



Aufgabe 1: Zentrale Begriffe der Kryptographie

(1) **Unterschiedliche Chiffren:** Bei einem **symmetrischen Kryptosystem** wird ein einziger Schlüssel zum ver- sowie entschlüsseln von Daten von beiden Kommunikationspartnern genutzt. Das zugrundeliegende Konzept von **asymmetrischen Kryptosystemen** sieht für jeden Kommunikationspartner hingegen jeweils einen öffentlichen und einen privaten Schlüssel vor. Die öffentlichen Schlüssel werden von den Kommunikationspartnern ausgetauscht, steht einem der öffentlichen Schlüssel eines Kommunikationspartners parat, so kann man Daten für diese Person verschlüsseln, die nur mit dem dazugehörigen privaten Schlüssel dieser Person wieder zu entschlüsseln sind.

(2a) Da symmetrische Verschlüsselungsverfahren performanter sind, wäre ein mögliches Einsatzszenario z.B. der Versand sehr großer Nachrichten / Datenmengen von Alice an Bob. Für sehr vertrauliche Daten eignet sich hingegen eher die Kommunikation mit asymmetrischen Verschlüsselungsverfahren, da hier eine höhere Sicherheit vorherrscht. Abgesehen davon ist die zu verwaltende Schlüsselmenge bei mehreren Kommunikationspartnern bei asymmetrischen Systemen kleiner.

Deshalb bietet sich allgemein ein hybrides Verfahren an, da alle oben aufgezählten Vorteile von symmetrischen und asymmetrischen Verfahren kombiniert werden: Sicherheit, Geschwindigkeit auch bei großen Datenmengen und einfacher zu verwaltende Schlüssel.

(2b) Konkret würde Alice dann die Nachricht N mit einem zufällig generiertem Schlüssel S_s symmetrisch verschlüsseln. Dieser symmetrische Schlüssel S_s wird von Alice dann mit dem öffentlichen Schlüssel K_p^B von Bob asymmetrisch verschlüsselt. Danach schickt Alice die Daten an Bob. Bob kann dann mit seinem privaten Schlüssel K_s^B den verschlüsselten Schlüssel S_s entschlüsseln und mit diesem dann die symmetrisch verschlüsselte Nachricht N wieder entschlüsseln.

(2c) In der Nachricht N sind die Daten, der eigentliche Kommunikationsinhalt gespeichert. Die Nachricht N ist mit dem zufällig generierten Schlüssel S_s symmetrisch verschlüsselt (z.B. mit AES, der Advanced Encryption Standard ist weitverbreitet und wird häufig genutzt). Der Schlüssel S_s selbst wiederum ist mit dem öffentlichen Schlüssel K_p^B von Bob asymmetrisch verschlüsselt. Sowohl N als auch S_s könnte Alice so sicher zusammen, z.B. in einer E-Mail an Bob, schicken. N und S_s könnten aber auch getrennt voneinander übermittelt werden.



Aufgabe 2: Parkhaus

(2) **Schwächen des Systems:** Auf den Tickets ist zu erkennen, dass der Barcode an der ersten Stelle stets der gleiche zu sein scheint. So haben alle Besucher des Kinos den Barcode „32“ erhalten, der ihnen das Parken für 2,50 Eur ermöglicht. Außerdem tauchen noch Barcodes mit den Bezeichnungen „34“ und „36“ auf, zu denen vermutlich auch der Einzelhändler mit den vergünstigten Parktickets gehört. So könnten sich versierte Individuen also selbst diesen Barcode auf ihre Parktickets drucken um vergünstigt zu parken.

Angreifermodell:

- a) **Rollen des Angreifers:** Außenstehender, Benutzer
 - b) **Verbreitung des Angreifers:** Der Angreifer hat lediglich Zugriff auf die Parktickets, nicht die Automaten
 - c) **Verhalten des Angreifers:** aktiv; vorhandene Parktickets werden verändert
 - d) **Rechenkapazität des Angreifers:** zum fälschen eines Parktickets wird keine besondere Rechenkapazität benötigt, der entsprechende Code muss nur korrekt aufgedruckt werden
- (3) Anstatt den Rabattcode unverschlüsselt aufzudrücken, könnte man ein hybrides Verschlüsselungssystem nutzen. Man definiert fixe Rabattcodes, z.B. „R01“ für 2,50 Eur Rabatt. Das macht man für jeden Rabattvorteil den ein Geschäft vergeben können soll. Außerdem wählt man ein asymmetrisches Verfahren aus und erzeugt für den Kassensautomaten ein Schlüsselpaar, bestehend aus privatem und öffentlichen Schlüssel. Der öffentliche Schlüssel wird an die Geschäfte verteilt.

Bei Vergabe eines Rabatts beispielsweise vom Kino wird dann ein zufälliger Schlüssel S für eine symmetrische Verschlüsselung erzeugt, mit dem man den Rabattcode, z.B. „R01“, verschlüsselt. Der Schlüssel S wird dann mit dem öffentlichen Schlüssel des Kassensautomaten asymmetrisch verschlüsselt. Beides wird auf das Parkticket aufgedruckt. Der Kassensautomat entschlüsselt nun mit seinem privaten Schlüssel den Schlüssel S und entschlüsselt danach den Rabattcode mit dem Schlüssel S .

Bei diesem System würde sich der aufgedruckte Rabattcode ständig ändern, weil er immer mit einem zufälligem symmetrischen Schlüssel verschlüsselt ist. Kein Angreifer könnte einen Rabattcode einfach kopieren. Da der private Schlüssel des Kassensautomaten geheim ist, könnte ein potentieller Angreifer auch nicht die geheimen Rabattcodes auslesen, da er den Schlüssel S nicht entschlüsseln kann. Somit könnte er auch nicht einfach selbst die Rabattcodes erzeugen.

Aufgabe 3: Authentifizierungsprotokolle

Aufgabe 4: ?Mensch ärgere Dich nicht? über das Telefon

Aufgabe 5: RSA-Verfahren