Challenge 3 — Is It Cake?
NKP4, SS24

Aufgabenstellung

Wir betrachten zwei verschiedene Verschlüsselungen, der Code liegt dir jeweils vor. Du hast nun die Möglichkeit, dir mit dem vorliegenden Code unter Verwendung eines dir nicht bekannten Schlüssels beliebig viele Klartexte verschlüsseln zu lassen. Ziel ist es, das jeweils unbekannte aber ebenfalls mitverschlüsselte „Cookie“ zu ermitteln.

Teilaufgabe 1

Dein erstes Verschlüsselungsorakel erreichst du unter der IP 193.170.192.172 und dem Port 31337. Jegliche Daten, die du in einer TCP-Verbindung schickst, werden mit folgender Methode verschlüsselt und wieder an dich retourniert. Deine Aufgabe ist, das „Cookie“ `secret`, das in `self.secret` gespeichert ist, zu ermitteln.

```
def createResponse(self, plaintext):

    cipher = Crypto.Chipher.ChaCha20_Poly1305.new(key=self.key)
    ciphertext, tag = cipher.encrypt_and_digest(zlib.compress(plaintext + b"secret="
        + self.secret))

    jsonkeys = [ "nonce", "ciphertext", "tag" ]
    jsonvalues = [ cipher.nonce.hex(), ciphertext.hex(), tag.hex() ]
    response = json.dumps(dict(zip(jsonkeys, jsonvalues))).encode("utf-8")

    return response
```

1.1 Auf die Länge kommt es an

Schicke an das Orakel testweise irgendeinen 7-Byte-langen Klartext. Schicke zum Vergleich den 7-Byte-langen Klartext `secret=`. Was fällt dir auf?

Nach dieser Teilaufgabe

- ist dir die Schwachstelle im Code bekannt.
- kannst du die retournierten Chiffrate den zugehörigen Klartexten zuordnen.

1.2 Mach den ersten Schritt

Überlege nun, wie du den ersten Character von `self.secret` erraten kannst. Wie viele Anfragen an das Orakel werden dazu in etwa notwendig sein? Ermittle den ersten Character.

Nach dieser Teilaufgabe

- weißt du, wie du die Schwachstelle im Code ausnutzen kannst.
- kennst du den ersten Character des Cookies.

1.3 Ein echtes CRIME

Ermittle nach dem Rezept aus Abschnitt 1.2 Schritt für Schritt das komplette Cookie. Mach aber dazwischen mal halblang! Wie viele Anfragen an das Orakel hast du insgesamt benötigt?

Nach dieser Teilaufgabe

- weißt du, wie viele Anfragen an das Orakel notwendig waren, um das Cookie zu ermitteln.
- kannst du für eine gegebene Cookie-Länge berechnen, wie viele Anfragen zur Ermittlung des Cookies in etwa notwendig sein werden.

Teilaufgabe 2

Dein zweites Verschlüsselungsorakel erreichst du unter der IP 193.170.192.172 und dem Port 80. Jegliche Daten, die du in einer TCP-Verbindung schickst, werden mit folgender Methode verschlüsselt und wieder an dich retourniert. Deine Aufgabe ist, das „Cookie“ `secret2`, das in `self.secret` gespeichert ist, zu ermitteln.

```
def createResponse(self, plaintext):

    cipher = Crypto.Cipher.AES.new(self.key, Crypto.Cipher.AES.MODE_CBC, self.iv)
    ciphertext = cipher.encrypt(Crypto.Util.Padding.pad(plaintext + b"secret2="
        + self.secret, 16))

    jsonkeys = [ "iv", "ciphertext" ]
    jsonvalues = [ cipher.iv.hex(), ciphertext.hex() ]
    response = json.dumps(dict(zip(jsonkeys, jsonvalues))).encode("utf-8")

    self.iv = ciphertext[-16:]

    return response
```

2.1 Du weißt, was die Zukunft bringt

Dir fällt auf, dass du ab dem zweiten Request den IV kennst, der zur Verschlüsselung deiner Nachricht verwendet werden wird. Mache dich schlau, wie der IV im CBC-Modus in die Verschlüsselung einfließt. Verwende dieses Wissen nun, um mit dem Orakel zwei Chiffrate zu erstellen, die identisch sind.

Nach dieser Teilaufgabe

- kannst du mit Hilfe des Verschlüsselungsorakels identische Chiffrate erzeugen.

2.2 Mach den ersten Schritt

Wähle nun deinen Klartext so lange, dass noch genau ein Character von `self.secret` im ersten Klartextblock landet und merke dir das vom Orakel retournierte Chiffrat. Wie kannst du dein Wissen aus Abschnitt 2.1 nutzen, um den ersten Character von `self.secret` zu ermitteln? Wie viele Anfragen an das Orakel werden dazu in etwa notwendig sein? Ermittle den ersten Character.

Nach dieser Teilaufgabe

- kannst du durch geschickte Wahl der Klartexte mit Hilfe des Verschlüsselungsorakels einen ersten Character erraten.
- kennst du den ersten Character des Cookies.

2.3 Ein richtiges BEAST

Ermittle nach dem Rezept aus Abschnitt 2.2 Schritt für Schritt das komplette Cookie. Stößt du dabei an deine (Block-)Grenzen, erweitere deinen (Block-)Horizont! Wie viele Anfragen benötigst du insgesamt?

Nach dieser Teilaufgabe

- kannst du dein Wissen aus Abschnitt 2.2 auch auf andere Blöcke anwenden.
- kennst du das komplette Cookie.
- weißt du, wie viele Anfragen an das Orakel notwendig waren, um das Cookie zu ermitteln.
- kannst du für eine gegebene Cookie-Länge berechnen, wie viele Anfragen zur Ermittlung des Cookies in etwa notwendig sein werden.

Und jetzt hol dir den Badge ...

Deine Angriffe waren erfolgreich und du hast die beiden Cookies ermittelt? Dann schicke sie als Cookies in einem HTTP-Request an `https://www.moneybit.at/challenge3.php`.

Nach dieser Teilaufgabe

- kannst du einen HTTP-Request mit einem HTTP-Cookie erstellen.