HE Übungen 3

Diese Übung ist Teil der Vorlesung Hacking Exposed an der Juventus Technikerschule HF in Zürich.

1 Warm-Up

Aussage	Wahr	Falsch
Zur Berechnung der Anzahl möglicher Kombinationen eines Passwortes bezeichnet die Basis die Menge möglicher Zeichen und der Exponent die Anzahl Stellen des Passworts.		
Mit Brute-Force kann man jedes Passwort knacken.		
Mit einem Salt kann man einen Passwort-Hash verstärken.		
Die Sicherheit eines Verschlüsselungsverfahrens darf nur von der Geheimhaltung des Algorithmus abhängen, nicht von der Geheimhaltung des Schlüssels.		
Die symmetrische Kryptographie verwendet für die Verschlüsselung und Entschlüsselung stets zwei verschiedene Schlüssel.		
In einem asymmetrischen Kryptographie-Algorithmus ist die Schlüssellänge immer gleich die Bit-Stärke.		
Eine Hashfunktion wird auch als Einweg- oder Falltürfunktion bezeichnet.		
Über die Bit-Stärke kryptographischer Verfahren lassen sich diese untereinander vergleichen.		
Die Anzahl öffentlicher Schlüssel in einem asymmetrischen Kryptosystem wächst schneller (genauer $O(n^3)$) als in einem symmetrischen Kryptosystem.		
AES-128, SHA-256 und RSA 3072 haben dieselbe Bitstärke.		

2 1 Attacke auf Galaxus Digitec AG

Am 3. Oktober 2019 wurde die Webseite von Galaxus Digitec AG respektive deren Datenbank abgegriffen: https://www.tagesanzeiger.ch/digital/internet/hacker-greifen-tausende-digitecgalaxuskonten-an/story/21818266

1. Prüfen Sie mit dem Dienst Have I Been Pwned von Troy Hunt, ob sich Ihre Daten auch einem Datenbank-Breach befinden.

3 Passwortstärke

Um ein Passwort zu knacken, müssen alle möglichen Kombinationen getestet werden. Also ist ein Passwort potentiell stärker, wenn es mehr mögliche Kombinationen gibt.

1. Berechnen Sie die Stärke folgender Passwörter in Anzahl möglicher Kombinationen und deren Bit-Stärke:

Passwort	Kombinationen	Bit-Stärke
`swordfish` [a-z]		
`42` [0-9]		
`zV]fRGC%}+` `[a-zA-Z !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~]`		

4 Kryptographie allgemein

1. Erklären Sie in eigenen Worten, was das Prinzip von Kreckhoff besagt.

2. Erklären Sie in eigenen Worten, wieso eine Brute-Force Attacke nicht zwingend die schnellste Möglichkeit ist, ein System zu knacken.

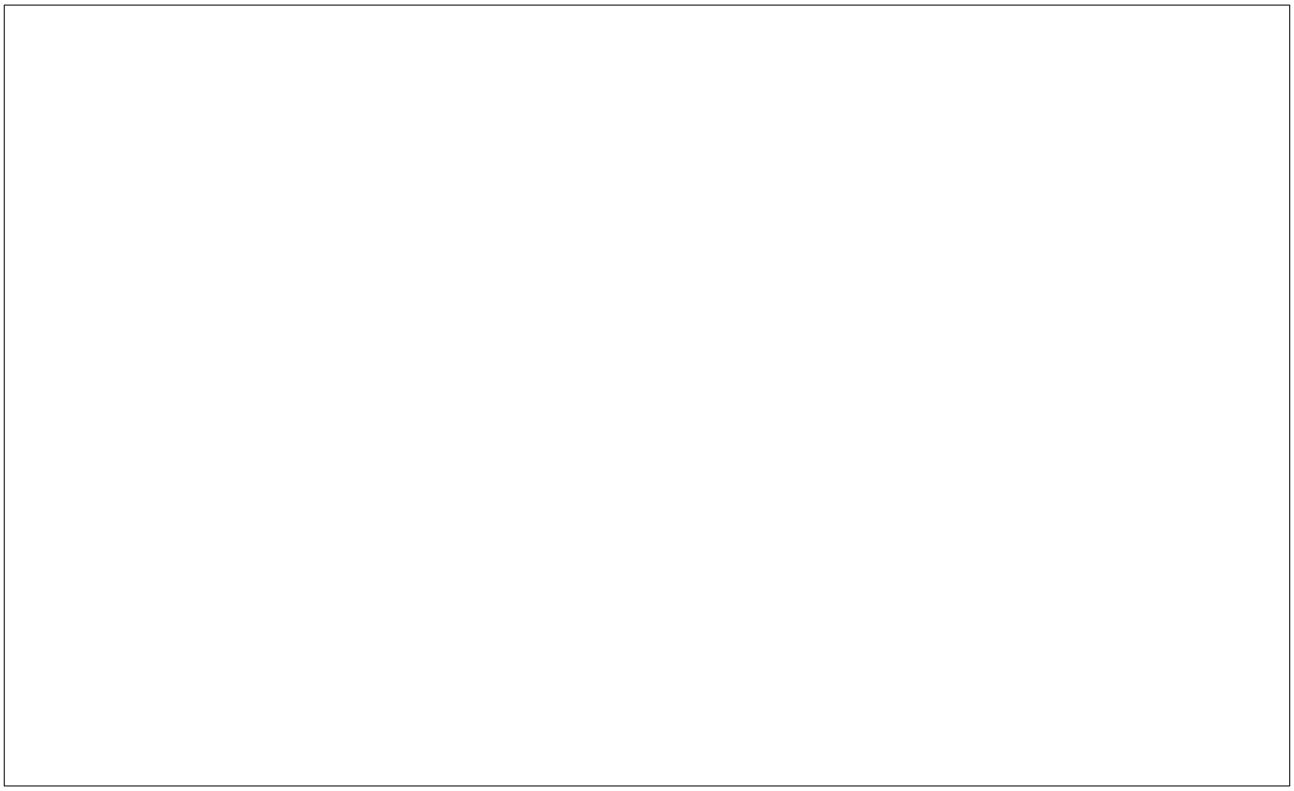
5 Digitale Signatur

1. Erklären Sie anhand einer Skizze, wie eine digitale Signatur eines Dokuments erstellt werden kann. Welche Komponenten brauchen Sie zwingend für eine digitale Signatur nebst dem Dokument selber?

6 SHA1 Problematik

Lesen Sie folgende Artikel und fassen Sie die wichtigsten Punkte zusammen. Zu diesem Thema gibt es auch das praktisches Lab SHA1 Shattered auf GitHub.

1. Arstechnica: PGP keys, software security, and much more threatened by new SHA1 exploit



2. Cloudflare: Why it's harder to forge a SHA-1 certificate than it is to find a SHA-1 collision