Prof. Dr. Ghassan Karame
M. Sc. Pascal Zimmer
M. Sc. Annika Wilde

Aufgabe 1

Python Hands-On

Belohnung: 10 Punkte
Modus: Einzelarbeit
Abgabefrist: 22.04.2024 - 14:15 Uhr

Was für eine Überraschung: anstatt der Flag wartet nun das richtige Aufgabenblatt auf dich!

Dir wurden Daten von einem Informanten zugespielt, welche aus der Kommunikation der Übungsleiter abgefangen wurden und die Lösungen für diese Aufgabe beinhalten. Für die Verschlüsselung der Daten haben sich die Übungsleiter leider an eine Person gewendet, die *nicht* mit der korrekten Verwendung von kryptographischen Primitiven vertraut ist. Als angehende*r Expert*in sollte es ein Leichtes für dich sein, die Lösung zu dieser Aufgabe zu erhalten.

Bei den Daten handelt es sich um:

- 128 verschlüsselte WAV-Audiodateien (AES-128-ECB) im Order `encrypted_audios`.
- eine Signatur (EdDSA)

  `d4f743ad83c57e89ec8b2461bc027c93b2f23b25c8649000bceb061117c764f6`
  `991d8fe62d10345c9fe601df841843c695c48e49e4ec239ec93d998adedfd304`

- ein Zertifikat (X.509-Format) in der Datei `certificate.pem`.

Für die Entschlüsselung der verschlüsselten WAV-Audiodateien benötigst du ein Passwort, welches dein Informant leider nicht abfangen konnte. Jedoch ist bekannt, dass die Schlüsselgenerierung nicht sicher sein soll und der möglichen Schlüsselraum stark in seiner Größe beschränkt ist.

Dein Informant konnte das verwendete Schlüsselenhancement in Erfahrung bringen:

```
# enhance password entropy
for i in range(16):
    key[i] = key[i] ^ 0xFF
    key[i] = key[i] & 60
    key[i] = key[i] | 0x81
    key[i] = key[i] << 5 //leftshift, no rotation
```

Aufgabe

Die Aufgabe ist es nun die Flag herauszufinden. Nachdem du die Datei entschlüsselt hast, erhältst den Tipp, dass die abgefangene Signatur zu genau einer dieser WAV-Audiodateien passt, *bevor* ein Padding angewandt worden ist. Nutze den öffentlichen Schlüssel aus dem Zertifikat, um die korrekte Audiodatei zu bestimmen. Die Flag ist das gesprochene Wort in dieser Datei.

Deliverables

Bitte reiche **sowohl die Flag**, als auch deinen **Python-Quellcode** ein, den du zur Berechnung verwendet hast. Ohne die Abgabe des Python-Quellcodes können bei dieser Aufgabe **keine** Punkte erreicht werden.

Plagiate[1]

ACM definiert Plagiat als die fälschliche Darstellung von Schriften, Ideen oder anderen kreativen Arbeiten einer anderen Person (einschließlich unveröffentlichter und veröffentlichter Dokumente, Daten, Forschungsvorschläge, Computercode oder anderer Formen des kreativen Ausdrucks, einschließlich elektronischer Versionen) als die eigene Arbeit. Ein Plagiat ist ein klarer Verstoß gegen die ACM-Publikationspolitik und ein möglicher Verstoß gegen den ACM-Ethikkodex. Plagiate können auch eine Verletzung des Urheberrechts darstellen. Plagiate äußern sich in einer Vielzahl von Formen, darunter:

- wortwörtliches Kopieren, nahezu wortwörtliches Kopieren oder absichtliches Paraphrasieren von Teilen der Arbeit eines anderen;
- die Verwendung automatisierter Tools, die vorhandene Arbeiten als eigenen Text umformulieren, ohne dass eine angemessene Namensnennung erfolgt;
- Kopieren von Elementen einer fremden Arbeit, wie Gleichungen, Tabellen, Diagramme, Illustrationen, Darstellungen oder Fotos, die nicht allgemein bekannt sind, oder Kopieren oder absichtliches Paraphrasieren von Sätzen ohne ordnungsgemäße oder vollständige Quellenangabe;
- wortwörtliches Kopieren von Teilen einer fremden Arbeit mit falscher Quellenangabe

Bei der Verwendung von Stack-Overflow oder ähnlich, bitten wir demnach um Angabe der Quelle von Code-Bausteinen, die nicht selbstständig geschrieben worden sind.

[1] Übersetzung von `https://www.acm.org/publications/policies/plagiarism-overview` mit DeepL.