تاریخ: **۱۴۰۱/۰۸/۲۰** **تمرین سری اول**

دانشکده مهندسی برق و کامپیوتر **مبانی امنیت**

جواب تمرینات را تا ۱۴۰۱/۰۹/۱۱ به sa.mortezavi+FIS14011@gmail.com ایمیل کنید.

تنها یک فایل پیوست به شکل hw1 + name + ID ضمیمه شود. تمرینات را خودتان حل کنید و در صورت تشابه دو تکلیف به یکدیگر به هیچکدام نمره‌ای تعلق نخواهد گرفت.

۱- در مورد مدهای کاری ECB, CBC, OFB توضیح دهید که آیا می‌توان عملیات رمزگذاری و رمزگشایی را به صورت موازی انجام داد یا نه.

۲- در مورد کلیدهای ضعیف DES تحقیق کنید و آنها را توضیح دهید.

۳- حمله‌ای برای الگوریتم رمزگذاری $\text{DES}_{k_1}\left(\text{DES}_{k_2}(m)\right)$ که سریعتر از جستجوی جامع باشد را مطرح کنید.

۴- چرا رمز جریانی LFSR برای رمزگذاری مناسب نیست.

۵- در مورد پدینگ PKCS#7 تحقیق و توضیح دهید.

۶- فرض کنید که کاربری از **سروری** پیام رمز شده $C = \text{Enc}_k(m)$ را دریافت می‌کند. مهاجمی در میان راه این پیام را شنود می‌کند و می‌خواهد که به محتوای پیام دسترسی داشته باشد. مهاجم می‌داند که الگوریتم رمزگذاری استفاده شده در **سرور** از الگوریتم رمزگذاری قالبی AES در مد کاری CBC به همراه پدینگ PKCS#7 است.

```
cipher = AES.new(KEY, AES.MODE_CBC)
encrypted = cipher.encrypt(pkcs7padding(plaintext))
```

این سرور همچنین پیام‌های رمزشده کاربران را دریافت و رمزگشایی می‌کند و در زمان رمزگشایی سرور ابتدا پیام را رمزگشایی و سپس unpad می‌کند تا به متن اصلی برسد و اگر الگوی پدینگ مناسب نباشد خطای ''error in padding'' را به کاربر برمی‌گرداند و در غیر این صورت سرور هیچ پیام خطایی را بر نمی‌گرداند.

توضیح دهید که مهاجم چگونه می‌تواند با استفاده از اطلاعات این **خطا** به محتوای پیام رمزشده اصلی دسترسی داشته باشد. برای سادگی فرض کنید که پیام رمزشده ارسالی تنها از سه قالب $C = IV, c_1, c_2$ تشکیل شده است (padding-oracle attack).

۷- به صورت مختصر حمله شامیر به رمز جریانی RC4 را توضیح دهید.

1) Fluhrer, Scott, Itsik Mantin, and Adi Shamir. "Weaknesses in the key scheduling algorithm of RC4." In International Workshop on Selected Areas in Cryptography, pp. 1-24. Springer, Berlin, Heidelberg, 2001.