

# تکلیف عملی اول

رسول صالحی  
۴۰۱۲۵۹۳۳

مجتبی ملائی  
۴۰۱۳۱۳۸۳

## ۱ سوال سوم

(آ) بررسی A: ابتدا به آن ورودی aaaa را دادیم.

```
1 ./A aaaa
2 Encrypted (hex): 61 4b 61 4b
```

سپس ورودی baaa را امتحان کردیم.

```
1 ./A baaa
2 Encrypted (hex): 62 48 62 48
```

و نهایتاً ورودی aaab را امتحان کردیم.

```
1 ./A aaab
2 Encrypted (hex): 61 4b 61 48
```

این موضوع نشان می‌دهد که بلاک اول تاثیر مستقیمی بر روی بلاک های بعدی دارد. پس ECB نیست. همچنین تغییر بلاک آخر ورودی فقط باعث تغییر در بلاک آخر رمز شده است. از یکسان بودی خروجی وقتی ورودی یکسان باشد نیز متوجه می‌شویم که چه CTR یا CBC باشد، IV ثابت است. اگر CTR باشد، چون IV ثابت است، اگر  $P_0$  را تغییر دهیم، فقط  $C_0$  باید تغییر کند اما همه بلاک های بعد از آن نیز تغییر کرده اند. پس فقط میتواند CBC باشد. زیرا در CBC تغییر هر بلاک باعث تغییر در بلاک های بعدی می‌شود. اما در دیگر مود ها اینگونه نیست.

**طول بلاک:** همانطور که دیدیم، با تغییر آخرین حرف ورودی، ۸ بیت آخر خروجی فقط تغییر کرد. پس طول هر بلاک ۸ بیت است.

(ب) بررسی B: ابتدا به آن ورودی aaaa را دادیم.

```
1 ./B aaaa
2 Encrypted (hex): e5 e4 e7 e6
```

سپس دوباره همان ورودی را امتحان کردیم.

```
1 ./B aaaa
2 Encrypted (hex): ca cb c8 c9
```

و نهایتاً ورودی aaab را امتحان کردیم.

```
1 ./B aaab
2 Encrypted (hex): 62 63 60 62
```

این موضوع نشان می‌دهد. حتی با ورودی ثابت هم خروجی کاملاً متفاوت است. پس ECB نیست. در نتیجه فقط می‌تواند CTR باشد. چون هر بار IV متفاوت است، خروجی نیز کاملاً متفاوت می‌باشد.

**طول بلاک:** از آنجایی که طول متن رمز با طول ورودی همواره یکسان است، پس طول هر بلاک آن به اندازه یک حرف یا ۸ بیت است.

(ج) بررسی C:

ابتدای آن ورودی aaaa را دادیم.

```
1 ./C aaaa
2 Encrypted (hex): 31 31 31 31
```

سپس ورودی baaa را امتحان کردیم.

---

```
1 ./C baaa
2 Encrypted (hex): 32 31 31 31
```

و نهایتاً ورودی aaab را امتحان کردیم.

```
1 ./C aaab
2 Encrypted (hex): 31 31 31 32
3
```

واضح است که اگر هر بلاک ورودی را تغییر دهیم، همان بلاک در خروجی تغییر می‌کند. همچنین خروجی آن همیشه به ازای ورودی یکسان ثابت است یعنی به IV ربطی ندارد. پس فقط میتواند ECB باشد.

**طول بلاک:** از آنجایی که طول متن رمز با طول ورودی همواره یکسان است، پس طول هر بلاک آن به اندازه یک حرف یا ۸ بیت است.