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

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.

Die Person hat die Flag zu dieser Aufgabe in einem ZIP-Archiv gespeichert und dieses Archiv mit einem komplexeren AES-Modus (CBC, OFB, oder CFB) verschlüsselt. Sowohl die Daten als auch das verwendete Passwort werden mit angehängten **Nullbytes** auf die Block- und Schlüsselgröße von 128-bit aufgefüllt. Zur Sicherung des Passwortes wird dieses in einem 600×600 großen PNG Bild gespeichert, in das RGBA-Format konvertiert (32-bit pro Pixel) und mit AES-ECB verschlüsselt.

Aufgabe

Die Aufgabe ist es nun die Flag herauszufinden. Für die Entschlüsselung des verschlüsselten ZIP-Archivs (`archive.enc`) benötigst Du das geheime Passwort, das in dem verschlüsselten Bild (`password.rgba`) gespeichert wurde. Leider konnte dein Informant den Schlüssel für das ECB-verschlüsselte Bild **nicht** abfangen.

Hinweis: Bei korrekter Entschlüsselung des ZIP-Archivs ist die Flag eindeutig zu erkennen.

Deliverables

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

Hinweise

Für die Aufgabe wurden folgende Versionen verwendet:

- Python 3.8
- `cryptography 42.0.5` (`https://pypi.org/project/cryptography/`)
- `numpy 1.24.4`
- `opencv-python 4.9.0.80`

Die SHA-3 Prüfsumme der Dateien lauten:

`password.rgba` : `b74127a0054faf76fe8dc7b9715594d582350a8989ee6db3944cb71a`
`archive.enc` : `74aecf95ebbf30df49c9f900fb9ee071a3c6b41e546c93ff7384e0e2`

und kann mit dem Befehl `openssl dgst -sha3-224 file` ermittelt 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.