CS4236 Assignment 1
Padding Oracle Attack

Syed Abdullah

September 14, 2017

1 General

1.1 Requirements

- Python 3.6.0
- pycrypto 2.6.1 (in `requirements.txt`)

1.2 Structure

`main.py` contains code used for the Padding Oracle attack, while `routines.py` contains methods related to AES & PKCS#7 scheme (e.g. the padding oracle)

`AES_Padding`, `AES_Valid_Padding` is located in `routines.py`.

1.3 Usage

This program utilises a command-line interface. The input to this system is supplied via standard input (*stdin*). To run the program, you would simply run `main.py`, like so:

```
> cat file1.in | python main.py
```

The above example will use file1.in contents as the plaintext to start from.

2 Test Instances

All test inputs are available in the `testcases` folder.

2.1 Manual Testing

Input:

```
#> python main.py
?> 12345abcdef
?> [CTRL+D/CTRL+Z]
```

Output:

```
F0 BC 4F 23 FF 0C B2 FA D2 E1 30 DF 69 14 5D C5
12345abcdef
```

2.2 `test1.in` – all possible printable characters

This test cases determines if our implementation can handle the printable characters in ASCII. Non-printable characters are excluded from testing, as their presence may affect the console/terminal.

Input:

```
> cat test1.in | python main.py
```

Output:

```
B6 5E 5A 9A D3 55 8B 8F F2 48 3D D2 BD 4E 07 C1 FB CB A3 D6 9A 5F EA 3A C3 65 B2 BB BD E4 0F
10 37 85 AA 81 BB 93 A5 5F 83 08 E0 4A D0 76 E3 75 EB B3 C3 4A 98 FA 5B 13 6D A4 4D 3C 6C 46
F6 45 98 13 44 FD E1 E7 62 2C C7 C3 41 62 13 65 45 CC BF C8 D2 61 14 70 0B 8E 90 0B F6 14 36
6C A0 A6 CE 06 D9 21 E7 C2 71 27 5E 12 58 D4 D2 C2 4E 37
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[
]^_`abcdefghijklmnopqrstuvwxyz|
```

2.3 `test2.in` – plaintext a multiple of blocksize

Input:

```
> cat test2.in | python main.py
```

Output:

```
4B F2 20 E9 AF E8 F4 7F B5 08 16 E1 16 2E 0D 76 1C 74 12 3B D1 1F DC C7 9D 70 63 5C 4C F5 7B
B1
sixteenbytes123
```

2.4 `test3.in` – plaintext has one byte in last block

Input:

```
> cat test3.in | python main.py
```

Output:

```
BE 42 2A 9D 8A 19 98 3D D5 A4 BC 26 F7 D1 78 2B FE 33 DC D5 F3 72 48 64 21 C5 9F 30 D4 AF 05
46
sixteenbytes1234
```

2.5 `test4.in` – plaintext exactly 300 bytes long

Input:

```
> cat test4.in | python main.py
```

Output:

```
1B D4 11 2E DB 2F A2 DA A7 30 30 ED CC 33 96 F8 EA E7 75 A6 13 4E 9D 5D 18 A4 89 E1 01 1E EA
68 4D 5B 83 40 67 19 A5 7B AB FD 8F F0 CF 32 7F B0 CC 5D 18 A4 32 52 69 3B 7A 4B A6 CB 9F A0
92 CB 89 77 18 1A EE 0C 28 74 FB 9D 70 3D 00 BB 57 5A 2F 96 1C 90 FF E8 CC 12 EF 5E F1 14 D6
25 B7 1D BD D2 94 4E 1F F2 68 DD 81 62 88 44 0D 2C 80 0D 89 6C 72 6A FD 71 1C CF C2 4F 5E 05
CE 98 21 C8 8E 30 1A DA D9 7C 08 68 C7 4D 1F E2 F3 F3 8B B4 D3 B7 E9 E9 7A 25 83 22 5F AE 06
5A A8 31 B1 61 D8 45 8E B9 86 42 3B 3D 05 2A DB 89 25 2F 2F 30 B9 5A 83 8D 30 A5 FE 45 5B 44
2F A4 16 E6 FB 2C 99 60 E9 77 AB 57 EA 99 CA 31 0E 42 FA 31 0E F8 45 13 2B D6 FC B7 4D F2 04
57 D6 53 5C FF 32 96 EC 9E 30 D0 76 3F 1A BA F0 C1 22 E7 B5 2C F8 CD F8 54 C9 1D 13 C0 0D 7E
B2 CC B6 1C 1B B9 8D 4B C2 05 4A 4E FF A1 56 01 DD 89 AF 84 63 1D A1 C9 D5 9F D6 CB C6 0E 5F
CD F8 E2 D5 97 19 4D 6E 43 C4 CF 0F B7 D8 91 9A C0 76 A2 98 48 C8 3C 03 F2
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivamus condimentum suscipit
mauris et iaculis. Phasellus molestie sagittis dui vitae vestibulum. Cras vestibulum
convallis sapien, id rhoncus nunc tristique et. Quisque condimentum vel felis sit amet
placerat. Duis vel justo id orci volutpat.
```

2.6 `test5.in` – single character per line

Input:

```
> cat test5.in | python main.py
```

Output:

```
00 0F 7C A9 B3 E3 E5 2B D6 7F B7 D6 62 9D E5 14 D0 4D 49 6B 17 00 AC FE B0 63 7F 71 75 D7 F8
C4
h
e
a
d
t
a
i
l
```

2.7 `test6.in` – 300 lines of text

Input:

```
> cat test6.in | python main.py
```

Output:

```
66 08 6F 69 07 CC AA D3 FB 4E 53 3A AD E1 7E 5C 75 2B 9A E7 C9 CB 1A 72 4C DA E1 08 CF 61 C2
62 67 02 8F 44 31 FF 4E 87 8B 93 21 D9 35 4C 24 D8 B2 91 4A 69 41 73 1B 9A 51 BF 1E DC 25 BB
83 47 12 2A AF 37 29 B5 F1 49 D3 04 6C E7 3A CE B2 5D CA 3F D5 20 82 F1 C7 B2 83 F8 12 56 21
C2 51 B8 51 AA 78 1B 4A 88 60 3F DA 72 29 9E 2B D2 10 CB 54 7D 93 72 D8 DC 0D F9 CD F1 05 8C
E2 A4 19 00 68 B6 19 0A 21 C2 34 B6 C8 41 A0 50 BA 8A 5F AD 0E 26 0D EF 8C 69 6A 2E 39 AD 19
21 D5 34 30 17 63 C4 25 A9 1B ED 2A 92 88 ED 39 A2 C9 44 DC 87 C0 84 DE 73 3B 82 09 AE C8 13
08 05 E3 A8 22 63 BB 88 C3 15 D3 A4 8A 9B E3 7F 72 42 0B EF 11 15 3F 51 85 B7 C2 D0 91 F8 1D
50 B4 A9 31 E4 63 B0 ED 6B D5 C2 4C F8 FF D2 2B 61 12 A2 AF ED F3 08 B6 26 77 67 8A 41 17 1A
43 92 56 FA 46 D9 05 8B F8 15 86 46 D2 8F A4 DA 74 DA 85 7B DA DB F2 32 77 4D 9C 37 B7 23 1A
63 69 9F 99 85 68 C9 1B 8F 7B 13 AF 0D D0 59 B5 9C 4C 3A 5B D3 40 22 21 3B 72 0E B3 01 87 44
50 6D 45 55 F4 6E 54 5A 2E F2 13 EB F1 87 45 CE E7 CE DA 66 42 D4 7A B2 60 85
```

(N.B. Omitted output due to length of output)