GSS-Übungsblatt 6

Alexander Timmermann, Jannis Krämer

Aufgabe 1: Zentrale Begriffe der Kryptographie

2. Bei einem symetrischen Kryptosystem wird für Ver- und Entschlüsselung nur ein Schlüssel verwendet, bei einem asymetrischen jeweils ein distinkter für Ver- und Entschlüsselung. Bei einem symetrischen Verfahren müssen demnach für jede mögliche Kombination aus sendender Person und empfangender Person ein Schlüssel generiert werden, insgesamt also $\binom{n}{2}$. Bei einem asymetrischen Kryptosystem benötigt jede Person einen öffentlichen und einen privaten Schlüssel und kann danach durch Herausgabe des öffentlichen Schlüssels und bei Geheimhaltung des privaten Schlüssels mit allen anderen Gruppenmitgliedern kommunizieren ohne dass jemand unbefugtes die Nachricht entschlüsseln könnte. Hierbei werden insgesamt also nur $2n$ Schlüssel benötigt.

3.

- Aufgrund des hohen Rechenaufwandes ausymetrischer Kryptosysteme wird Alice für zeitkritische Übertragungen (Echtzeitapplikationen o.ä.) sowie für große Datenmengen. Auch für das Versenden einer Nachricht an mehrere Empfänger*innen ohne erneute Verschlüsselung kann Alice sich für ein hybrides Kryptosystem entscheiden.
- Alice erzeugt mit einem symmetrischen Verschlüsselungssystem einen neuen Schlüssel. Damit verschlüsselt sie die Nachricht. Den symmetrischen Schlüssel verschlüsselt sie ebenfalls, jedoch mit Bobs öffentlichen Schlüssel. Dann schickt sie beide Chiffres an Bob. Dieser kann nun zuerst den symetrischen Schlüssel entschlüsseln und mit diesem dann die Nachricht selbst entschlüsseln.
- Die Nachricht würde vorraussichtlich aus einem Header bestehen, in dem der symetrische Schlüssel übertragen wird und einem Teil für die codierte Nachricht. Die genaue Umsetzung ist dabei von Protokoll zu Protokoll unterschiedlich.

Aufgabe 2: Parkhaus

2. Der Barcode, der vom Kassenautomaten auf das Ticket gestempelt wird, scheint immer der gleiche zu sein und kann somit wohl nur eine binäre Bestätigung des Bezahlens sein. Dieser, sowie die menschenlesbaren Informationen unten links, könnte ein*e Angreifer*in also auf das Ticket drucken und damit versuchen, gratis zu parken.

Auch die Rabattbarcodes scheinen sich nicht sehr zu verändern und ließen sich nach Probieren verschiedener Kombinationen zu fälschen; in unser Stichprobe erscheinen nur drei unterschiedliche Rabattbarcodes.

Dem System liegt offenbar ein Angreifermodell zugrunde dass von einem externen Angriff ausgeht, der zwar über beliebig viel Rechenkapazität, jedoch nicht über einen Barcodedrucker verfügen kann.

3. Die besten Ergebnisse würde eine Umstellung des Ticket-Systems auf ein generell sicheres System (z.B. RFID-Parktickets) erzielen.

Das vorhandene System würde davon profitieren, wenn sowohl in den Rabattcodes als auch im Kassenautomaten-Barcode das Datum und die Uhrzeit codiert wäre. Das würde das System zwar auch nicht endgültig absichern, jedoch wäre eine Entschlüsselung deutlich aufwendiger. Dies scheint bisher nicht der Fall zu sein.

Aufgabe 3: Authentifizierungsprotokolle

2. Ein*e Angreifer*in kann sich bei diesem System immer noch beim Server athentifizieren, indem sie*er als passive*r Angreifer*in während der Übertragung r und c abgreift. Da bei diesem Ansatz die Daten immer noch unverschlüsselt übertragen werden, ist dies ungehindert möglich.

Einzig ein Angriff bei dem ein*e Angreifer*in versucht, die Login-Daten u und p abzugreifen wird dadurch verhindert.

3. Durch das Challenge-Response-System müsste ein*e Angreifer*in die Verschlüsselungsfunktion E und den Schlüssel k kennen um dem Server die korrekte Response zu liefern, ohne die es nun nicht mehr möglich ist sich als jemand anders auszugeben.

Dieses System schützt jedoch nicht vor einem Man-in-the-Middle-Angriff, bei dem sich der*die

Angreifer*in zwischen Server und Client schaltet und sowohl die Challenge des Servers als auch die Response des Client abgreift und diese dann weiterleitet, als hätte die Generierung auf dem angreifenden System stattgefunden.

Nach der Authentifizierung kann durch die Man-in-the-Middle-Attack außerdem der (immer noch unverschlüsselte) Daten mitlesen und ggf. anpassen.

Aufgabe 5: RSA-Verfahren

Nach der Berechnung von $d = 4343$ ergibt sich folgender entschlüsselter Text:

> Fuer die GSS-Klausur sind folgende Themen wichtig: Angreifermodelle, Schutzziele, Rainbow Tables, die (Un-)Sicherheit von Passwoertern und dazugehoerige Angriffe, Zugangs- und Zugriffskontrolle, Timing-Attack und Power-Analysis, Biometrische Verfahren, Grundlagen der Kryptographie, das RSA-Verfahren, Authentifikationsprotokolle und natuerlich alle anderen Inhalte, die wir in der Uebung und der Vorlesung behandelt haben :-)

Nachfolgend der benutzte Code:

```
1  #!/usr/bin/env python3
2  import itertools
3
4  p = 271
5  q = 379
6  e = 47
7
8  data = [14979, 20999, ...]
9
10 n = p*q
11 p1q1 = (p-1)* (q-1)
12 for d in itertools.count():
13     if (e*d) % p1q1 == 1:
14         break
15
```

```
16 def decode(c):
17     return chr((c ** d) % n)
18
19 print('d = {}'.format(d))
20 print("".join(map(decode, data)))
```