085 43 E5 76 51 D5 55 9A 6E 68 24 2E D2 91 06 C7 07 F2 26 4D C.vQ.U.nh$......&M
00000098 1E 99 2D 16 4D D7 FC AD A5 A7 36 59 E8 90 8B A7 BE 6E B9 ..-.M.....6Y.....n.
000000ab 89 86 EC 61 FF BB 54 AC DB 6E C0 33 85 83 1B 04 6B A8 19 ...a..T..n.3....k..
000000be 34 7C 4|

```

**F2**

## 2.2 Task 2: Understanding MD5's Property

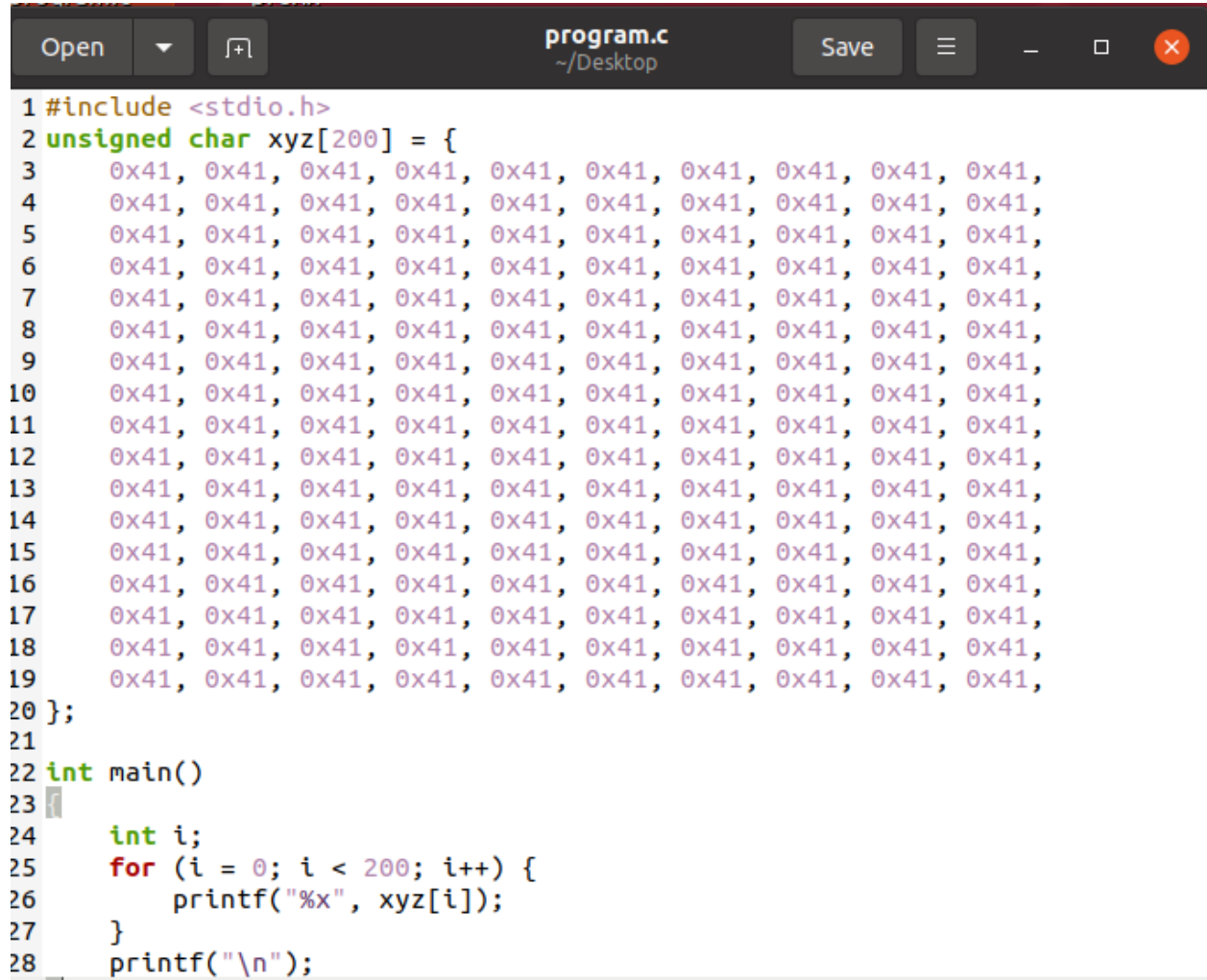
Bunu test etmek için prefix dosyası oluşturup md5collgen çalıştırdım ve ikisinin aynı hash değerini verdiğini gördüm. Ardından iki dosyanın sonuna da “odev1” stringini ekledim ve tekrardan md5collgen çalıştırdım. mdsum ile tekrardan kontrol ettiğim ikisinin tekrardan aynı hash değerini aldığını gözlemledim.

```
ayse@ubuntu:~/Desktop$ 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'
Error: cannot open inputfile: 'prefix.txt'
ayse@ubuntu:~/Desktop$ md5sum out1.bin out2.bin
d41d8cd98f00b204e9800998ecf8427e  out1.bin
d41d8cd98f00b204e9800998ecf8427e  out2.bin
ayse@ubuntu:~/Desktop$ echo odev1 >> out1.bin
ayse@ubuntu:~/Desktop$ echo odev1 >> out2.bin
ayse@ubuntu:~/Desktop$ md5sum out1.bin out2.bin
e5bc057d34915a88abd6736391592534  out1.bin
e5bc057d34915a88abd6736391592534  out2.bin
```

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

İlk olarak açıklamada belirtildiği gibi bir C programı yazdım ve bu programı çalıştırarak çıktısına baktım.



```
1 #include <stdio.h>
2 unsigned char xyz[200] = {
3     0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
4     0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
5     0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
6     0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
7     0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
8     0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
9     0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
10    0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
11    0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
12    0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
13    0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
14    0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
15    0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
16    0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
17    0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
18    0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
19    0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,
20 };
21
22 int main()
23 {
24     int i;
25     for (i = 0; i < 200; i++) {
26         printf("%x", xyz[i]);
27     }
28     printf("\n");
```

xxd ve grep yardımıyla dosya içerisindeki 'A' karakterlerinin başladığı yerin indexini 0x3020=12320 olarak buldum. Prefix uzunluğu 64'ün katı olması gerektiği için 12320'ye yakın 64'ün katını buldum ve buraya kadar prefixi head komutu ile aldım. wc komutu ile prefix uzunluğunun doğru olup olmadığını kontrol ettim. Ardından bu prefix yardımıyla md5collgen çalıştırdım. `dd if=out1.bin of=program_1 bs=12480 count=1 conv=notrunc`

Bu satırda out1.bin dosyasından verileri okuyarak, her biri 12480 byte uzunluğunda olan bir dosya oluşturduk ve bunu program\_1 olarak adlandırdım. Daha sonra aynı işlemi out2.bin dosyası için de yaptım. Sonrasında md5sum ile bu iki dosyanın aynı hash değerlerine sahip olduğunu ancak bu

[illegible]