ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Algorithmen für drahtlose Netzwerke

Public-Key-Kryptografie und Byzantinische Generäle

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer

Asymmetrische Verschlüsselungsmethoden

- **z.B. RSA, Ronald Rivest, Adi Shamir, Lenard Adleman, 1977**
  - Diffie-Hellman, PGP
- **Geheimer Schlüssel privat**
  - kennt nur der Empfänger der Nachricht
- **Öffentlichen Schlüssel offen**
  - Ist allen Teilnehmern bekannt
- **Wird erzeugt durch Funktion**
  - keygen(privat) = offen
- **Verschlüsselungsfunktion f und Entschlüsselungsfunktion g**
  - sind auch allen bekannt
- **Verschlüsselung**
  - f(offen,text) = code
  - kann jeder berechnen
- **Entschlüsselung**
  - g(privat,code) = code
  - nur vom Empfänger

Beispiel: RSA

- **R. Rivest, A. Shamir, L. Adleman**
  - On Digital Signatures and Public Key Cryptosystems, Communication of the ACM
- **Verfahren beruht auf der Schwierigkeit der Primfaktorzerlegung**
- **1. Beispiel:**
  - 15 = ? * ?
  - 15 = 3 * 5
- **2. Beispiel:**
  - 3865818645841127319129567277348359557444790410289933586483552047443 = 12345678901234567890123456789002093131313131313131313131313131300227

- **Bis heute ist kein effizientes Verfahren zur Primfaktorzerlegung bekannt**
  - Aber das Produkt von Primzahlen kann effizient bestimmt werden
  - Primzahlen können effizient bestimmt werden
  - Primzahlen sehr häufig

RSA

- **Erzeugung der Schlüssel**
  - Wähle zufällig zwei Primzahlen p und q mit k bits (k ≥ 500).
  - n = p·q
  - e ist Zahl, die teilerfremd ist mit (p - 1)·(q - 1).
  - d = e-1 mod (p - 1)(q - 1)
    - es gilt $d \cdot e \equiv 1 \bmod (p-1)(q-1)$
- **Public Key P = (e, n)**
- **Secret Key S = (d, n)**

- **Kodierung**
  - Teile Nachricht in Blöcke der Größe 2k auf
  - Interpretiere Block M als Zahl $0 \leq M < 2^{2k}$
  - Chiffre: $P(M) = M^e \bmod n$
- **Dekodierung**
  - $S(C) = C^d \bmod n$
- **Korrektheit gilt nach dem kleinen Satz von Fermat**

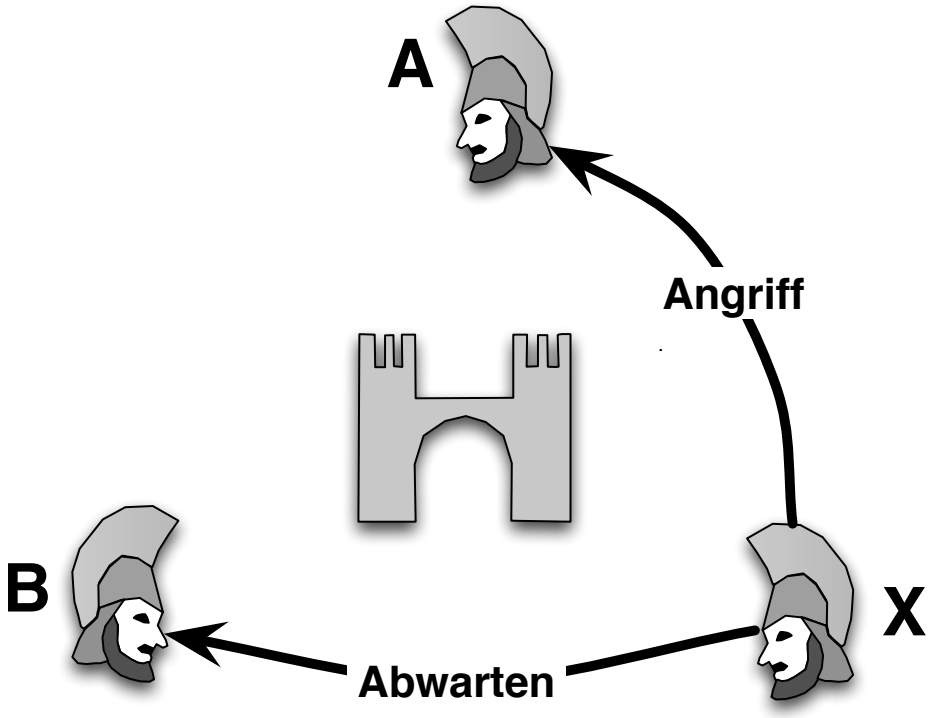
Elektronische Unterschriften

- **Digitale Signaturen**
  - Unterzeichner besitzt einen geheimen Schlüssel
  - Dokument wird mit geheimen Schlüssel unterschrieben
  - und kann mit einem öffentlichen Schlüssel verifiziert werden
  - Öffentlicher Schlüssel ist allen bekannt

- **Beispiel eines Signaturschemas**
  - m: Nachricht
  - Unterzeichner
    - berechnet h(text) mit kryptographischer Hashfunktion
    - und veröffentlicht m und signatur = g(privat, h(text)), für die Entschlüsselungsfunktion g
  - Kontrolleur
    - berechnet h(text)
    - und überprüft f(offen, signatur) = h(text), für die asymmetrische Verschlüsselungsfunktion g

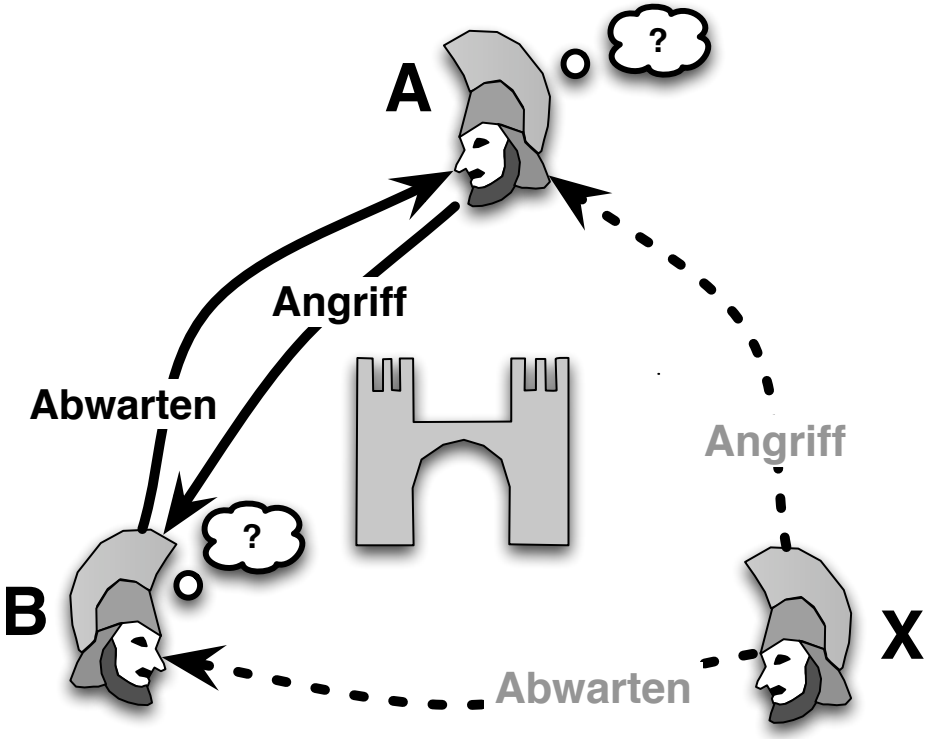
Das Problem der byzantinischen Generäle

- **Durch Infiltration eines Knoten in einem Netzwerk kann dieser bösartige Aktionen im Netzwerk verursachen**
  - Dieses Problem ist bekannt als das Problem der byzantinischen Generäle
- **3 Armeen stehen bereit die gegnerische Burg zu besiegen**
  - Diese sind getrennt und kommunizieren über Boten
  - Greift nur eine Armee an, so verliert diese.
  - Greifen zwei an, so gewinnen diese
  - Greift keine an, so wird die Burg ausgehungert
- **Aber ein General ist bösartig**
  - man weiß nicht, wer...



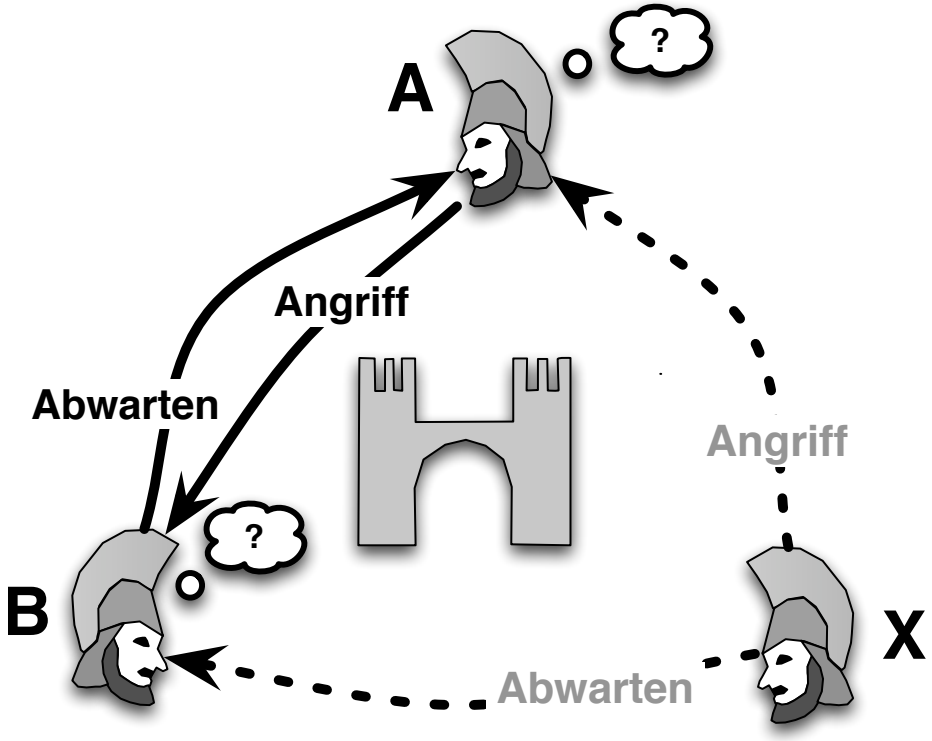
Das Problem der byzantinischen Generäle

- **Der übergelaufene General X versucht nun**
  - A zum Angriff zu überreden
  - B zum Abwarten
- **A übermittelt den Befehl an B**
- **B übermittelt den Befehl an A**
  - Widerspruch!



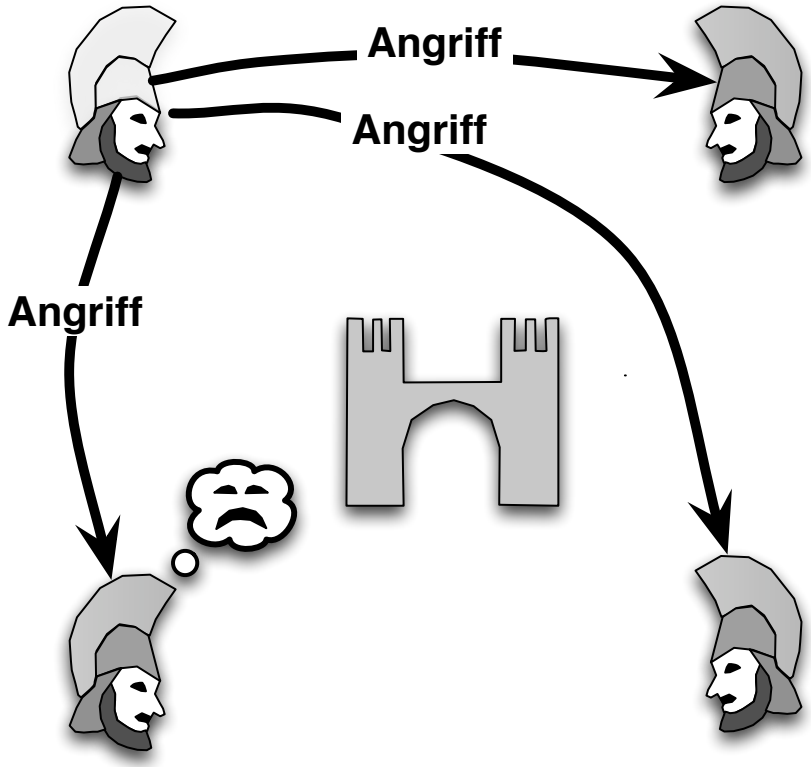
Das Problem der byzantinischen Generäle

- **A übermittelt den Befehl an B**
- **B übermittelt den Befehl an A**
  - Widerspruch!
- **Weder B noch A können X als Betrüger überführen**
  - da X A oder B als Überläufer darstellt



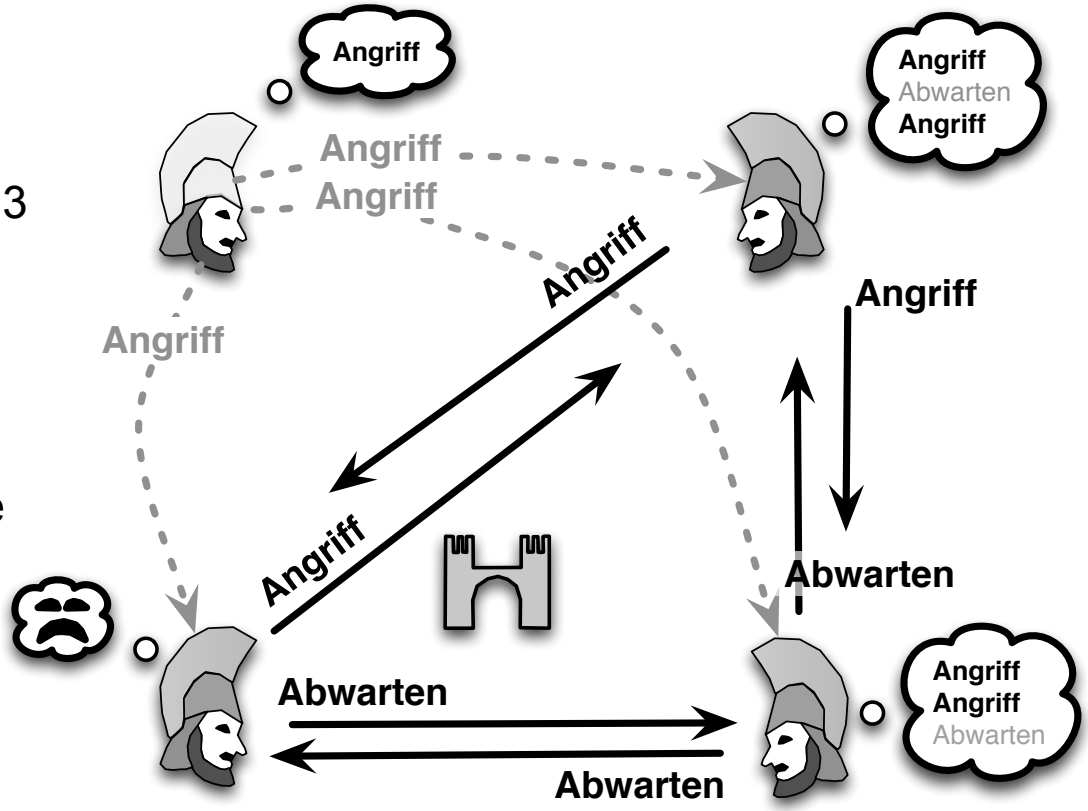
Byzantinische Abstimmung

- **Theorem**
  - Das Problem der drei byzantinischen Generäle kann nicht gelöst werden
- **Für vier Generäle ist das Problem lösbar**



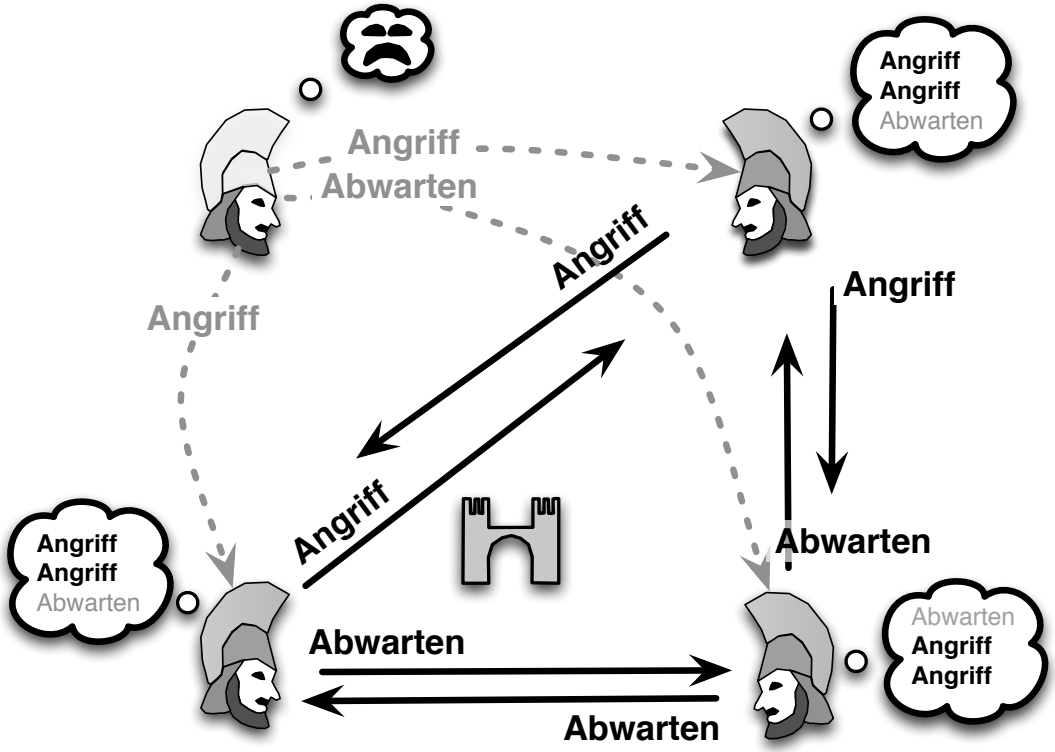
Byzantinische Abstimmung

- **Für vier Generäle ist das Problem lösbar:**
  - 1-General, 3 Offiziere-Problem
  - Betrachte einen (loyalen) General und 3 Offiziere.
  - Verbreite Information des loyalen Generals an alle Offizieren
- **Algorithmus**
  - General A sendet seinen Befehl an alle anderen (A bleibt bei seinem Befehl)
  - Jeder andere General sendet diesen erhaltenen Befehl an alle anderen
  - Jeder berechnet die Mehrheitsentscheidung aus den Befehlen von B, .., D



Byzantinische Abstimmung
Der Überläufer als General A

- **Für vier Generäle ist das Problem lösbar:**
  - 1-General, 3 Offiziere-Problem
  - Betrachte einen (illoyalen) General und 3 Offiziere.
  - Verbreite Information des loyalen Generals an alle Offizieren
- **Algorithmus**
  - General A sendet seinen Befehl an alle anderen (A bleibt bei seinem Befehl)
  - Jeder andere General sendet diesen erhaltenen Befehl an alle anderen
  - Jeder berechnet die Mehrheitsentscheidung aus den Befehlen von B, .., D



Lösung des Byzantinischen Generäle-Problems

- **Theorem**
  - Falls m Generäle Überläufer sind, müssen mindestens 2m+1 Generäle ehrlich sein, damit das Problem der Byzantinischen Generäle lösbar ist.
- **Diese Schranke ist genau, wenn keine kryptographischen Annahmen gemacht werden**
  - D.h. wenn man genug Zeit hat jede Verschlüsselung zu brechen
- **Theorem**
  - Steht ein digitales Signaturschema zur Verfügung, dann kann eine beliebige Anzahl von falschen Generälen verkraftet werden
- **Lösung:**
  - Jeder General unterschreibt seinen Befehl
  - In jeder Runde gibt jeder General alle Befehle an alle anderen weiter
  - Jeder inkonsistenter Befehl oder jede falsche Weitergabe kann sofort aufgedeckt und bewiesen werden
  - Schweigt ein General, so kann das unter den ehrlichen Generälen festgestellt werden

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Algorithmen für drahtlose Netzwerke

Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Rechnernetze und Telematik
Prof. Dr. Christian Schindelhauer