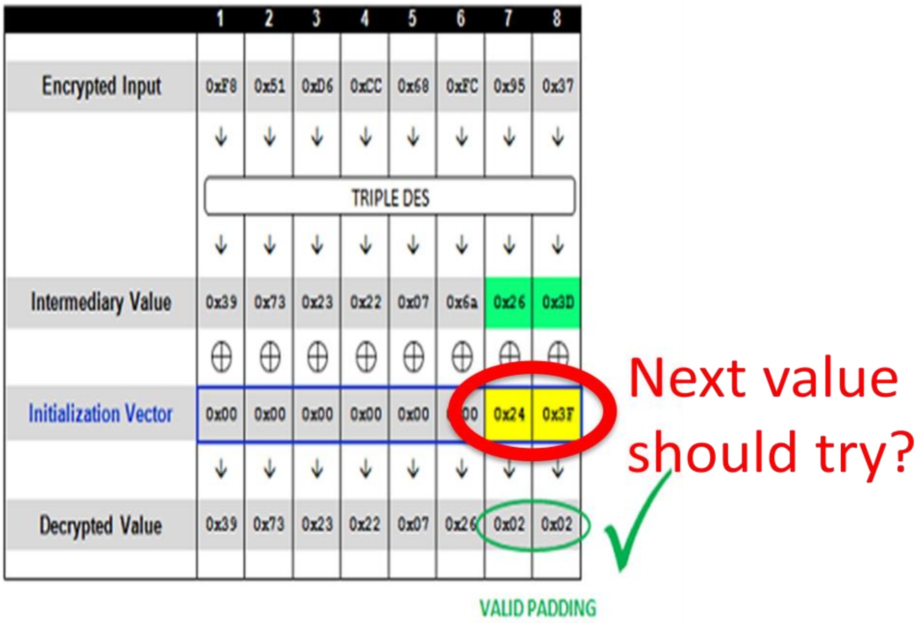
COMP444: Internet Infrastructure Security
Workshop 1: Padding Oracle Attack

Due at 11:55pm on 26 February 2015
Submission site: https://submit.comp.polyu.edu.hk/

1. **Explain in your own words why the padding oracle attack can compromise CBC even though the secret key is not compromised** (5 marks)**.**

2. **After obtaining this status, what is the next value of Initialization Vector we should try?**
   – Support your answer with explanation. (5 marks)



	1	2	3	4	5	6	7	8
Encrypted Input	0xF8	0x51	0xD6	0xCC	0x68	0xFC	0x95	0x37
Intermediary Value	0x39	0x73	0x23	0x22	0x07	0x6a	0x26	0x3D
Initialization Vector	0x00	0x00	0x00	0x00	0x00	00	0x24	0x3F
Decrypted Value	0x39	0x73	0x23	0x22	0x07	0x26	0x02	0x02

3. Decrypt the ciphertext. (5 marks)

- Choose either the first one or the second one. No need to answer both.

3.1 The first choice: decrypt_me.php [Prepared by Zetta KE (ozetta@vxrl.org) and Anthony LAI (darkfloyd@vxrl.org) from VXRL.]

Decrypt the ciphertext! (Don't copy other's work, the texts are random)

Hint: Block Size = 8, Encoding = Lower HEX

3.2 The second choice: crypto-class.appspot.com

See https://class.coursera.org/crypto-preview/quiz/attempt?quiz_id=123 and slides.

No additional hints, just think and try.

Pad Buster Command:

Plaintext:

4. **Draw the cipher block graphs (10 marks)**
   - We are given web server logs that appear to show an attacker exploiting a vulnerability.
     - https://raw.github.com/SaveTheRbtz/crypto-class/master/ex4/proj4-log.txt
   - Read this blog post and analyze how he captures the secret.
     - http://hackeroutfit.wordpress.com/2012/07/06/oracle-padding-attack-challenge/
   - **Your task:** Draw two complete cipher block graphs to explain his procedure.
     - One to obtain all Intermediary Values (HEX)
     - One to obtain the stolen secret (plaintext)