# Aufgabe E

*2Tell* ist ein großer Messengerdienst. Er wirbt damit, Nachrichten zwischen Kommunikationspartnern so zu versenden, dass niemand Drittes diese Nachrichten unbefugt lesen kann.

a) Für die Nachrichtenübermittlung besitzt jeder Nutzer ein Schlüsselpaar bestehend aus einem öffentlichen und einem privaten Schlüssel. Das Schlüsselpaar wird auf dem eigenen Gerät erzeugt.
Beschreiben Sie, wie mithilfe der Schlüsselpaare ein verschlüsselter Nachrichtenaustausch zwischen den beiden Kommunikationspartnern Alice und Bob durchgeführt werden kann.
Während der Entwicklungsphase des Messengers wurde vorgeschlagen, nach der Installation der App bei der Erstanmeldung auf einem Server der Firma *2Tell* ein Schlüsselpaar von *2Tell* generieren zu lassen und das Schlüsselpaar unmittelbar unverschlüsselt an den Nutzer zu übersenden.
Erläutern Sie zwei Aspekte, die an dieser vorgeschlagenen Vorgehensweise problematisch sind.

[8 BE]

b) Alice und Bob möchten über *2Tell* miteinander kommunizieren. Eve schaltet sich permanent unbemerkt zwischen Alice und Bob. Der durch Eve beeinflusste Schlüsselaustausch ist in Abbildung 1 im Material dargestellt.
Erläutern Sie eine Möglichkeit für Eve, den weiteren Nachrichtenaustausch zu manipulieren.
Beschreiben Sie, wie eine solche Manipulation mithilfe von Zertifikaten verhindert werden kann.

[8 BE]

c) Ein öffentlich bekanntes Verfahren generiert aus einer beliebig langen Nachricht einen „digitalen Fingerabdruck“ in Form einer Binärzahl fester Länge. Dieses soll im Allgemeinen für verschiedene Nachrichten verschiedene digitale Fingerabdrücke erzeugen.

David erzeugt zu einer Nachricht einen digitalen Fingerabdruck, wendet seinen privaten Schlüssel darauf an und verschickt das Ergebnis zusammen mit der Nachricht an Felix.

Erläutern Sie, welche Rückschlüsse Felix aus dem Ergebnis und der Nachricht ziehen kann.

Ein Verfahren zur Erzeugung eines digitalen Fingerabdrucks soll unter anderem die folgenden Anforderungen erfüllen:

i) Die Veränderung eines Bit einer Nachricht soll mindestens die Hälfte der Bits des digitalen Fingerabdrucks verändern.

ii) Es soll nicht möglich sein, aus dem digitalen Fingerabdruck die Nachricht wiederherzustellen.

Es wird vorgeschlagen, das in der Abbildung 2 exemplarisch dargestellte Verfahren zur Erzeugung eines digitalen Fingerabdrucks für Nachrichten der Länge 16 Bit zu verwenden.

Bestimmen Sie unter Verwendung des Verfahrens den digitalen Fingerabdruck für die Nachricht `0010111110011001` mithilfe der Tabelle im Material in Abbildung 3.
Die binären Nachrichten in Abbildung 2 und Abbildung 3 unterscheiden sich nur an der letzten Stelle der Nachricht.
Beurteilen Sie, ob das vorgeschlagene Verfahren die Anforderungen i) und ii) erfüllt.

[9 BE]

# Material

**zu Aufgabenteil b)**

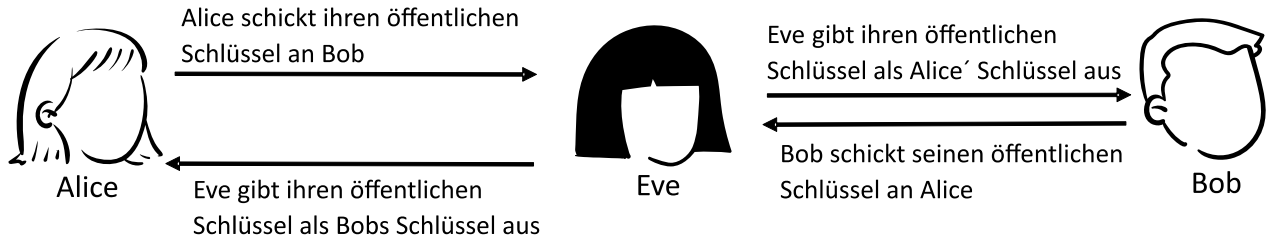


Abbildung 1: Eingriff in den Schlüsselaustausch durch Eve

**zu Aufgabenteil c)**

Die zu übertragende binäre Nachricht wird in 4-Bit-Blöcke aufgeteilt und der digitale Fingerabdruck wie im folgenden Beispiel berechnet:

| **Binäre Nachricht** | **0010** | **1111** | **1001** | **1000** |
|---|---|---|---|---|
| **Dezimaler Wert** | 2 | 15 | 9 | 8 |
| **Ziffernsumme** | 2 + 1 + 5 = 8 | | 9 + 8 = 17 | |
| **Prüfung** | 8 | | 17 - 16 = 1 | |
| **Binär** | 1000 | | 0001 | |
| **Digitaler Fingerabdruck** | 10000001 | | | |

In der Zeile Prüfung wird bei einer berechneten Ziffernsumme größer 15 die Zahl 16 subtrahiert, andernfalls die Ziffernsumme übernommen.

Der digitale Fingerabdruck der Nachricht `0010111110011000` ist damit `10000001`.

*Abbildung 2: Verfahren zur Berechnung des digitalen Fingerabdrucks*

| **Binäre Nachricht** | **0010** | **1111** | **1001** | **1001** |
|---|---|---|---|---|
| **Dezimaler Wert** | 2 | 15 | | |
| **Ziffernsumme** | 2+1+5 = 8 | | | |
| **Prüfung** | 8 | | | |
| **Binär** | 1000 | | | |
| **Hashwert** | | | | |

*Abbildung 3: Hashwertberechnung der veränderten binären Nachricht*