دانشکده مهندسی کامپیوتر

درس امنیت سیستم های کامپیوتری
تمرین حمله به DES

ملیکا محمدی فخار - ستاره باباجانی

۹۹۵۲۱۱۰۹-۹۹۵۲۲۰۸۶

استاد درس: دکتر ابوالفضل دیانت

بهار ۱۴۰۳

سوال اول: حمله تفاضلی به DES

یکی از مهم‌ترین حملات به DES، حمله تفاضلی است که توسط Biham Eli و Shamir Adi در دهه ۱۹۹۰ مطرح شد. در مورد این حمله تحقیق کنید و نحوه این حمله را با یک مثال ساده شده DES بیان کنید. مثلا با DES سه دور یا شش دور.

پاسخ: حمله تفاضلی به DES

حمله تفاضلی یک تکنیک رمزنگاری است که به تحلیل تغییرات در ورودی و خروجی یک الگوریتم رمزنگاری پرداخته و از تفاوت‌های مشاهده شده برای کشف کلید مخفی استفاده می‌کند. در DES این حمله با استفاده از تفاوت‌های ورودی و خروجی در چندین دور از الگوریتم، سعی در یافتن کلید دارد.

به عنوان مثال، فرض کنید دو متن ساده P و P' که در یک بیت تفاوت دارند (یعنی $\Delta P = P \oplus P'$) به الگوریتم DES داده می‌شوند و متن‌های رمز شده C و C' تولید می‌شوند. تفاوت متن رمز شده $\Delta C = C \oplus C'$ است.

حمله کننده با تحلیل تفاوت‌های ورودی و خروجی در چندین دور DES و استفاده از جدول‌های تفاوتی برای هاS-box می‌تواند بخشی از کلید مخفی را پیدا کند.

در یک DES سه دور، فرض کنید تفاوت ورودی ΔP را می‌دانیم. با تحلیل تفاوت‌ها در خروجی هر S-box و استفاده از خواص آن‌ها، می‌توانیم تفاوت در خروجی هر دور را محاسبه کنیم و از این اطلاعات برای حدس زدن کلید استفاده کنیم.

سوال دوم: الگوریتم AES

نکات کلیدی

- **الگوریتم کلید متقارن:** AES از یک کلید برای هر دو فرآیند رمزگذاری و رمزگشایی استفاده می‌کند. این به این معنی است که هم فرستنده و هم گیرنده باید به همان کلید دسترسی داشته باشند.
- **رمز بلاکی:** AES داده‌ها را در بلاک‌های با اندازه ثابت رمزگذاری می‌کند. اندازه استاندارد بلاک ۱۲۸ بیت است، اما می‌تواند بلاک‌هایی با اندازه ۱۹۲ و ۲۵۶ بیت را نیز پردازش کند.

مراحل الگوریتم AES

گسترش کلید

کلید اولیه داده شده به چندین کلید دوری با استفاده از برنامه کلید AES گسترش می‌یابد. تعداد دورها بستگی به طول کلید دارد:

- ۱۰ دور برای کلیدهای ۱۲۸ بیتی
- ۱۲ دور برای کلیدهای ۱۹۲ بیتی

- ۱۴ دور برای کلیدهای ۲۵۶ بیتی

دور اولیه

- **AddRoundKey**: هر بایت از بلاک با یک بایت از کلید دوری با استفاده از عملیات XOR ترکیب می‌شود.

دورهای اصلی

(۹، ۱۱، یا ۱۳ بار بسته به اندازه کلید تکرار می‌شود):

- **SubBytes**: هر بایت از بلاک با بایت معادل در یک جدول جایگزینی ثابت (S-box) جایگزین می‌شود.
- **ShiftRows**: ردیف‌های بلاک به صورت چرخشی جابجا می‌شوند. هر ردیف به میزان متفاوتی جابجا می‌شود.
- **MixColumns**: ستون‌های بلاک با ضرب در یک چندجمله‌ای ثابت در میدان گالوا مخلوط می‌شوند.
- **AddRoundKey**: بلاک جاری با کلید دوری با استفاده از XOR ترکیب می‌شود.

دور نهایی

(همانند دورهای اصلی اما بدون مرحله :(MixColumns

- SubBytes
- ShiftRows
- AddRoundKey

رمزگشایی

فرآیند رمزگشایی معکوس رمزگذاری است. شامل همان مراحل است اما به ترتیب معکوس و با عملیات معکوس:

- SubBytes Inverse
- ShiftRows Inverse
- MixColumns Inverse
- AddRoundKey

کد

تحلیل کد

این کد پایتون از کتابخانه `PyCryptodome` برای رمزنگاری و رمزگشایی متن با استفاده از الگوریتم AES در حالت CBC استفاده می‌کند. کد شامل مراحل زیر است:

- وارد کردن کتابخانه‌ها
- تولید کلید و داده ورودی
- رمزنگاری
- چاپ داده‌های رمزنگاری شده
- رمزگشایی
- نتایج

```python
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad, unpad
from Crypto.Random import get_random_bytes

# تولید کلید و داده ورودی
key = get_random_bytes(16)  # کلید 16 بایتی
data = 'It is a test message'.encode('utf-8')

# رمزنگاری
cipher = AES.new(key, AES.MODE_CBC)
ciphertext = cipher.encrypt(pad(data, AES.block_size))
iv = cipher.iv

# چاپ داده های رمزنگاری شده
print("key:", key.hex())
print("IV:", iv.hex())
print("cipher text:", ciphertext.hex())

# رمزگشایی
decipher = AES.new(key, AES.MODE_CBC, iv)
plaintext = unpad(decipher.decrypt(ciphertext), AES.block_size)

# چاپ داده های رمزگشایی شده
print("plain text:", plaintext.decode('utf-8'))
```

شکل ۱: کد زده شده

```
key: 694e41a4a5b2a673f63f3e50b463e0cb
IV: 500888fee6c6fa5bfd69736d137fa2e1
cipher text: 73134e593bb259e4fe84515001f1a9918ef86be61ed632682dff8a8b2fdf99db
plain text: It is a test message
```

شکل ۲: خروجی کد