Visuelle Kryptographie mit Komplementärfarben-Segmenten

Ramon Pfeiffer

Eberhard-Karls-Universität Tübingen
Wilhelm-Schickard-Institut für Informatik
Arbeitsbereich Theoretische Informatik / Formale Sprachen

13. Dezember 2012

Übersicht

Motivation

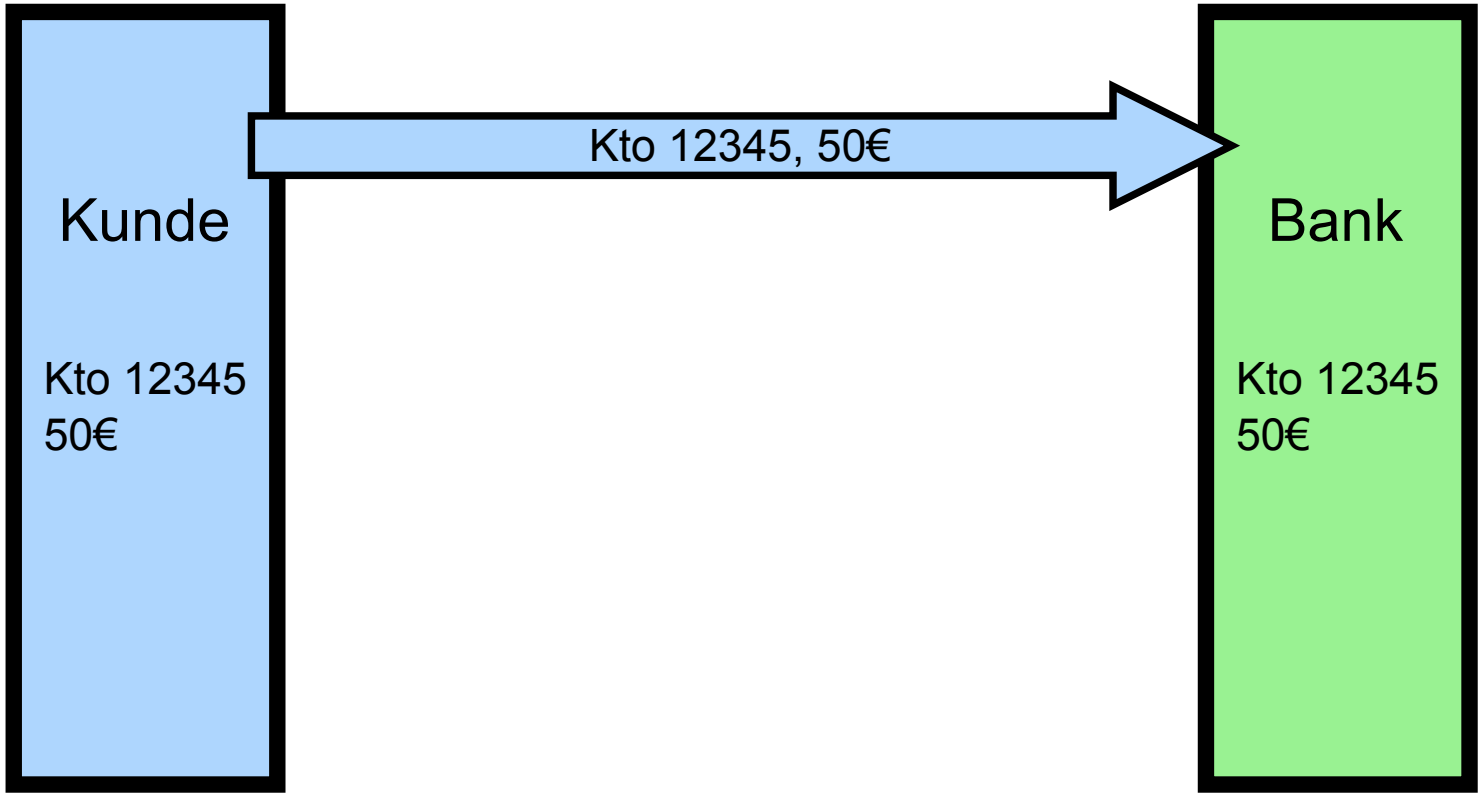
- Umfrage des Branchenverbands deutscher Banken (April 2011):
  - 50% der Bevölkerung nutzt das Internet für Bankgeschäfte
  - 50% davon mindestens einmal pro Woche
  - Fast die Hälfte der Benutzer schätzt das Online-Banking als sicher oder sehr sicher ein.
- Dennoch Möglichkeiten für Angriffe, zum Beispiel durch Banking-Trojaner

Motivation

Man-in-the-Middle-Angriff

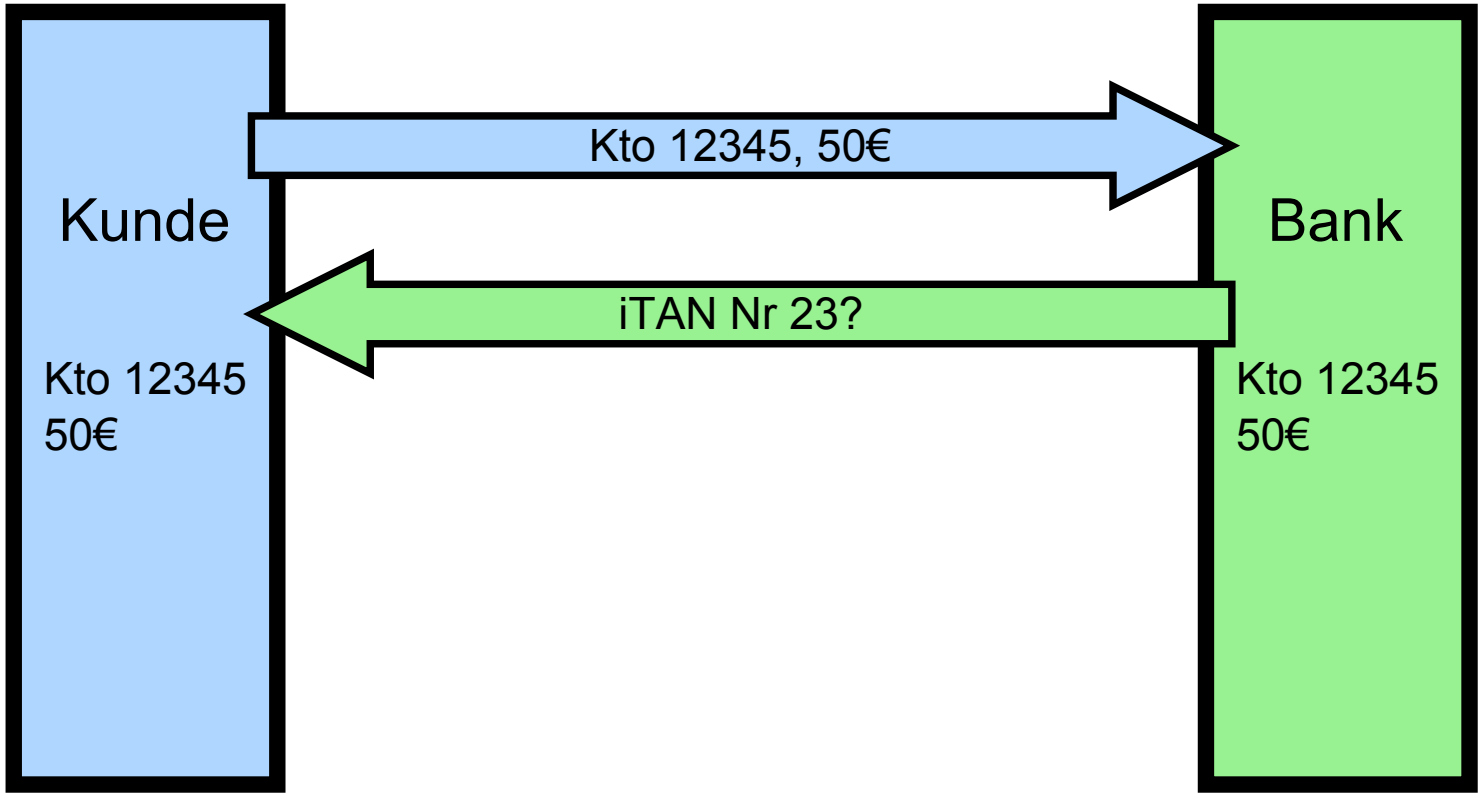
Motivation

Man-in-the-Middle-Angriff



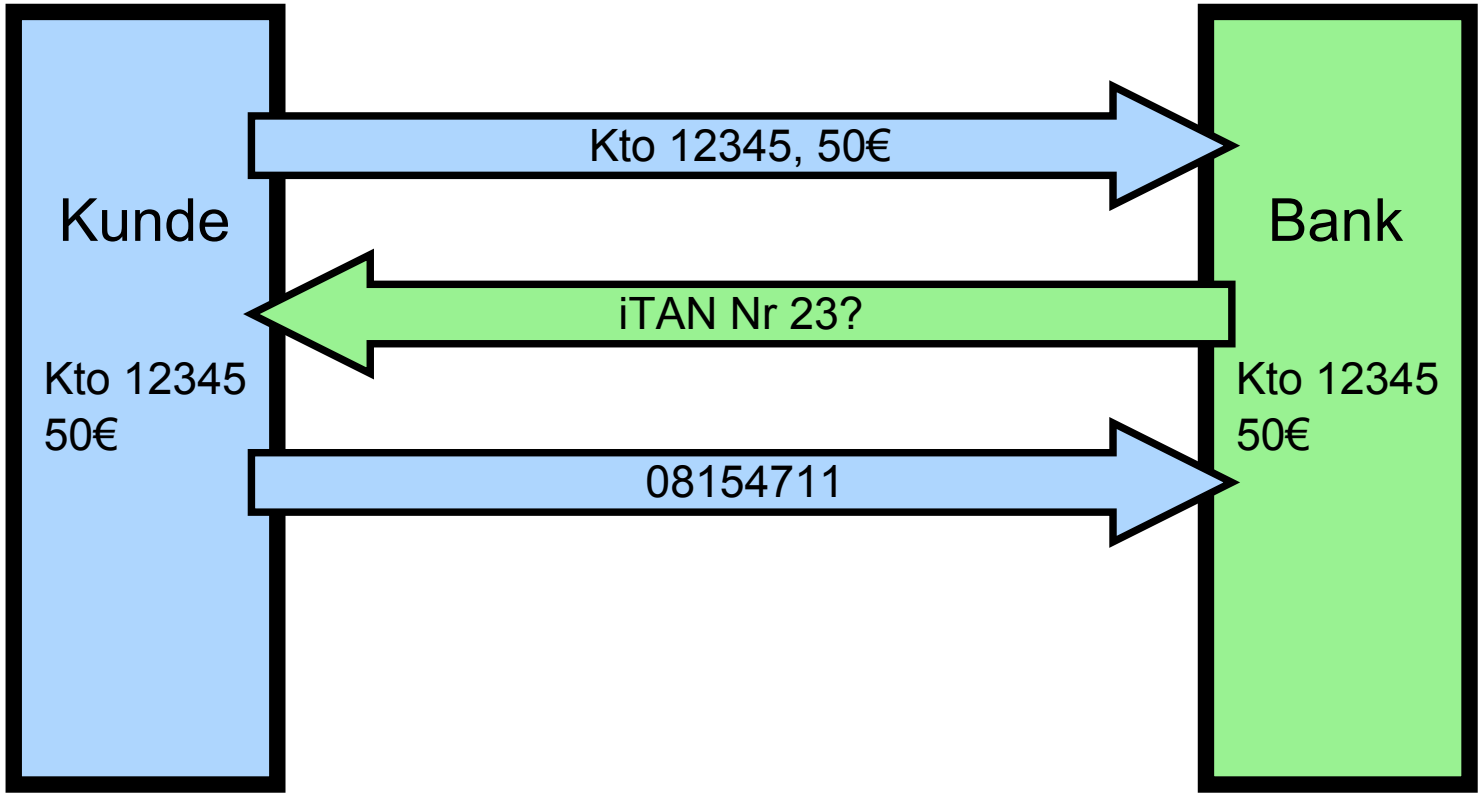
Motivation

Man-in-the-Middle-Angriff



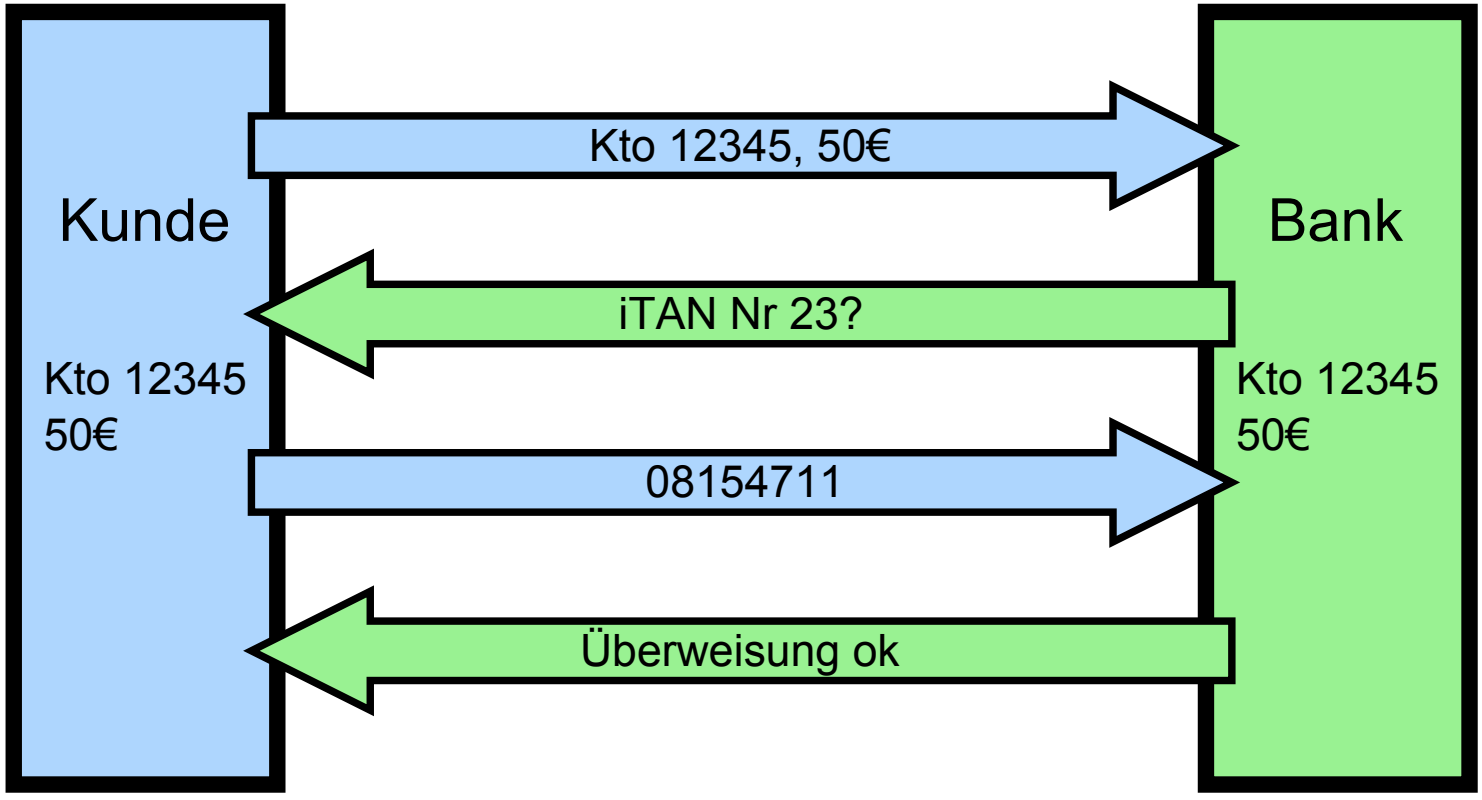
Motivation

Man-in-the-Middle-Angriff



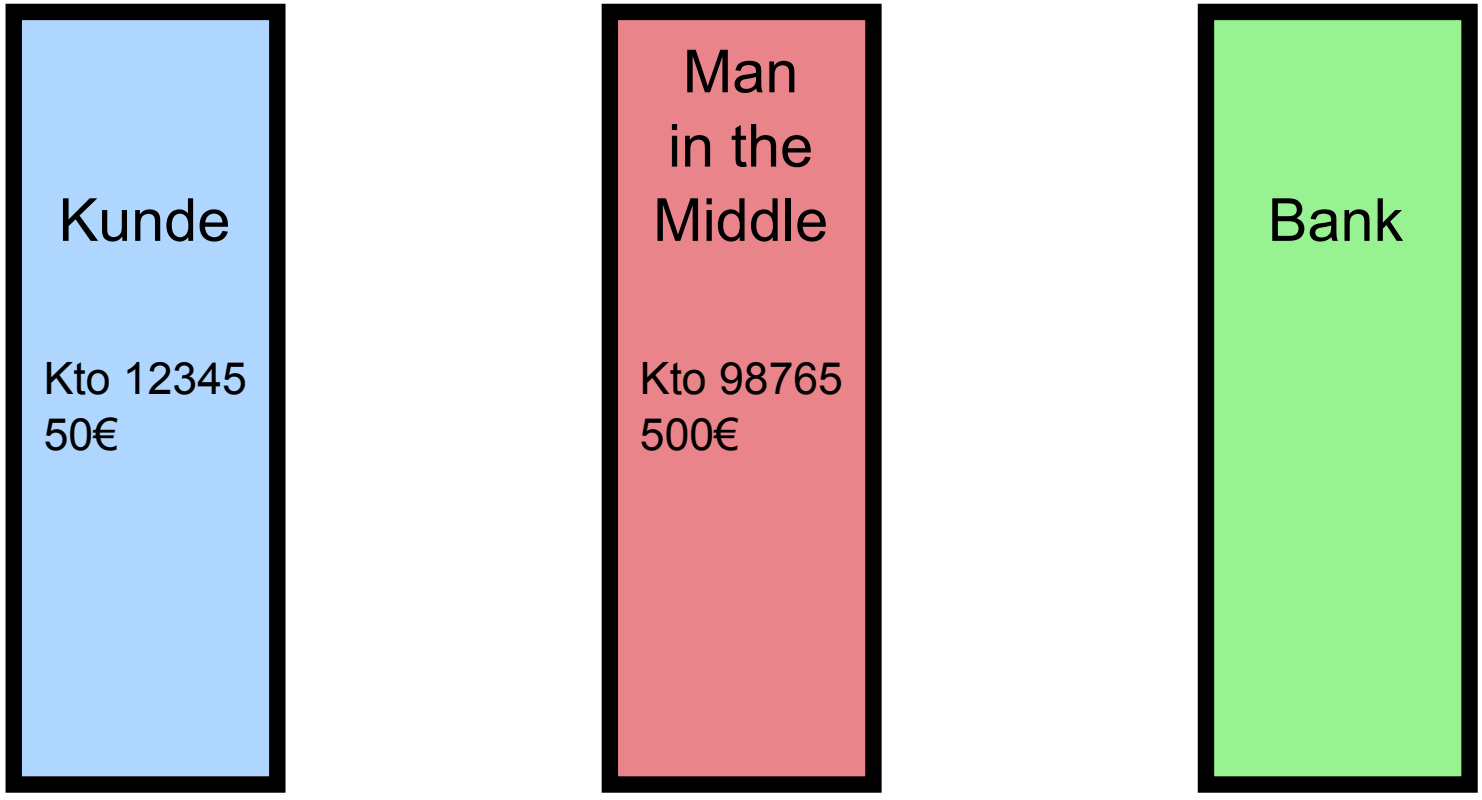
Motivation

Man-in-the-Middle-Angriff



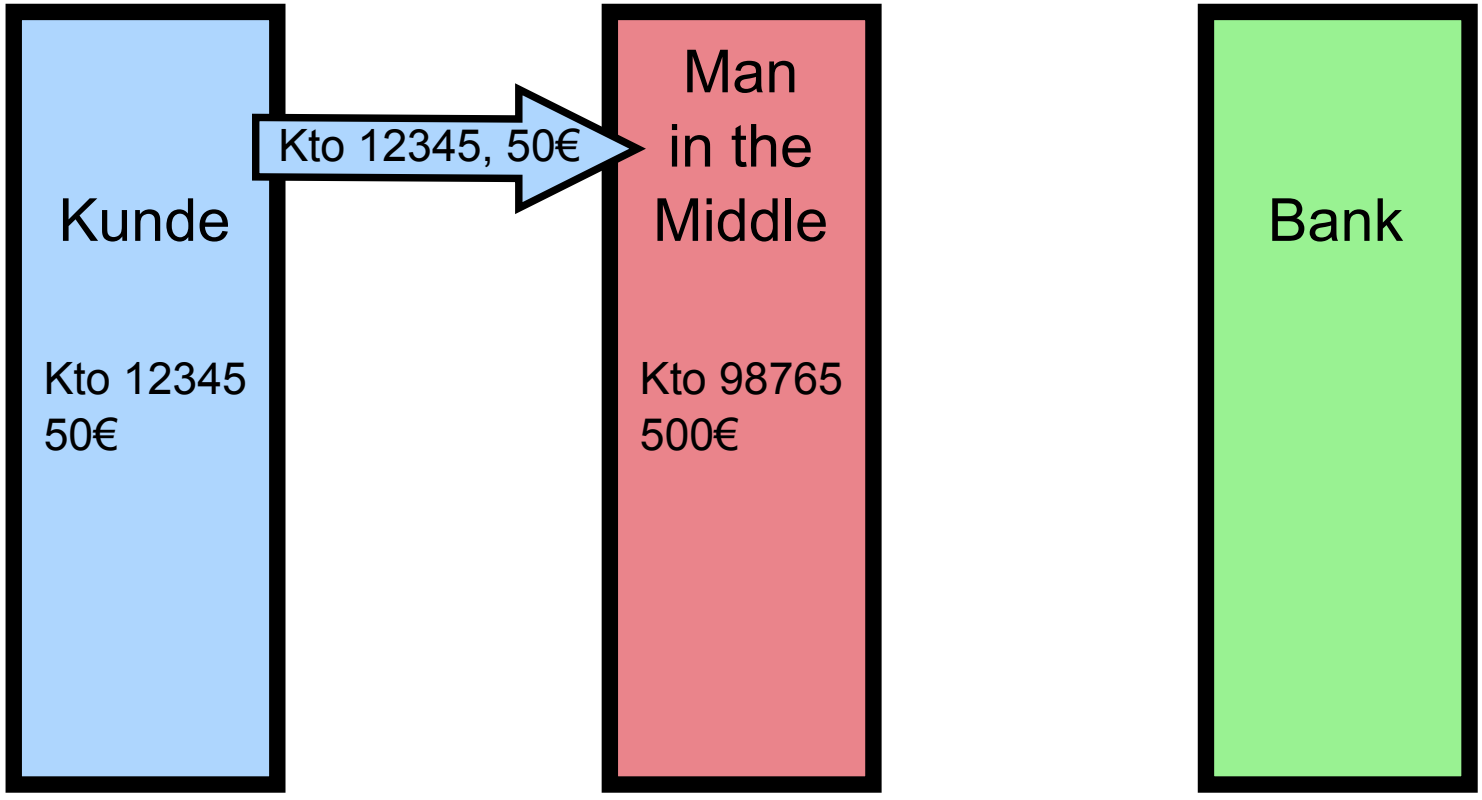
Motivation

Man-in-the-Middle-Angriff



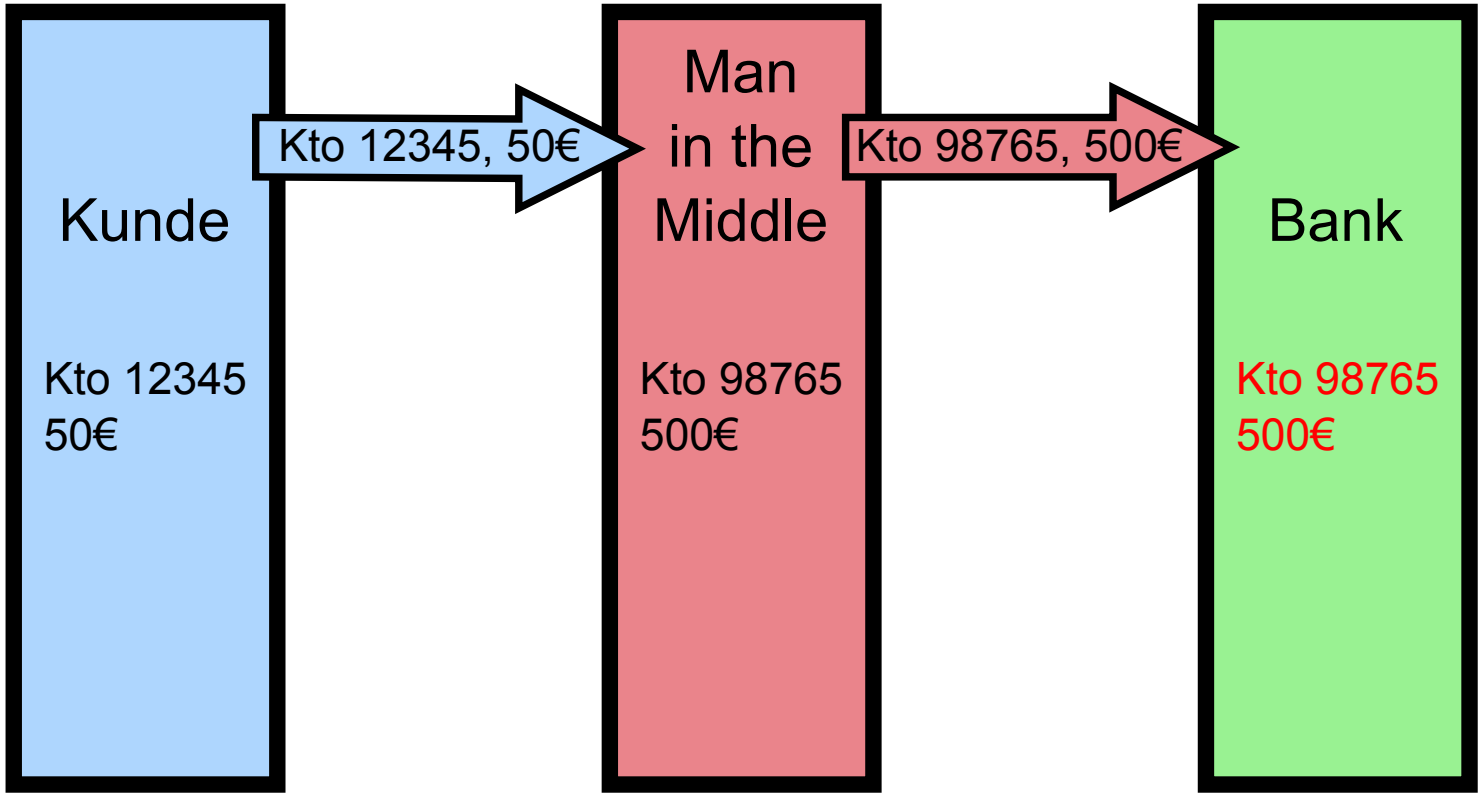
Motivation

Man-in-the-Middle-Angriff



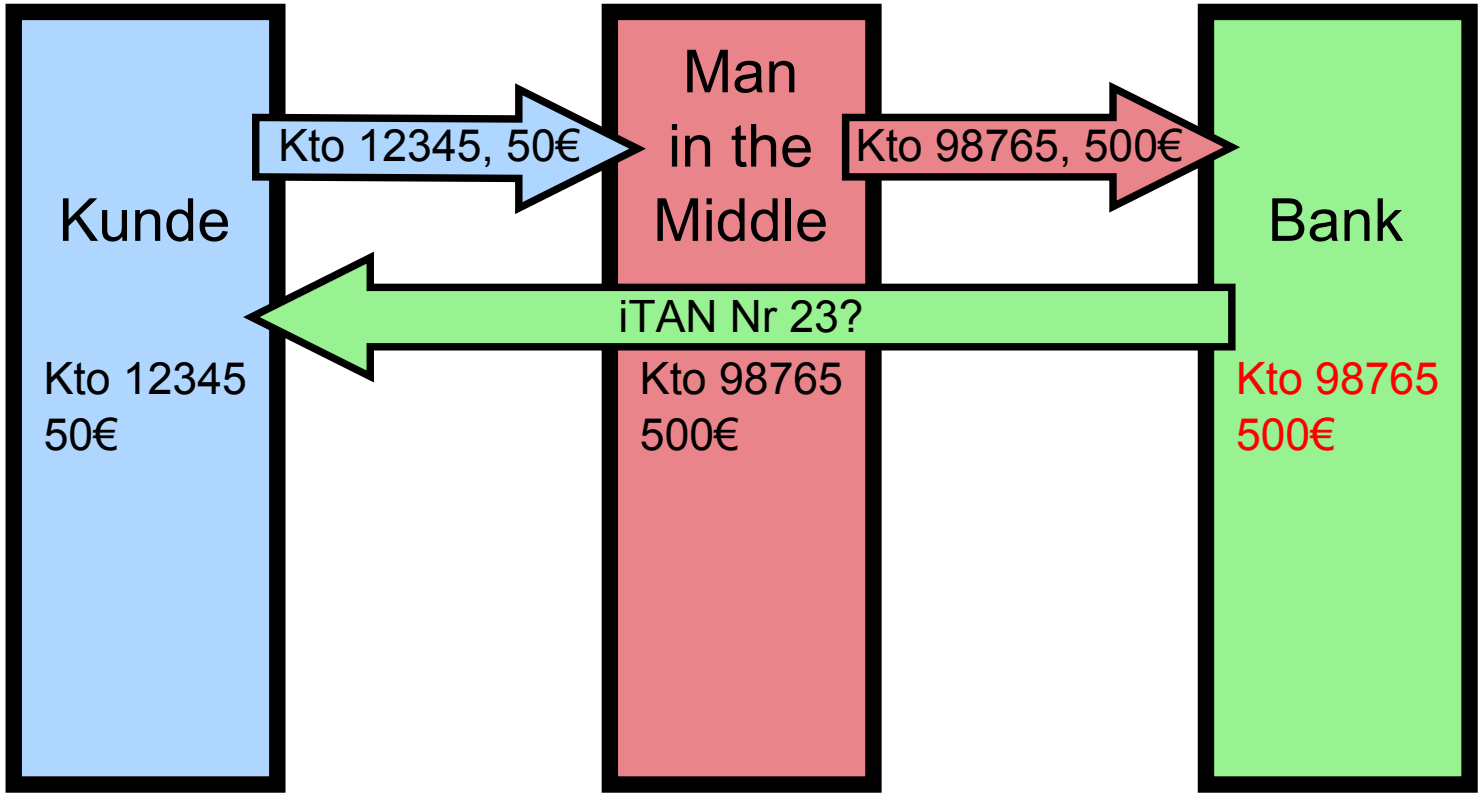
Motivation

Man-in-the-Middle-Angriff



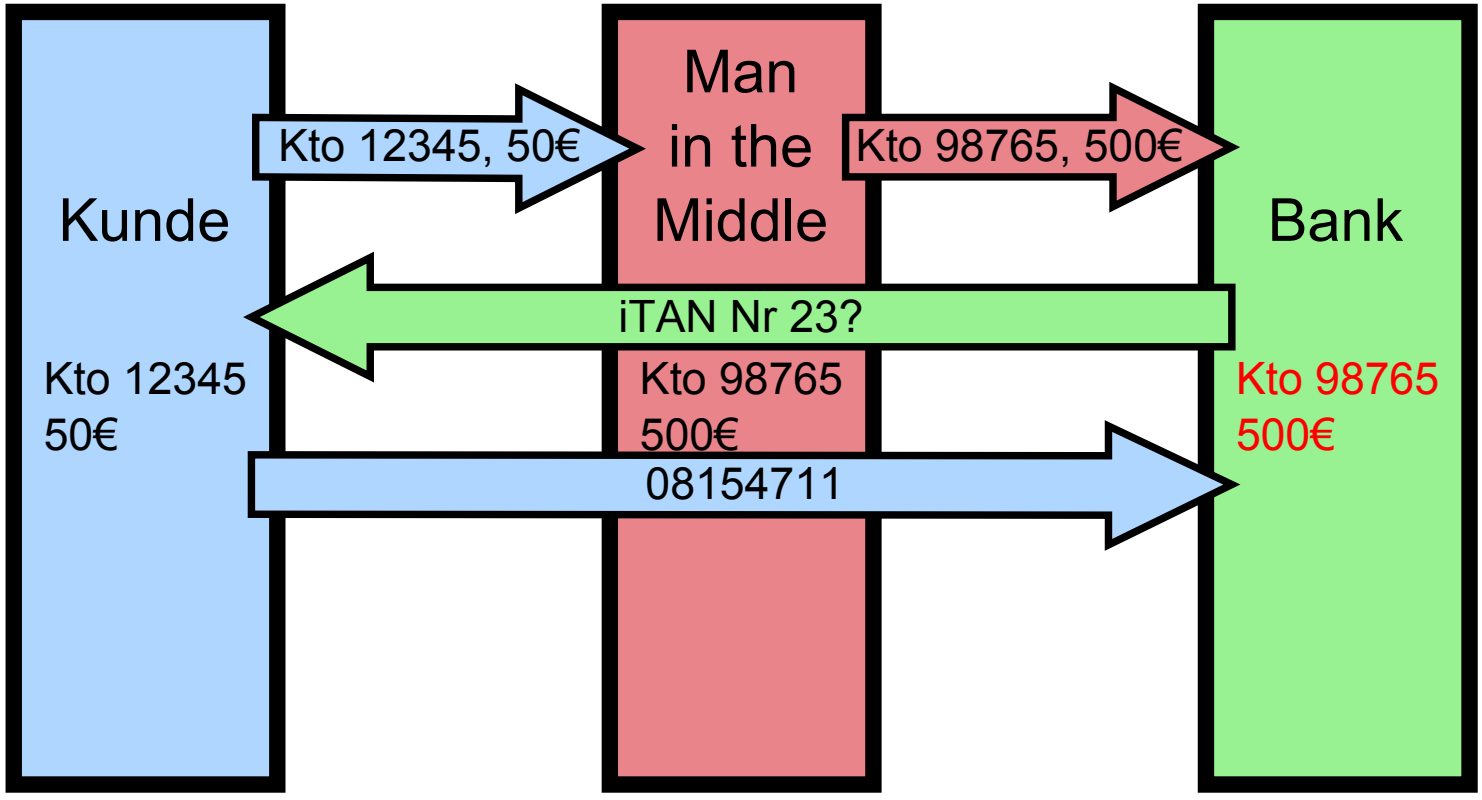
Motivation

Man-in-the-Middle-Angriff



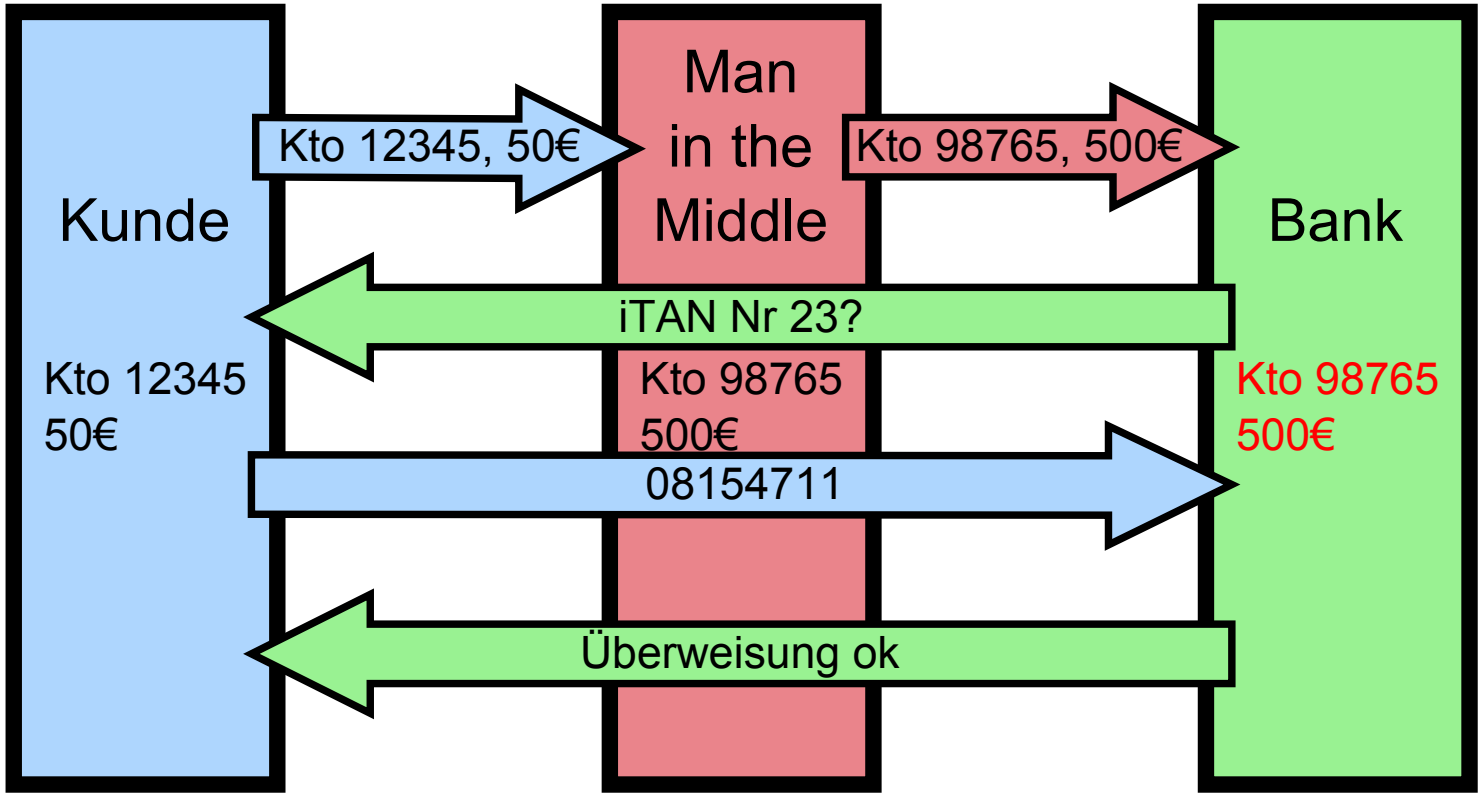
Motivation

Man-in-the-Middle-Angriff



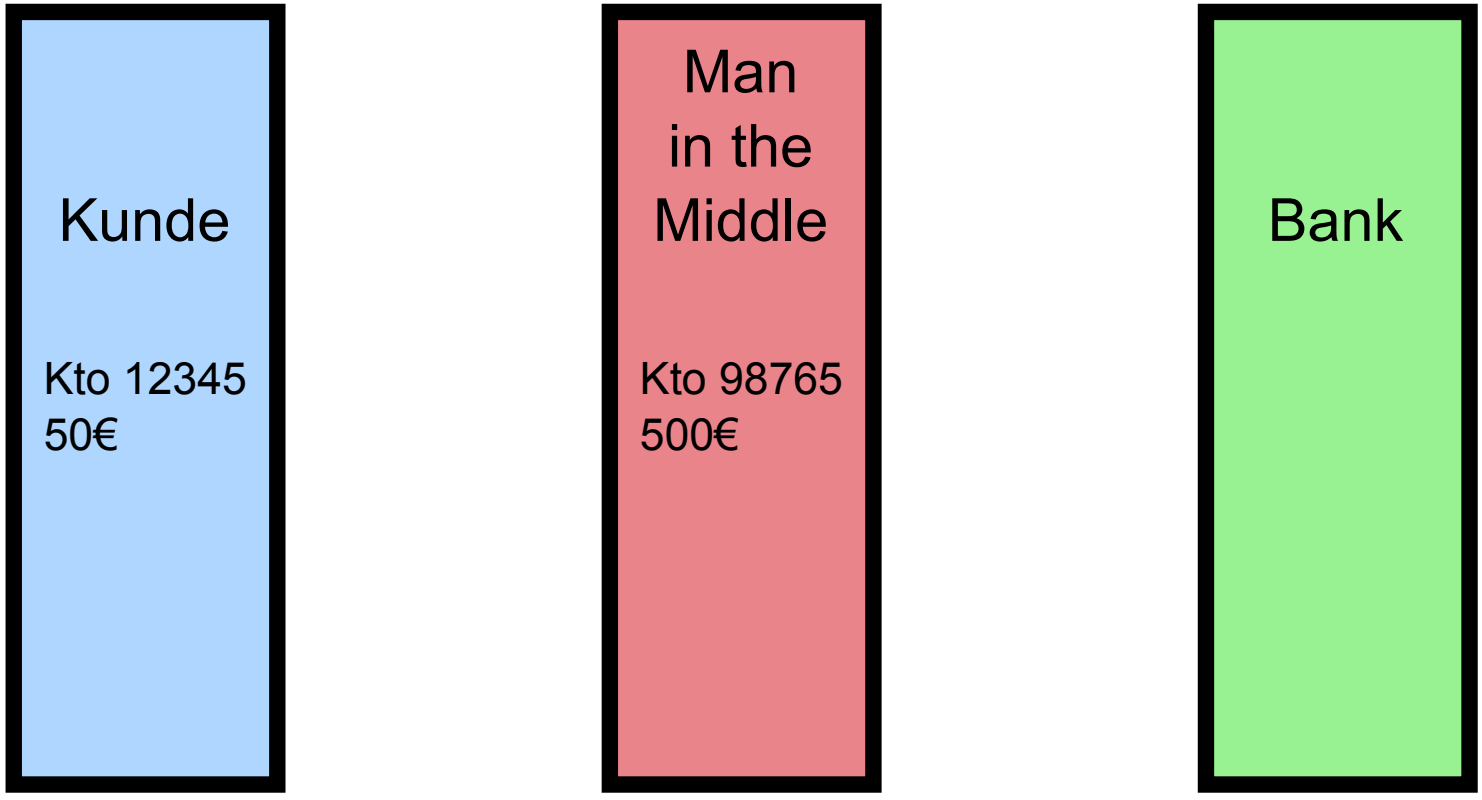
Motivation

Man-in-the-Middle-Angriff



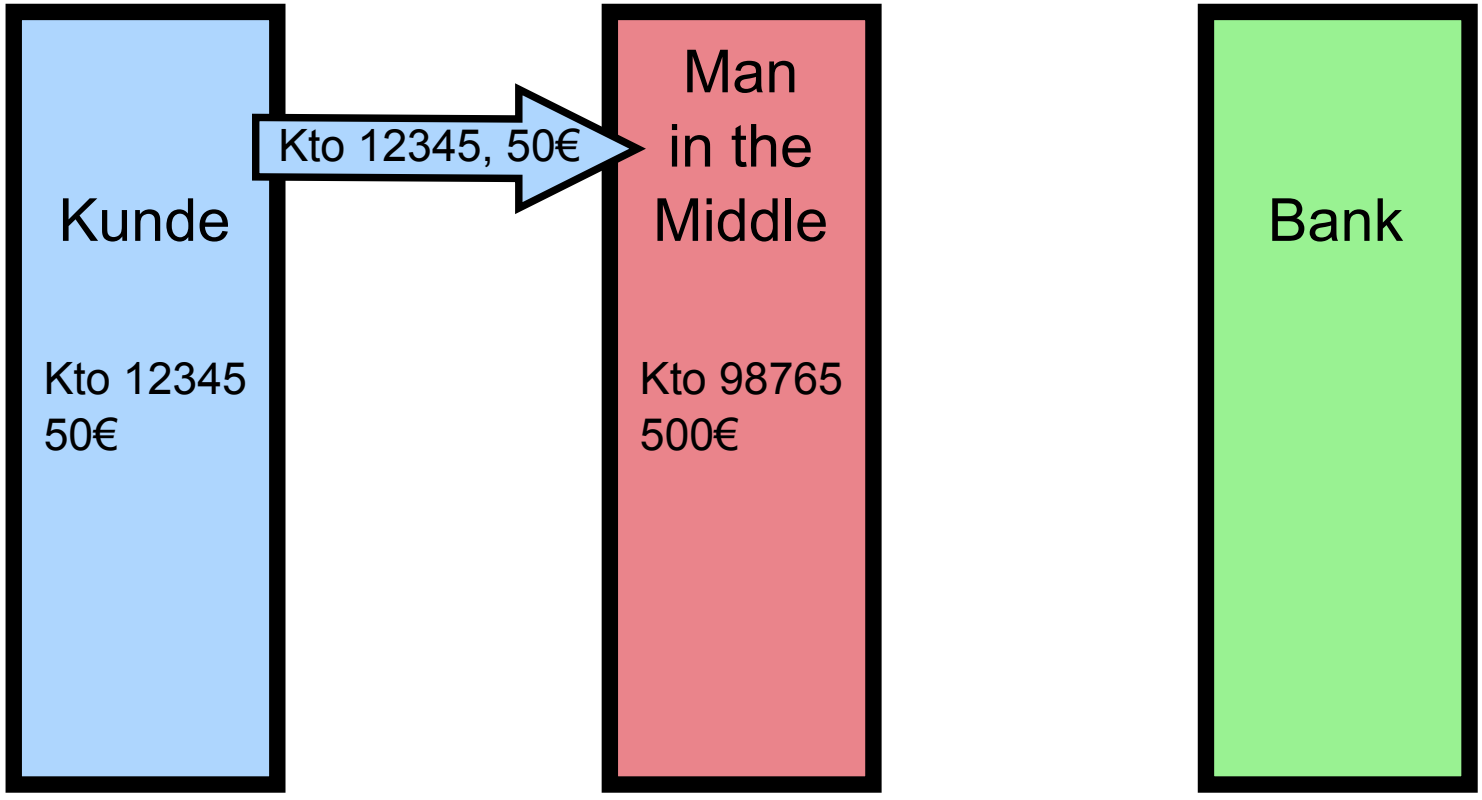
Motivation

Man-in-the-Middle-Angriff



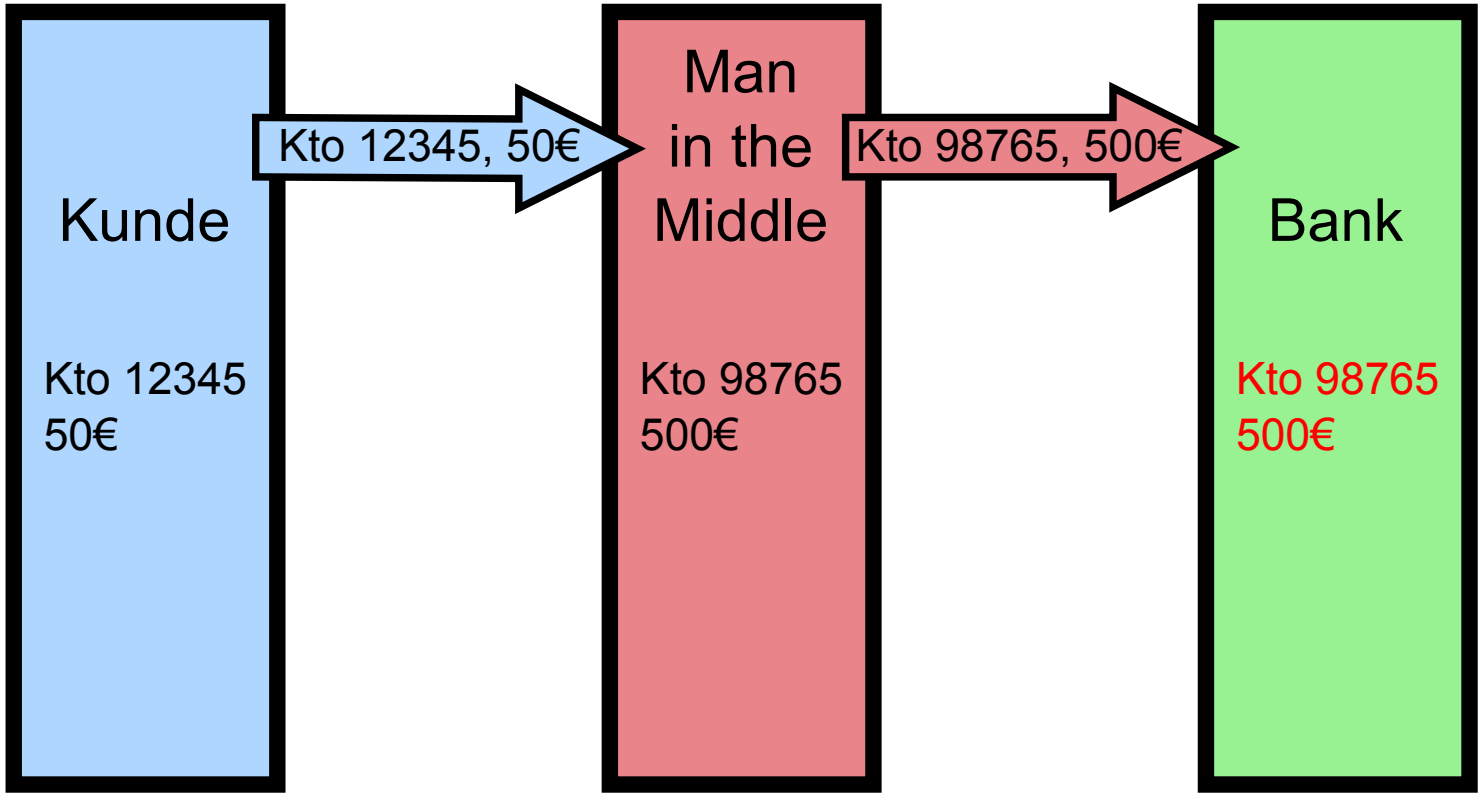
Motivation

Man-in-the-Middle-Angriff



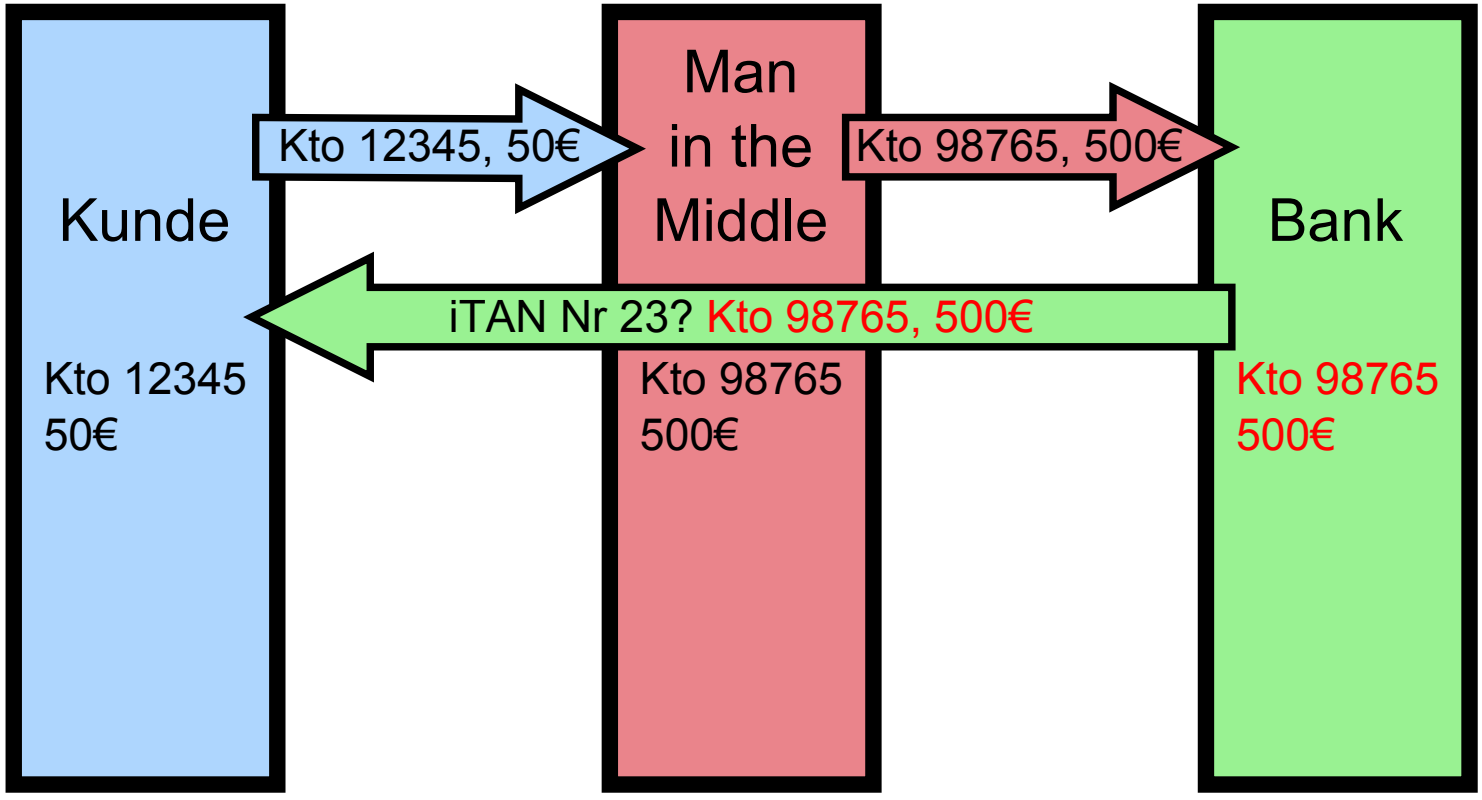
Motivation

Man-in-the-Middle-Angriff



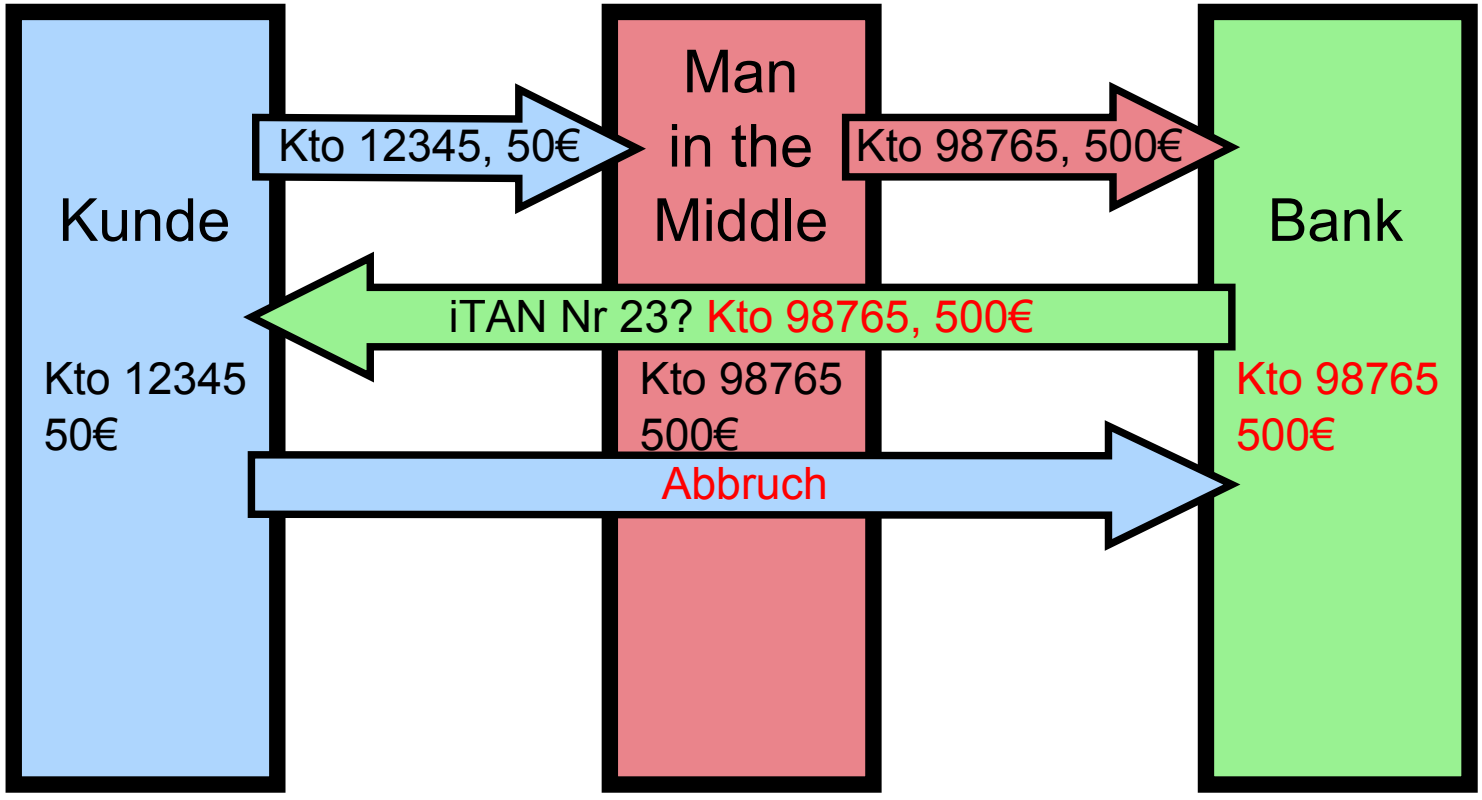
Motivation

Man-in-the-Middle-Angriff



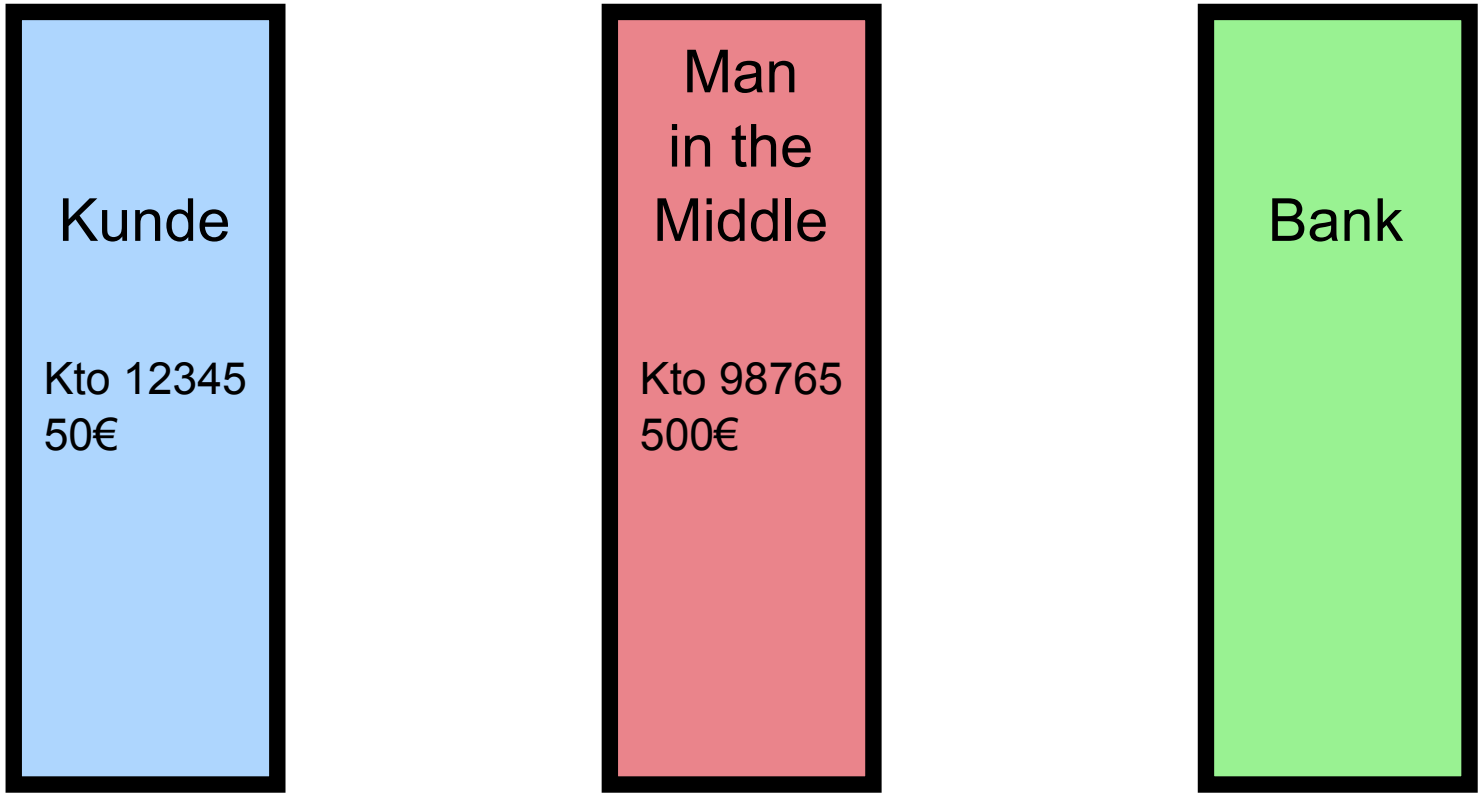
Motivation

Man-in-the-Middle-Angriff



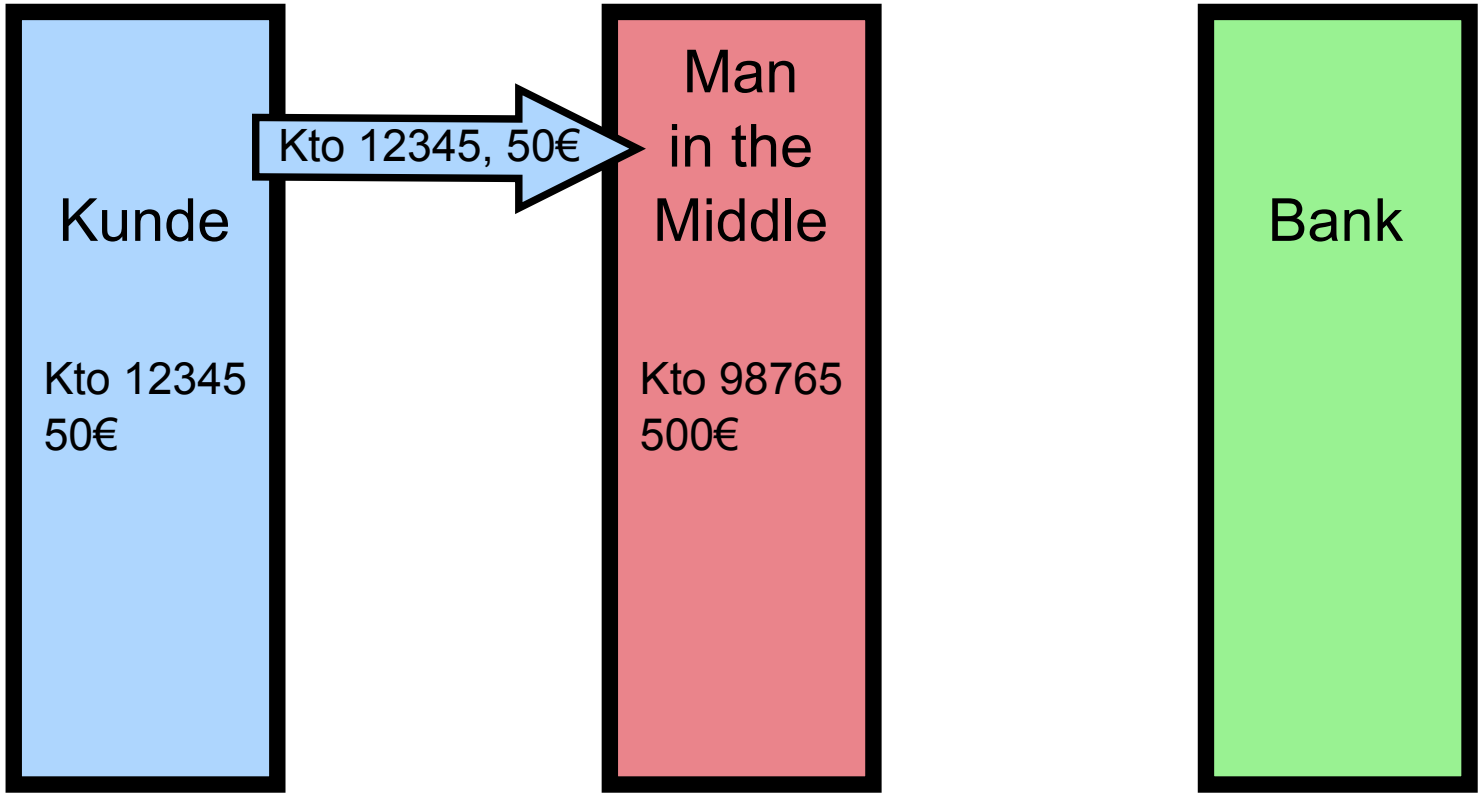
Motivation

Man-in-the-Middle-Angriff



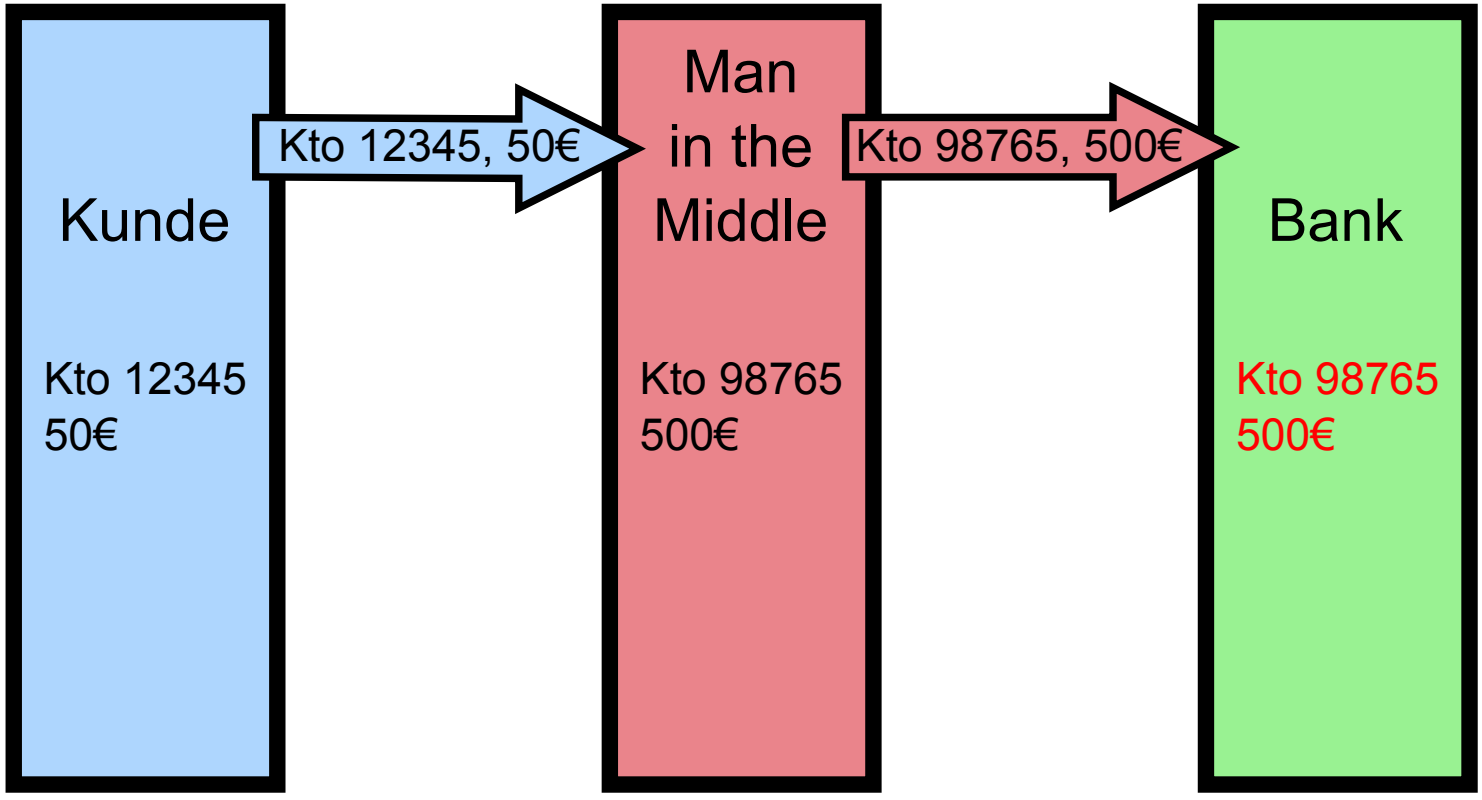
Motivation

Man-in-the-Middle-Angriff



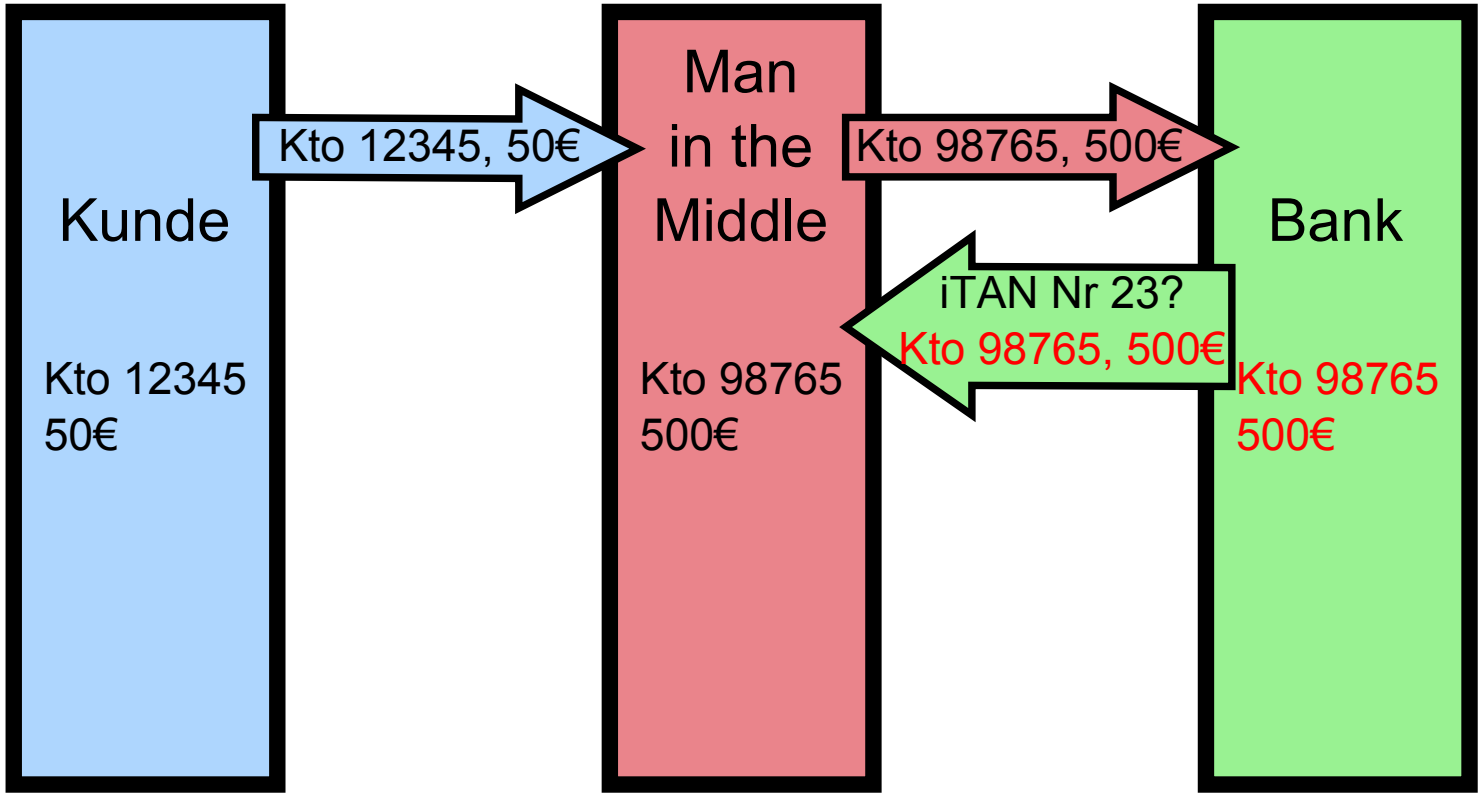
Motivation

Man-in-the-Middle-Angriff



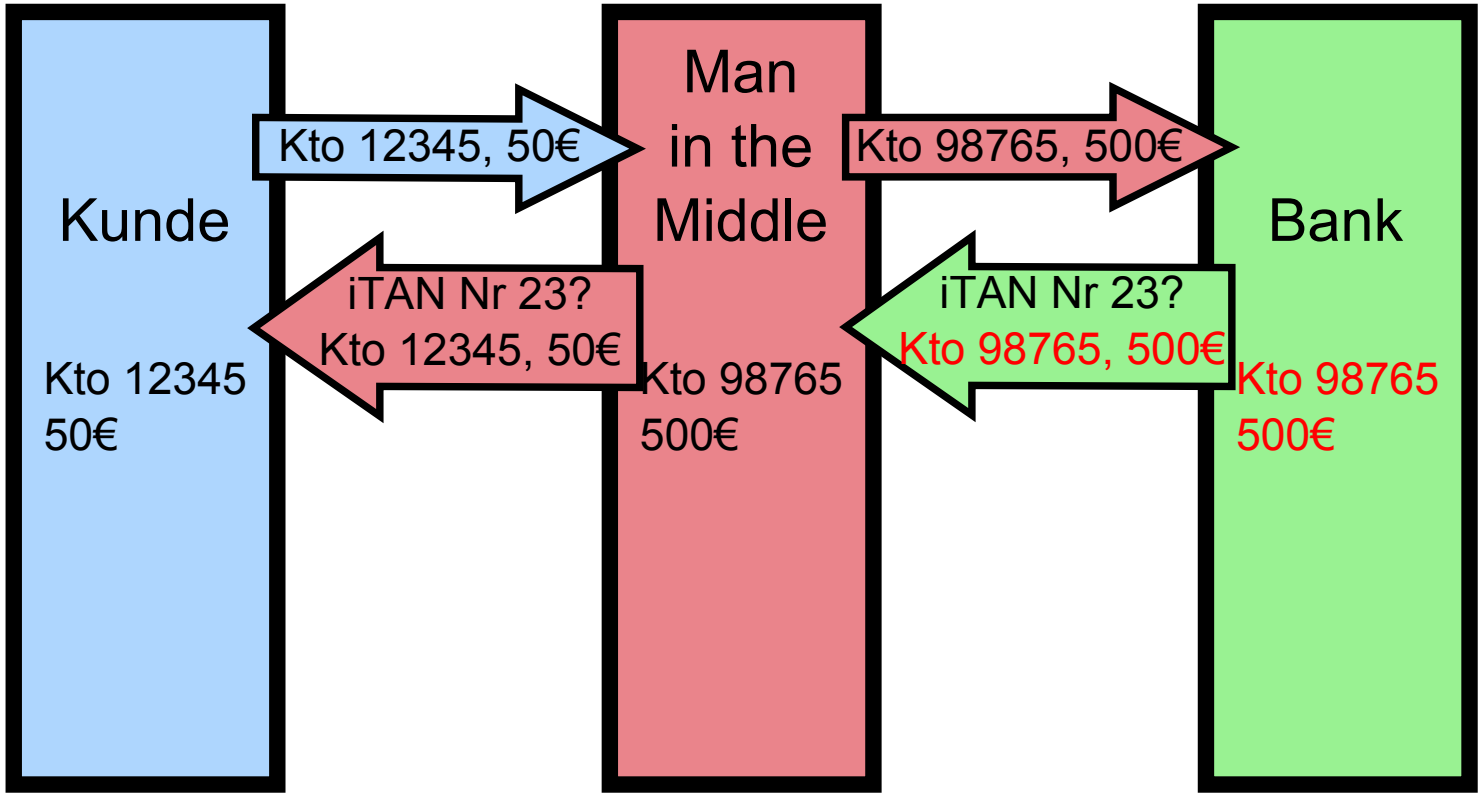
Motivation

Man-in-the-Middle-Angriff



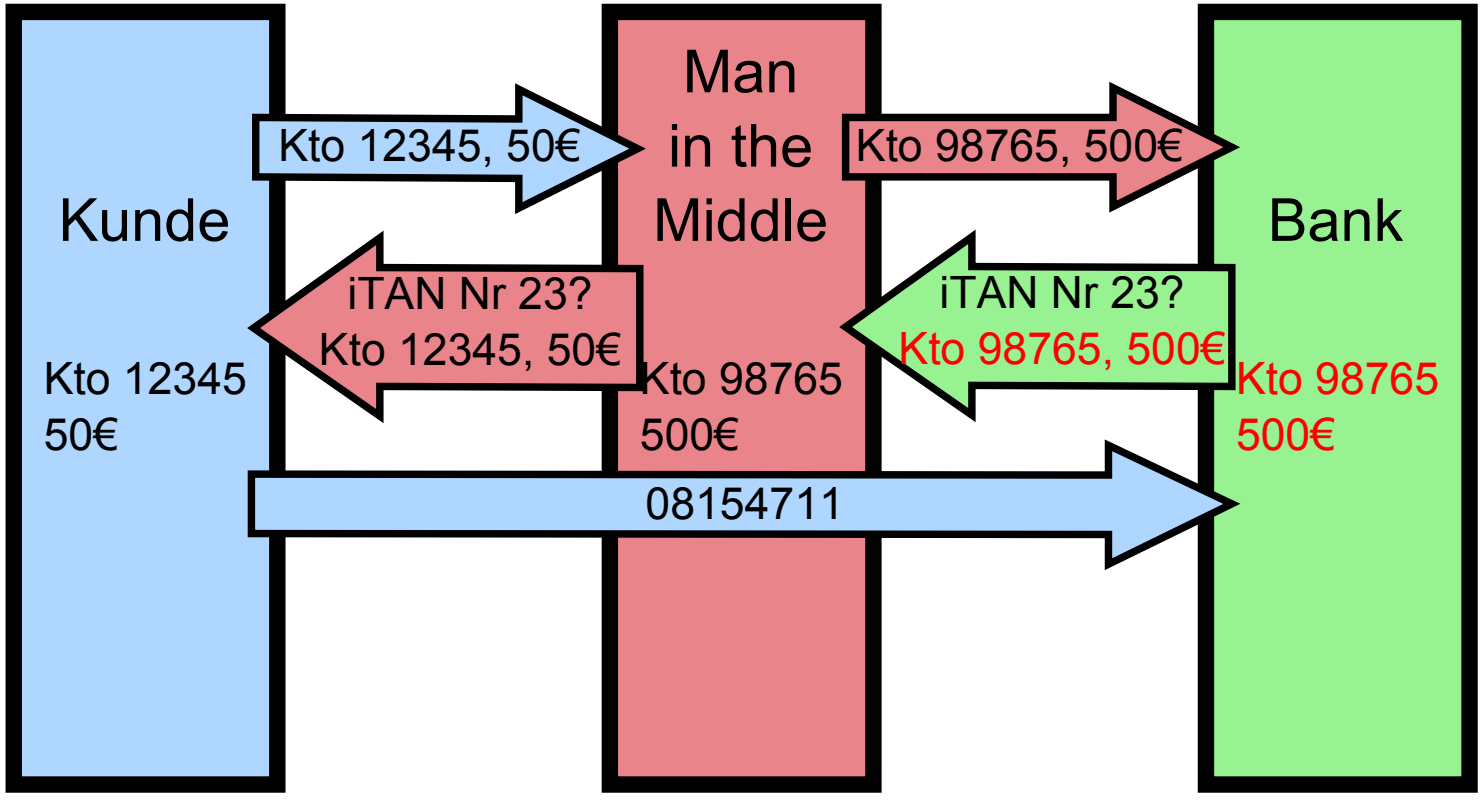
Motivation

Man-in-the-Middle-Angriff



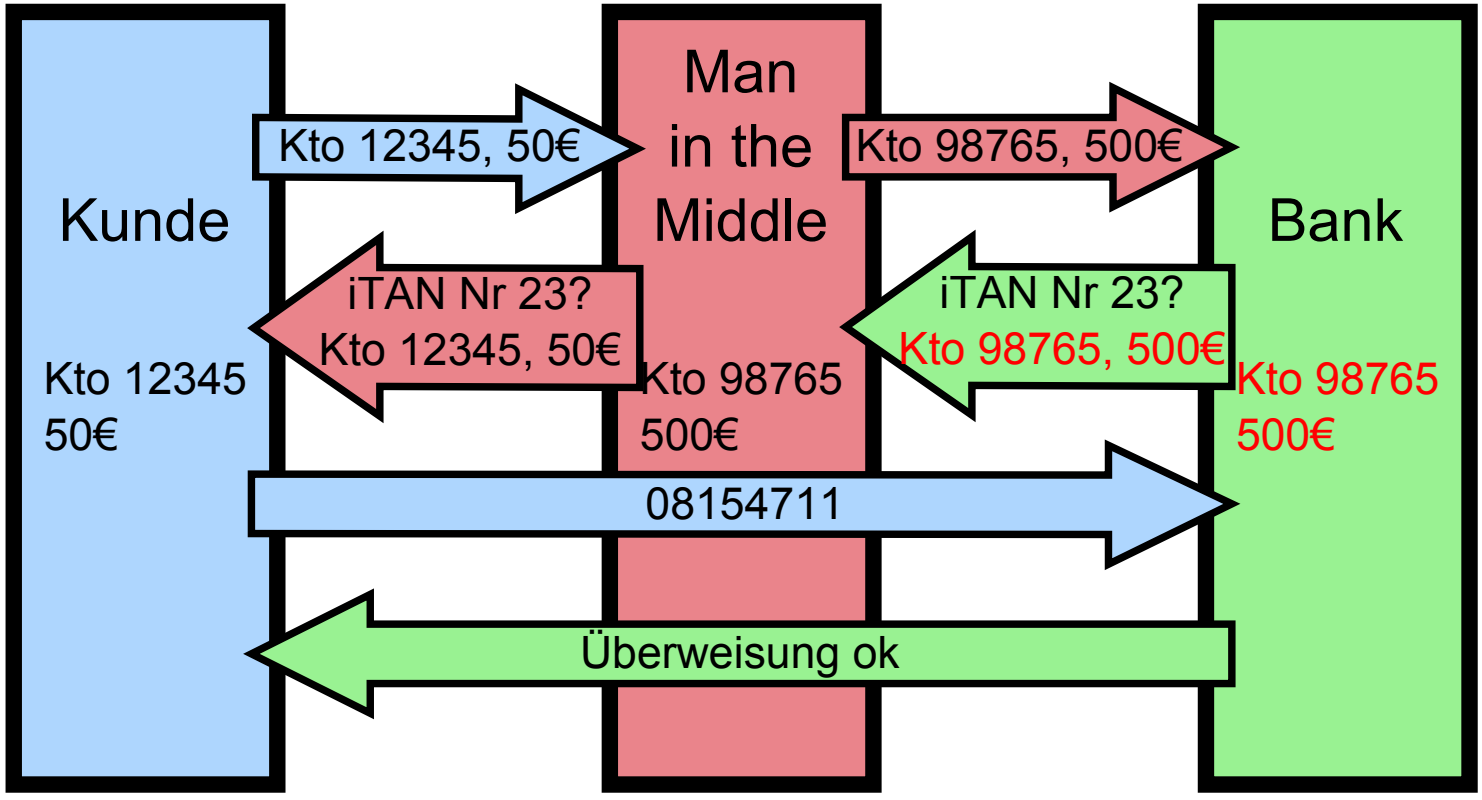
Motivation

Man-in-the-Middle-Angriff



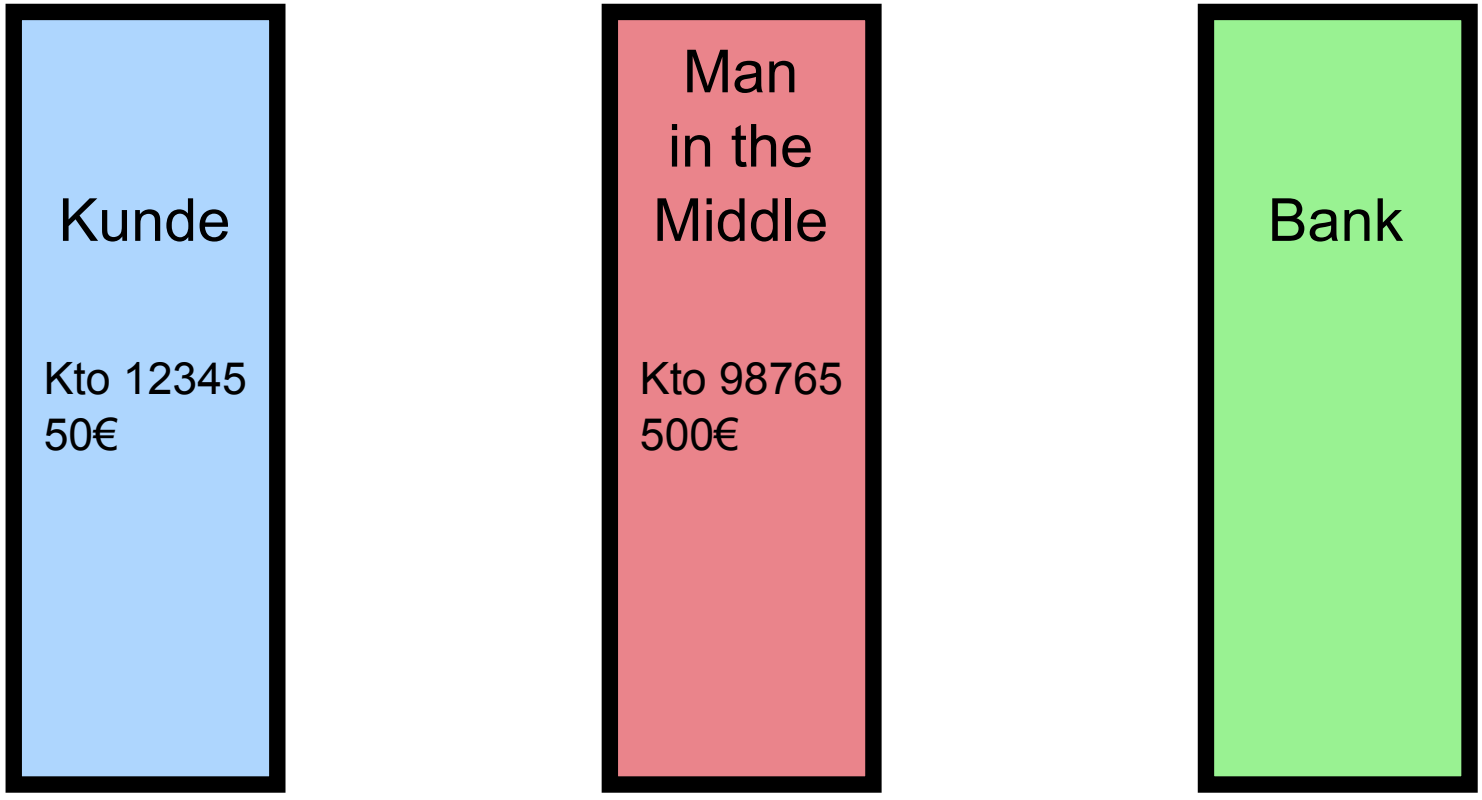
Motivation

Man-in-the-Middle-Angriff



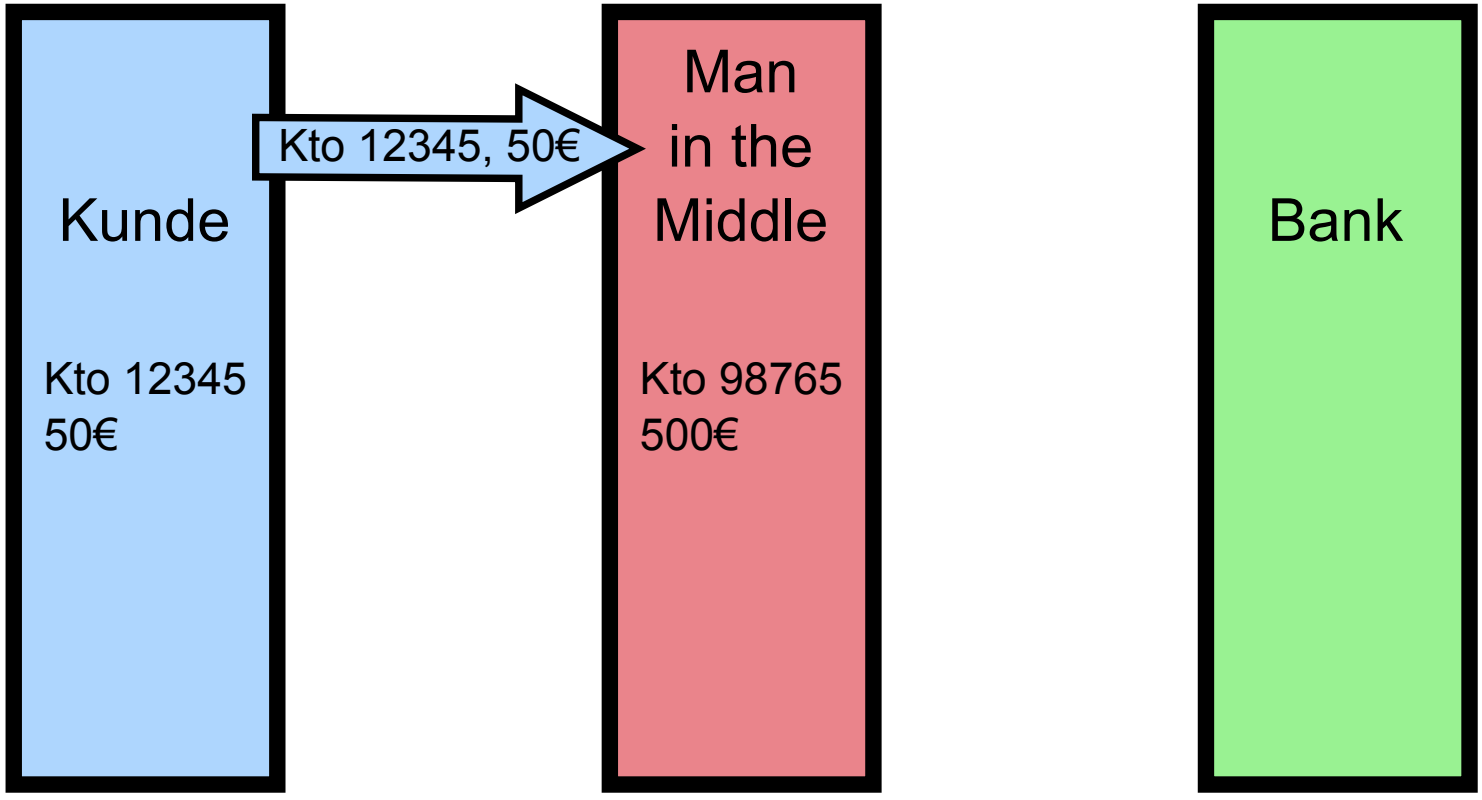
Motivation

Man-in-the-Middle-Angriff



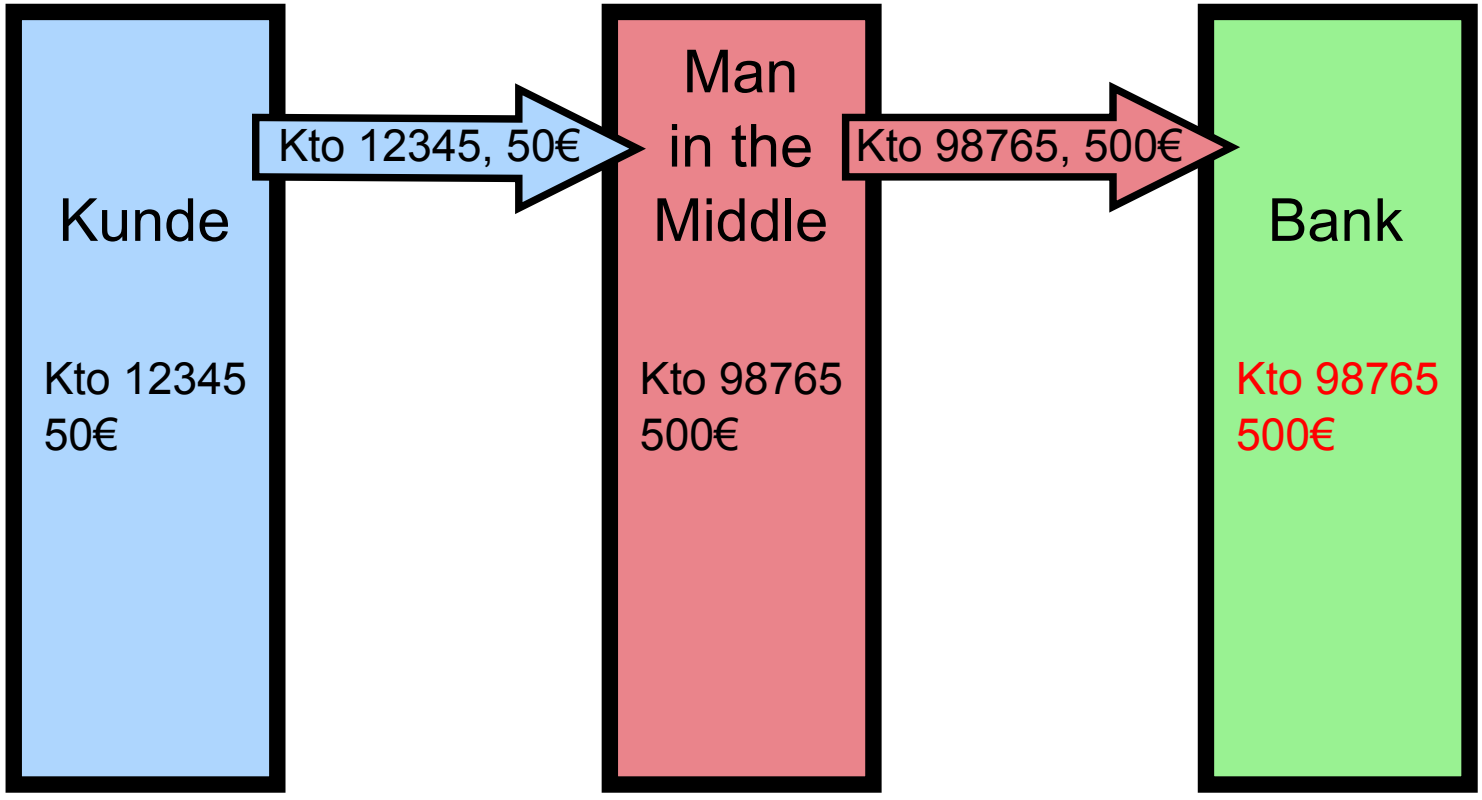
Motivation

Man-in-the-Middle-Angriff



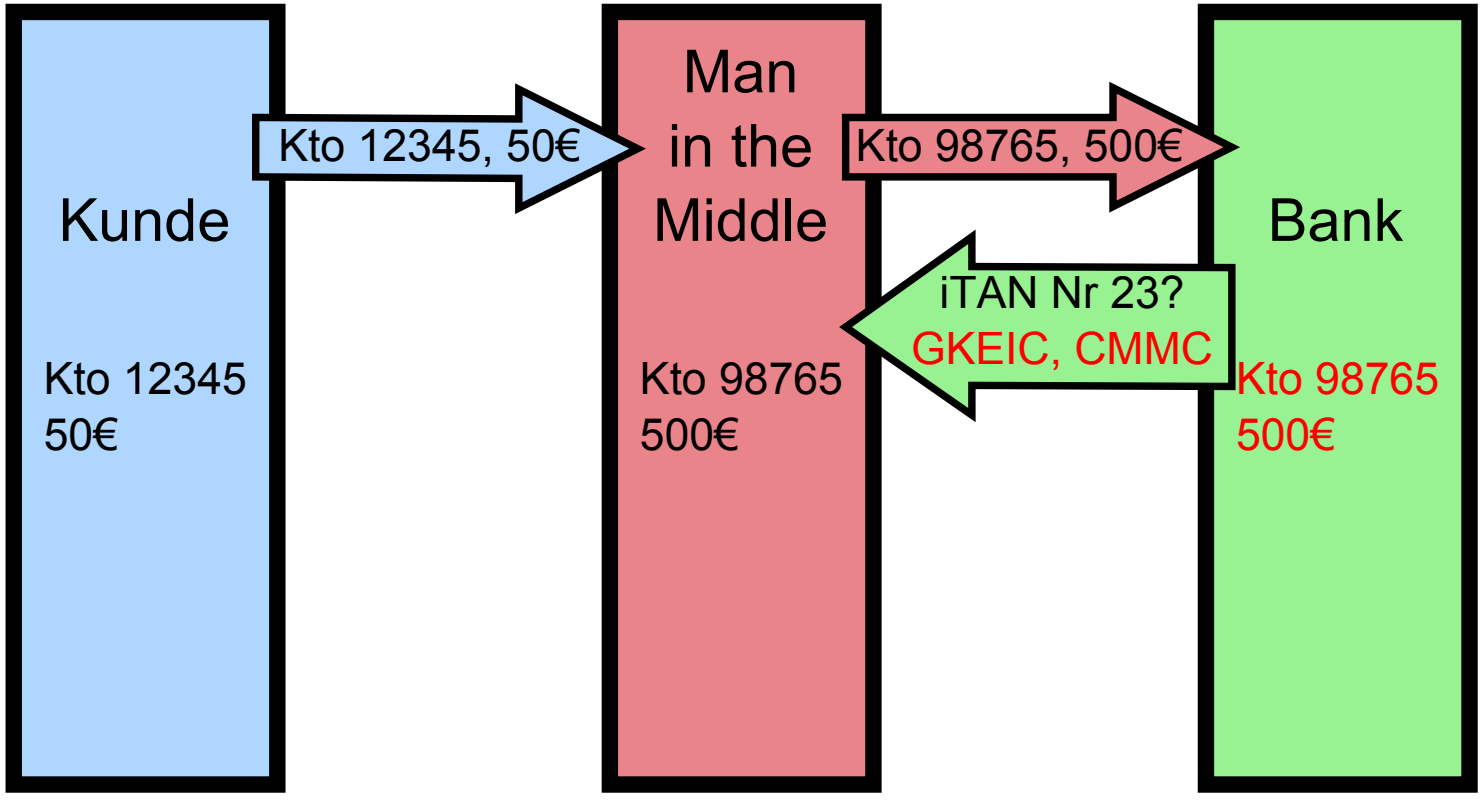
Motivation

Man-in-the-Middle-Angriff



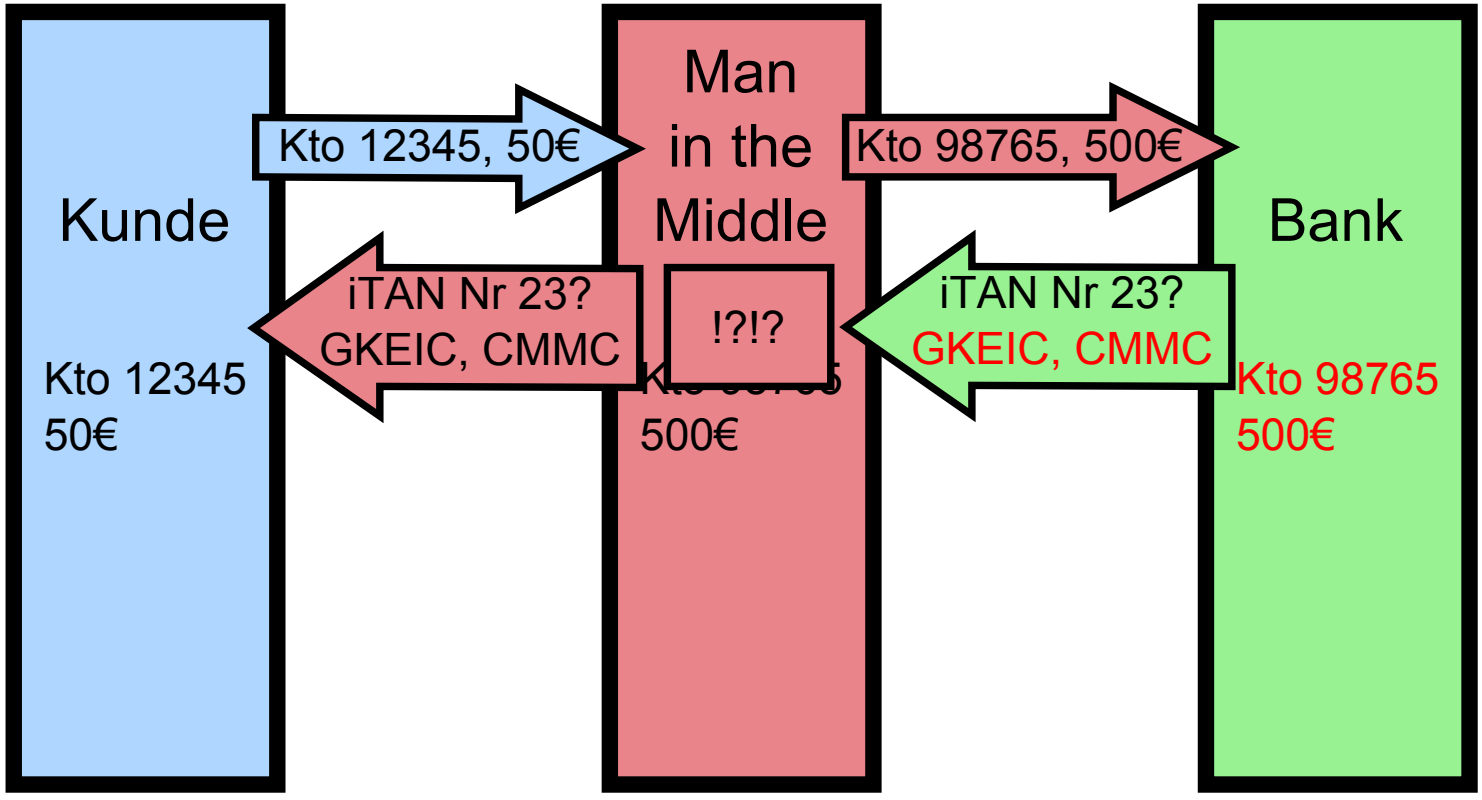
Motivation

Man-in-the-Middle-Angriff



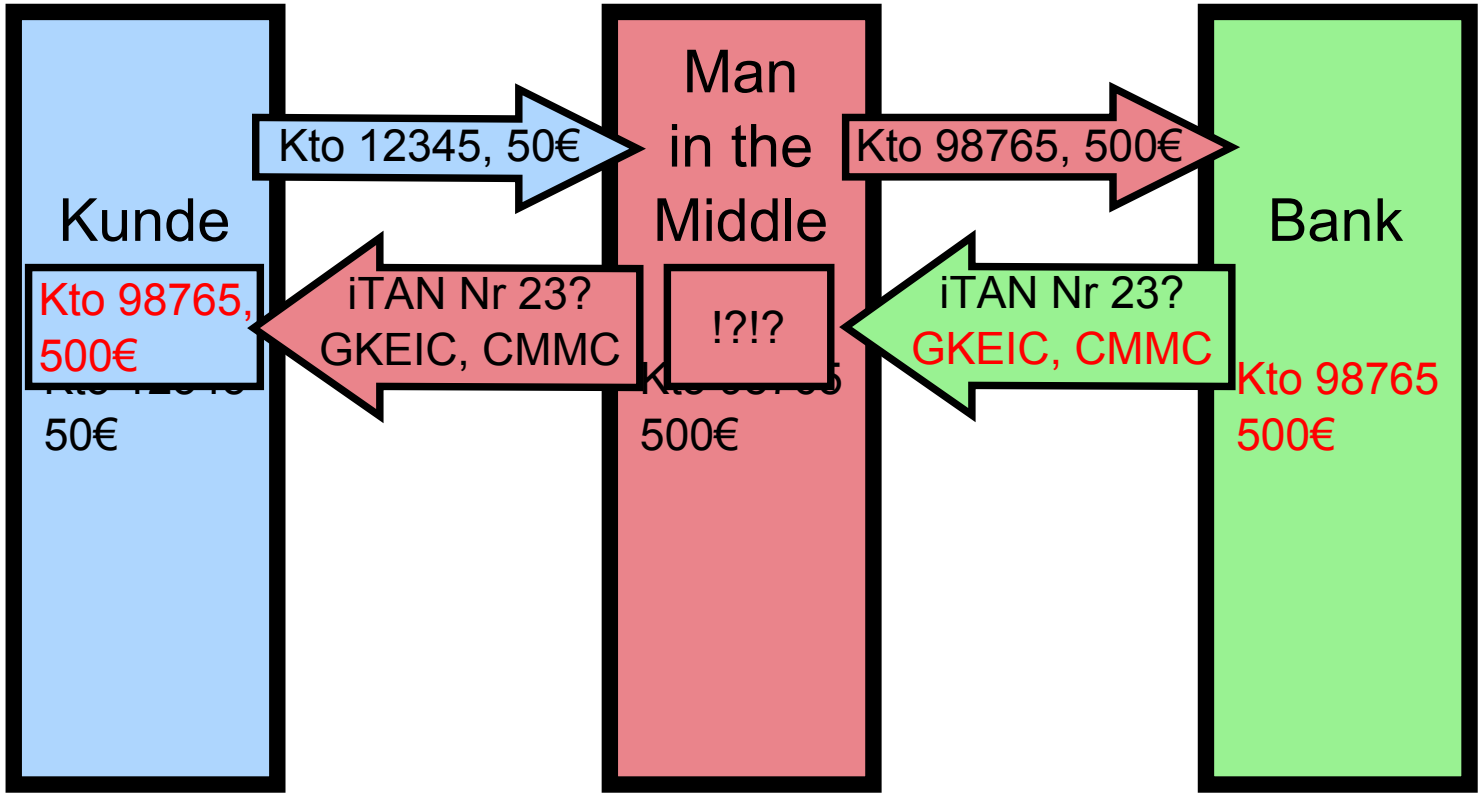
Motivation

Man-in-the-Middle-Angriff



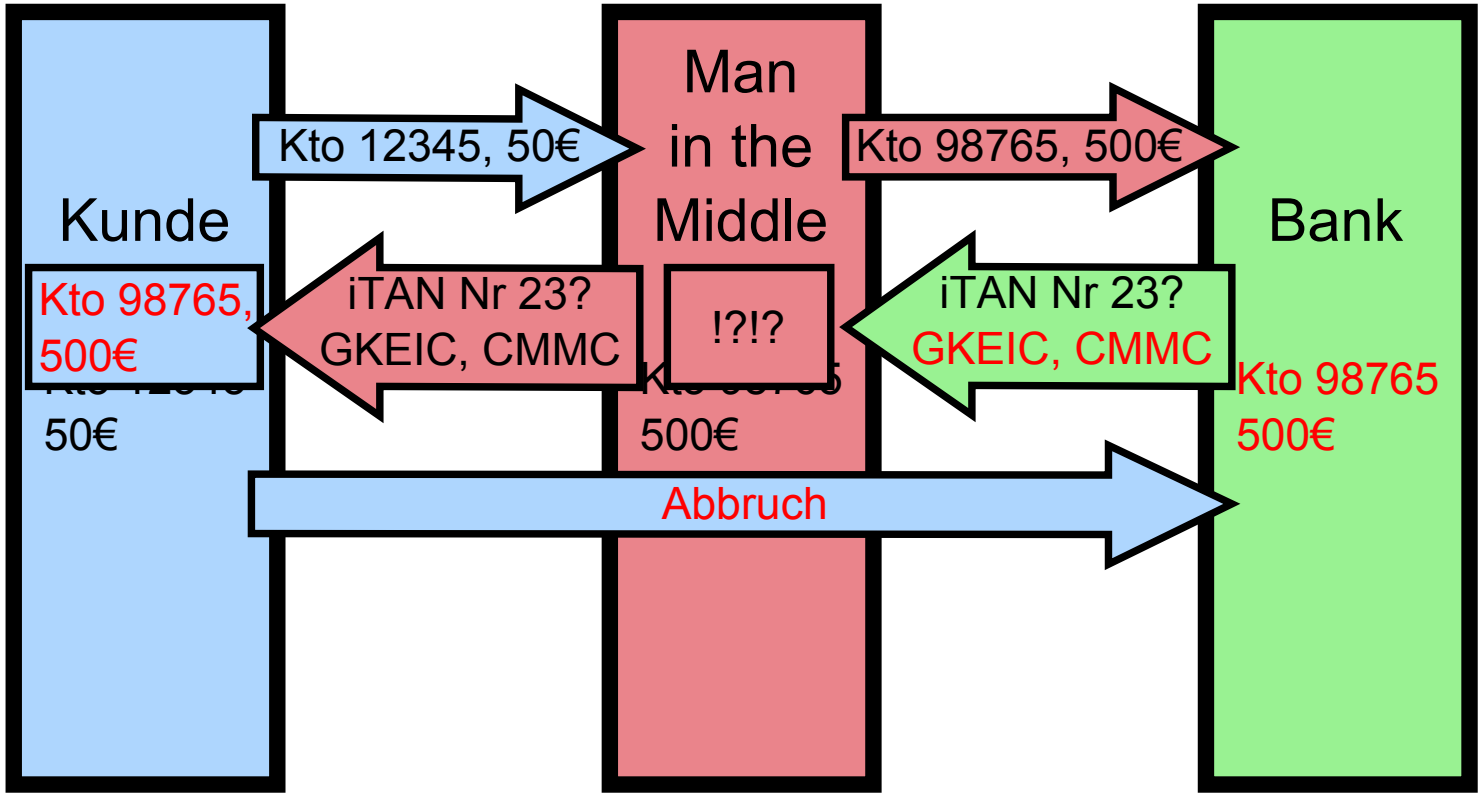
Motivation

Man-in-the-Middle-Angriff



Motivation

Man-in-the-Middle-Angriff

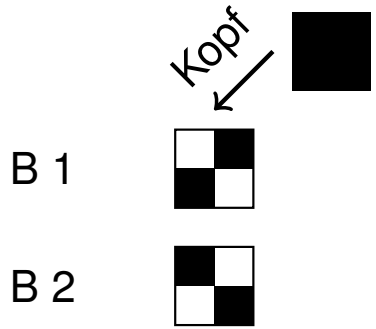


Grundlagen
Visuelle Kryptographie

- Vorgestellt 1994 von Naor und Shamir
- Schwarz-weiß Bild B wird zerlegt in zwei Bilder B1 und B2, dabei wird ein Pixel aus B dargestellt durch 4 Pixel in B1 und B2

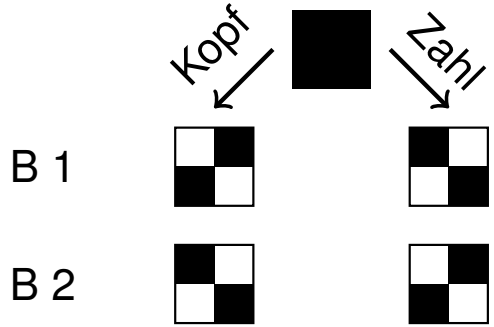
Grundlagen
Visuelle Kryptographie

- Vorgestellt 1994 von Naor und Shamir
- Schwarz-weiß Bild B wird zerlegt in zwei Bilder B1 und B2, dabei wird ein Pixel aus B dargestellt durch 4 Pixel in B1 und B2



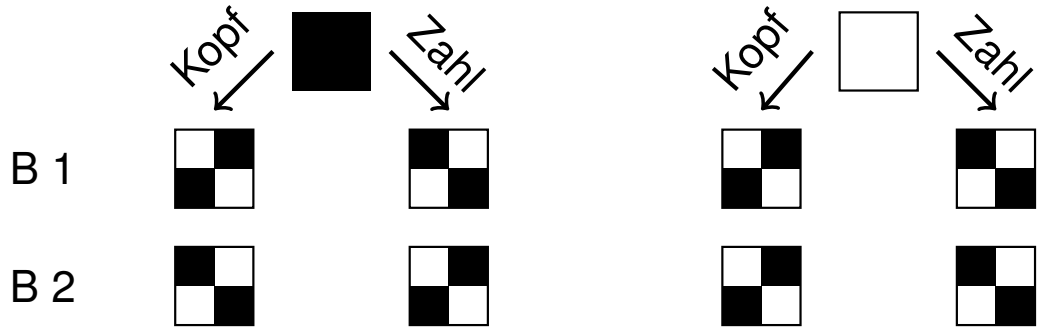
Grundlagen
Visuelle Kryptographie

- Vorgestellt 1994 von Naor und Shamir
- Schwarz-weiß Bild B wird zerlegt in zwei Bilder B1 und B2, dabei wird ein Pixel aus B dargestellt durch 4 Pixel in B1 und B2



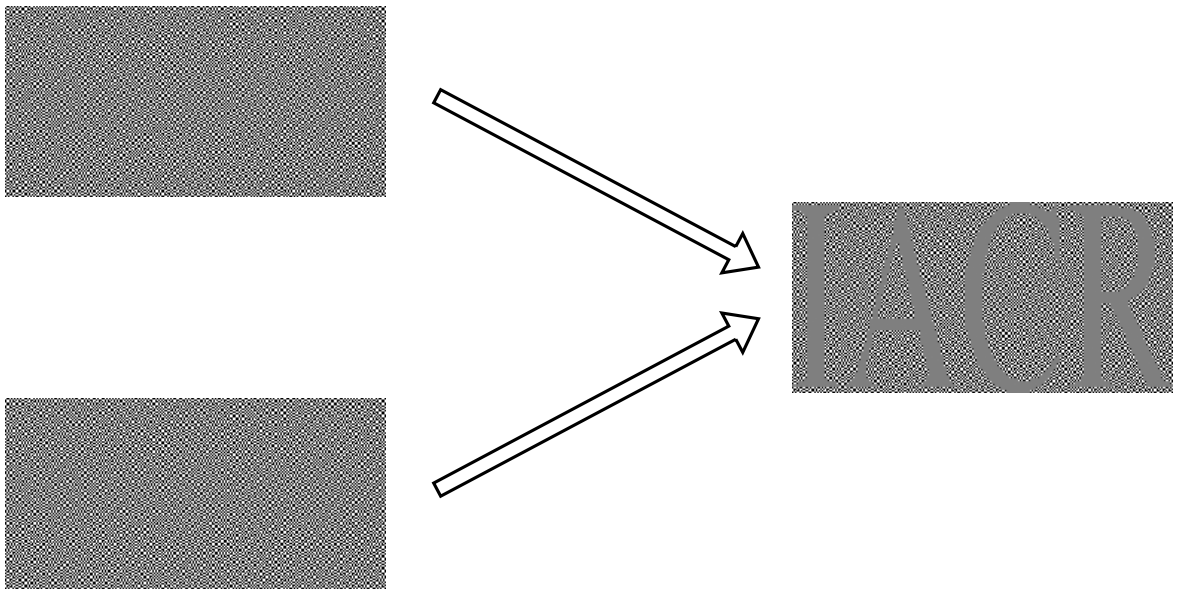
Grundlagen
Visuelle Kryptographie

- Vorgestellt 1994 von Naor und Shamir
- Schwarz-weiß Bild B wird zerlegt in zwei Bilder B1 und B2, dabei wird ein Pixel aus B dargestellt durch 4 Pixel in B1 und B2



Grundlagen
Visuelle Kryptographie

Bei Überlagerung von B1 und B2 entsteht wieder B



Grundlagen
Visuelle Kryptographie

Nachteile der Visuellen Kryptographie:

- B1 und B2 müssen exakt ausgerichtet werden, damit B sichtbar wird
- Kontrastverlust von 50% durch pseudo-weißes Pixel
- Jedes Teilbild B2 nur einmal verwendbar

Grundlagen
Visuelle Kryptographie

Lösungsansätze:

- Größere Strukturen verwenden, zum Beispiel Segmente einer 7-Segment-Anzeige
- Komplementärfarben gegen Kontrastverlust
- Einmalverwendbarkeit bleibt Problem

Grundlagen
Komplementärfarben

Komplementärfarben:

- Mischung aus einer Primär- und einer Sekundärfarbe

Grundlagen
Komplementärfarben

Komplementärfarben:

- Mischung aus einer Primär- und einer Sekundärfarbe
- Primärfarbe?
- Rot, Gelb, Blau

Grundlagen
Komplementärfarben

Komplementärfarben:

- Mischung aus einer Primär- und einer Sekundärfarbe
- Primärfarbe?
- Rot, Gelb, Blau
- Sekundärfarbe?
- Mischung aus je zwei Primärfarben
  Orange (= Rot + Gelb), Lila (= Rot + Blau), Grün (= Gelb + Blau)

Grundlagen
Komplementärfarben

Komplementärfarben

- ergeben in der Mischung schwarz
- zeichnen sich aus durch hohen Kontrast zueinander

Grundlagen
Komplementärfarben

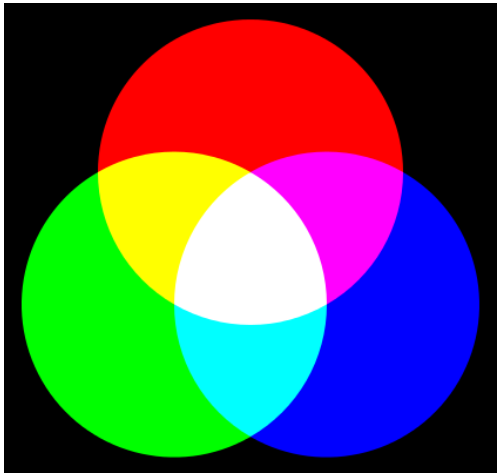
Komplementärfarben sind abhängig vom gewählten Farbmodell

Farbkreis nach Itten
Primärfarben Rot, Gelb, Blau

Grundlagen
Komplementärfarben

Komplementärfarben sind abhängig vom gewählten Farbmodell

Additive Farbmischung, RGB-Modell
Primärfarben Rot, Grün, Blau



Grundlagen
Komplementärfarben

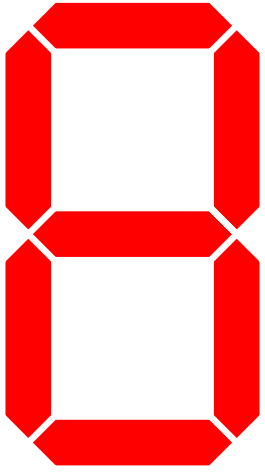
Komplementärfarben sind abhängig vom gewählten Farbmodell

Subtraktive Farbmischung, CMY-Modell
Primärfarben Cyan, Magenta, Gelb (Yellow)

Grundlagen
Segment-Anzeige

Segmentanzeigen:

- erfunden 1908 von F. W. Wood
- einzelne Segmente werden erleuchtet oder bleiben dunkel
- Am weitesten verbreitet ist die 7-Segment-Anzeige.
- Darstellung von Ziffern und wenigen Buchstaben, wenige Sonderzeichen



Grundlagen
14- und 16-Segment-Anzeigen

- Außerdem 14-Segment-, 16-Segment-Anzeige

- Höherer Zeichenvorrat, bessere Lesbarkeit
- In dieser Arbeit nicht benutzt, da komplexere Darstellung

Grundlagen
Visuelle Kryptographie mit Komplementärfarben

Visuelle Kryptographie mit Komplementärfarben

Grundlagen
Visuelle Kryptographie mit Komplementärfarben

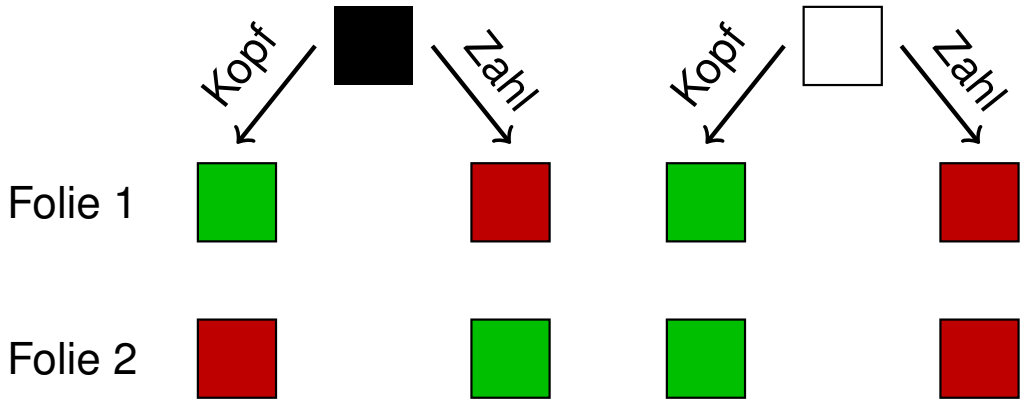
Visuelle Kryptographie mit Komplementärfarben

Keine Unterteilung eines Pixel in Subpixel mehr

Grundlagen
Visuelle Kryptographie mit Komplementärfarben

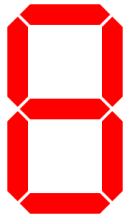
Visuelle Kryptographie mit Komplementärfarben

Keine Unterteilung eines Pixel in Subpixel mehr



Segmentbasierte Visuelle Kryptographie mit Komplementärfarben

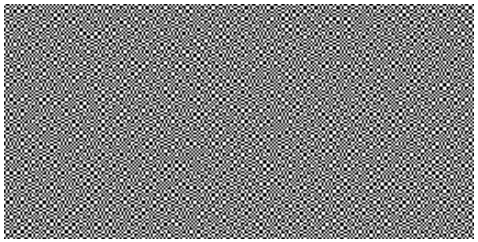
- Segmentbasierte ...



Segmentbasierte Visuelle Kryptographie mit Komplementärfarben

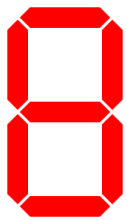
- Segmentbasierte . . .

- . . . Visuelle Kryptographie

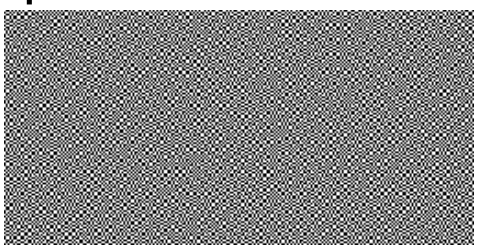


Segmentbasierte Visuelle Kryptographie mit Komplementärfarben

- Segmentbasierte . . .

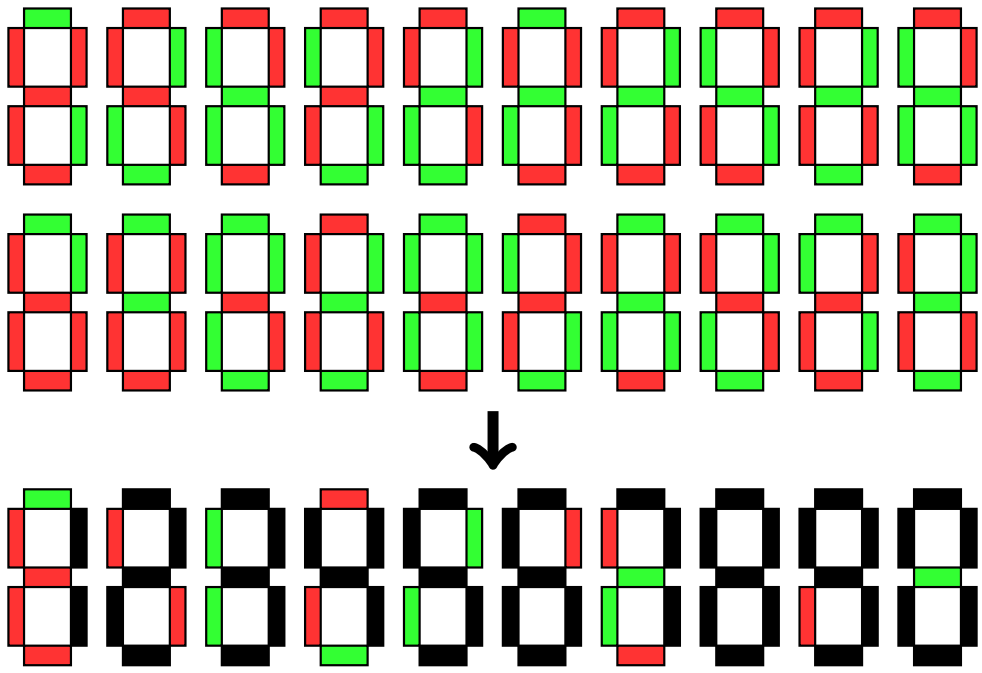


- . . . Visuelle Kryptographie

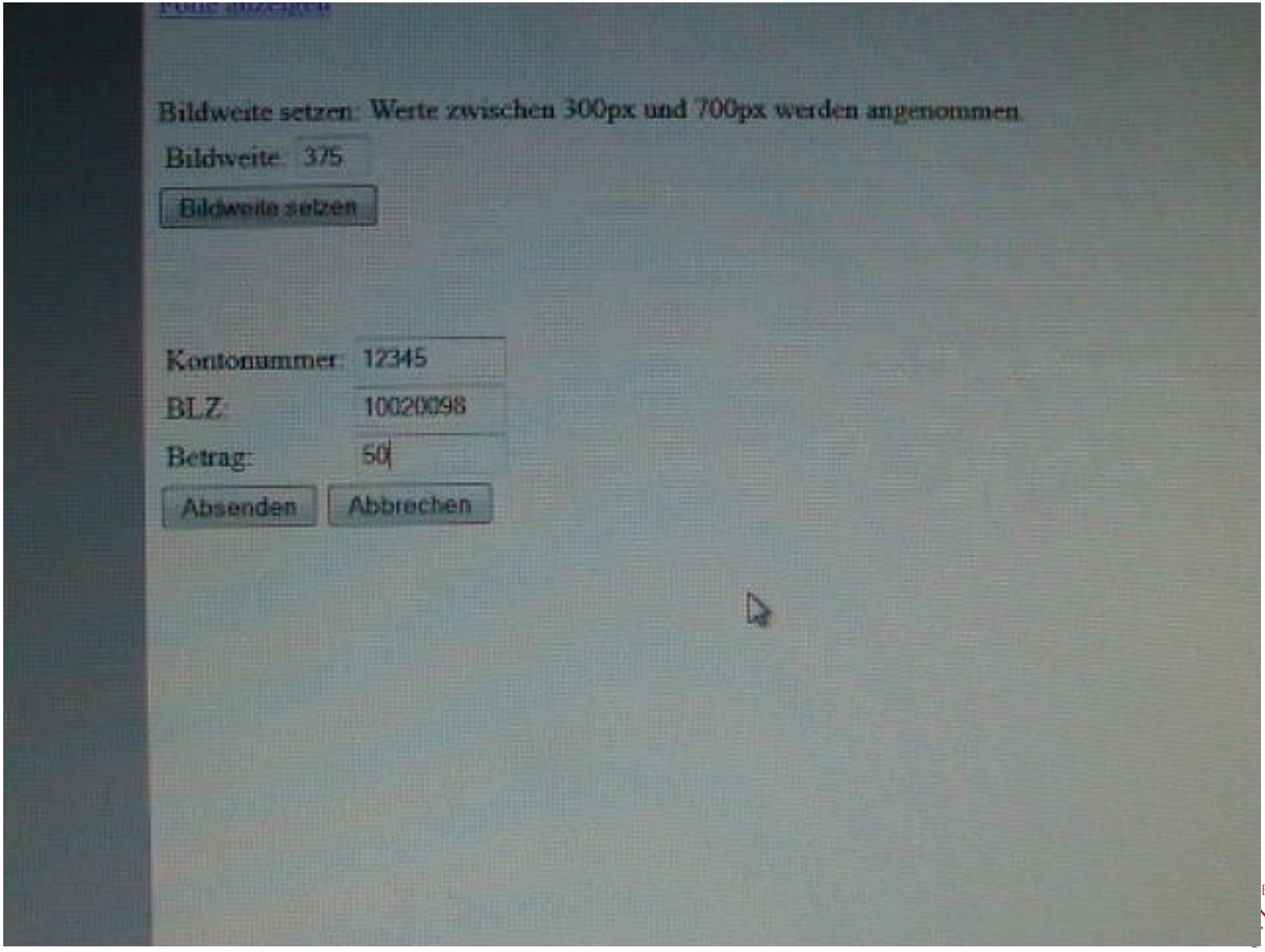


- . . . mit Komplementärfarben

Segmentbasierte Visuelle Kryptographie mit Komplementärfarben



Demonstration einer Online-Implementierung



Zusammenfassung

Segmentbasierte Visuelle Kryptographie mit Komplementärfarben

- bietet erhöhte Lesbarkeit durch größere Strukturen und geringeren Kontrasverlust
- Kein zusätzliches Gerät benötigt, um Sicherheit herzustellen
- Alle Daten in Kommunikation zwischen Bank und Kunde verschlüsselt

- Ausblick
  - Rot-Grün-Blindheit?
  - Fehlende Wiederverwendbarkeit der Folien?