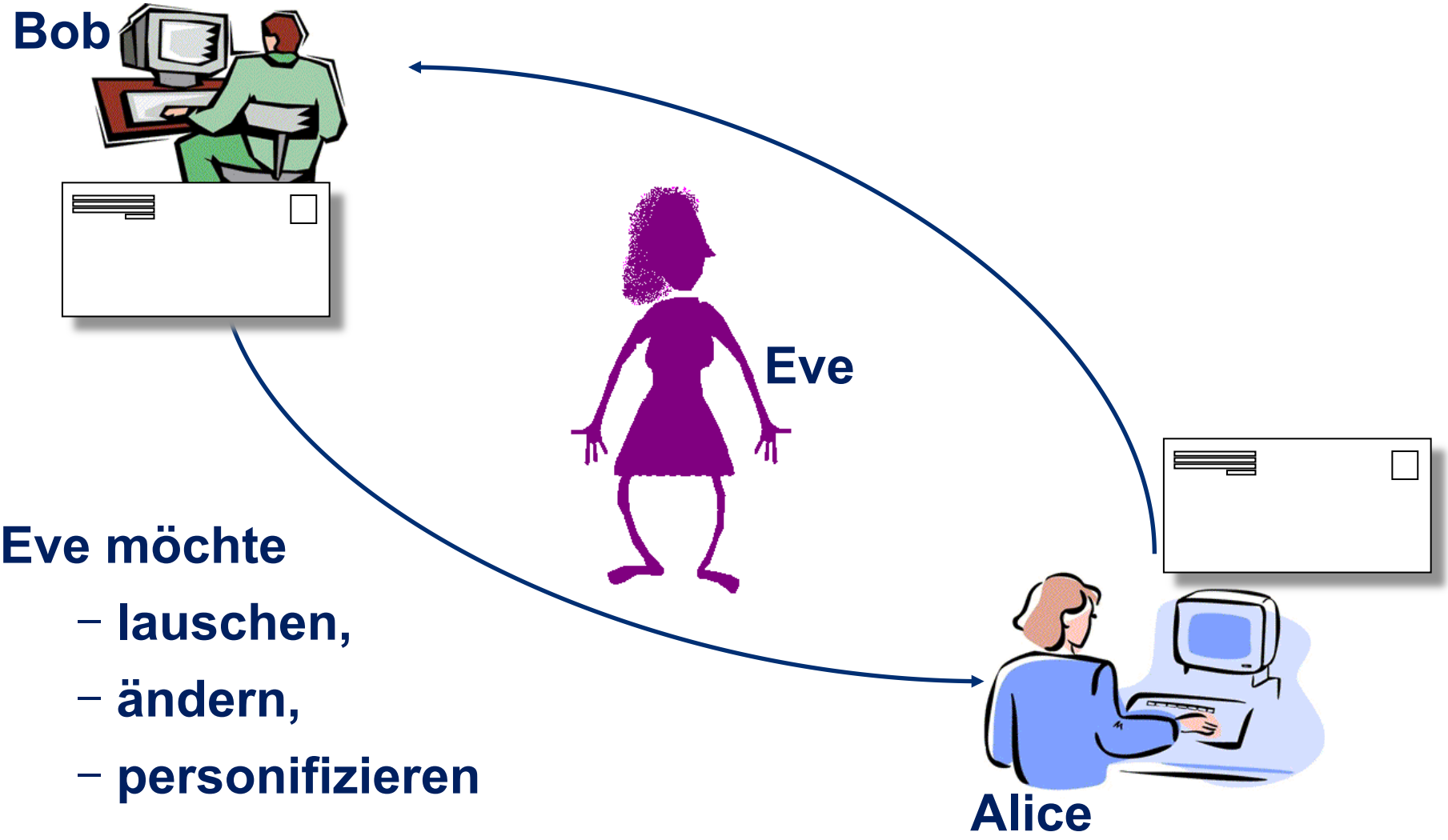
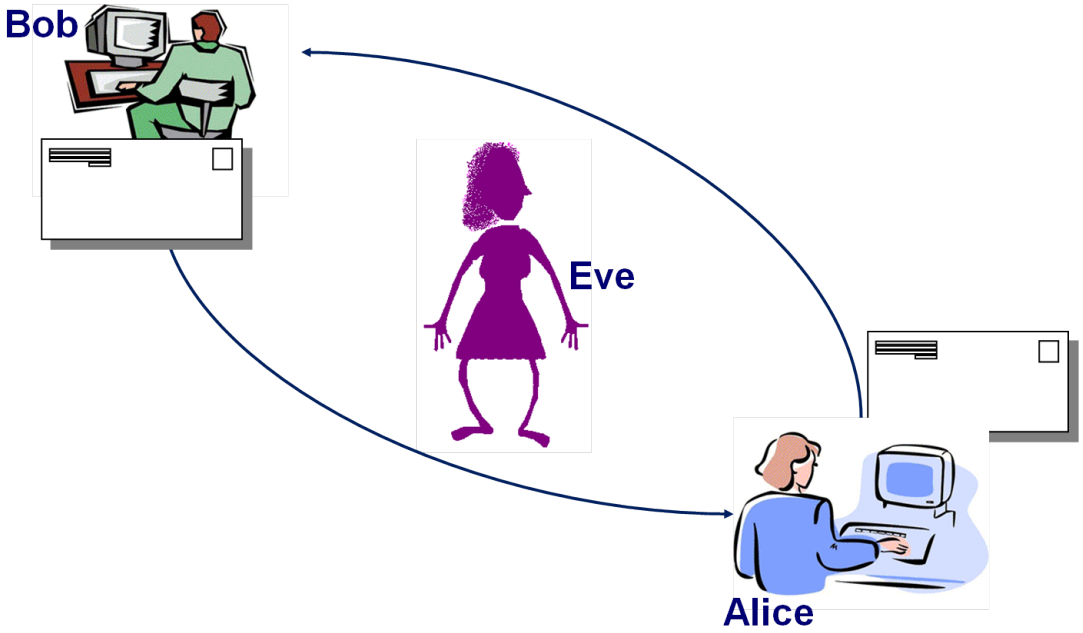
I. Einführung



Eve möchte

- lauschen,
- ändern,
- personifizieren

Aufgaben



- Vertraulichkeit - Lauschen
- Authentizität - Tauschen des Datenursprungs
- Integrität - Änderung der Daten
- Zurechenbarkeit - Leugnen des Datenursprungs

Beispiel WLAN

Access Point

Hier sind meine Kontozugangsdaten ....

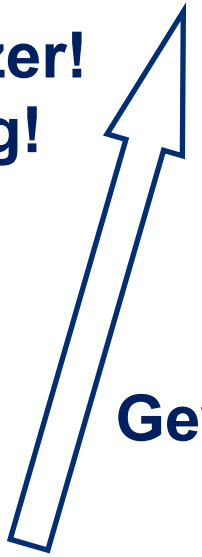
Hier sind meine Kontozugangs-daten ....

Vertraulichkeit!

Beispiel WLAN

Ich bin’s, dein Besitzer!
Gewähr mir Zugang!

Authentifizierung!

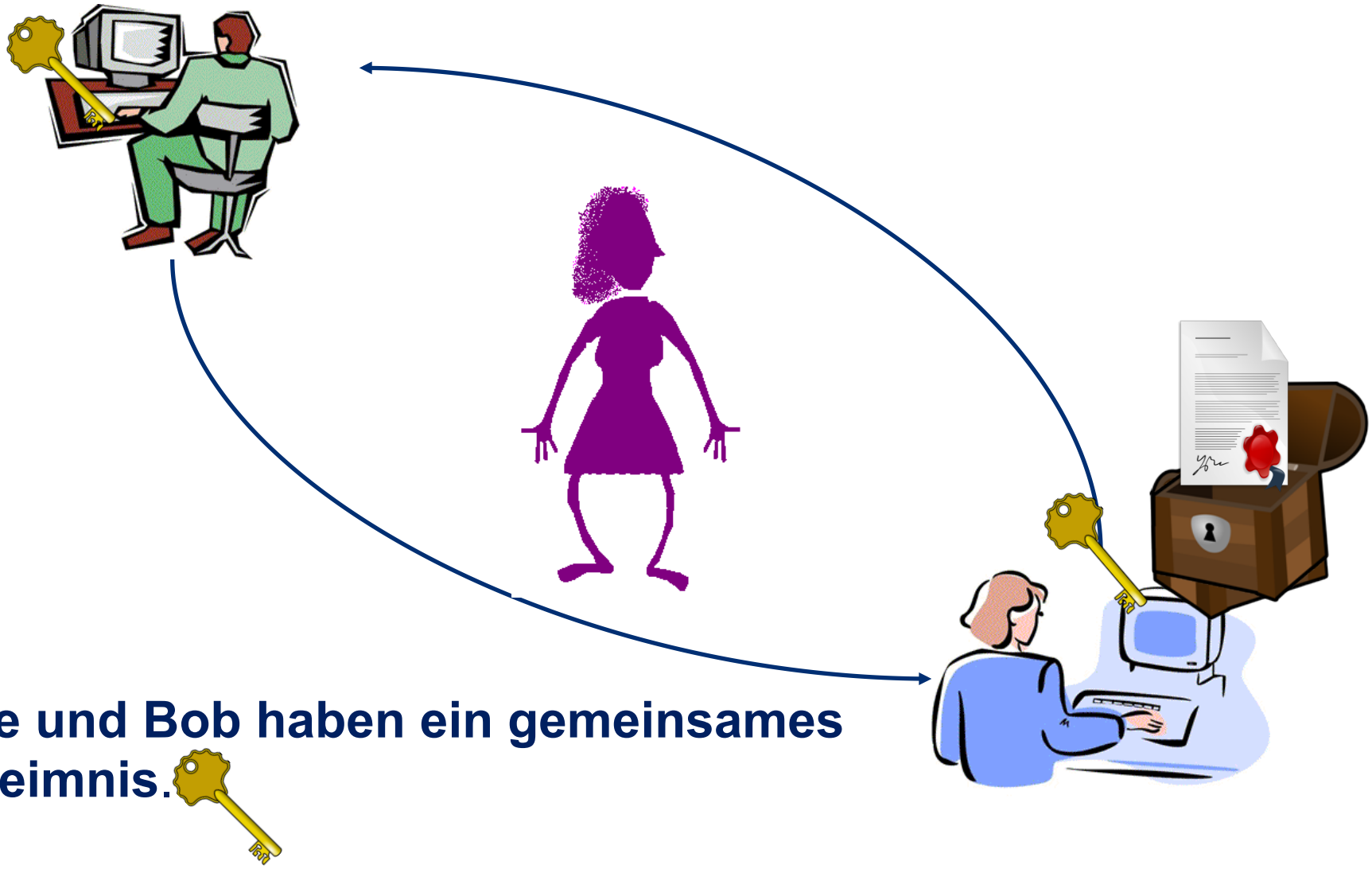


Ich bin’s,
dein Besitzer!
Gewähr mir Zugang!

Kryptographische Verfahren

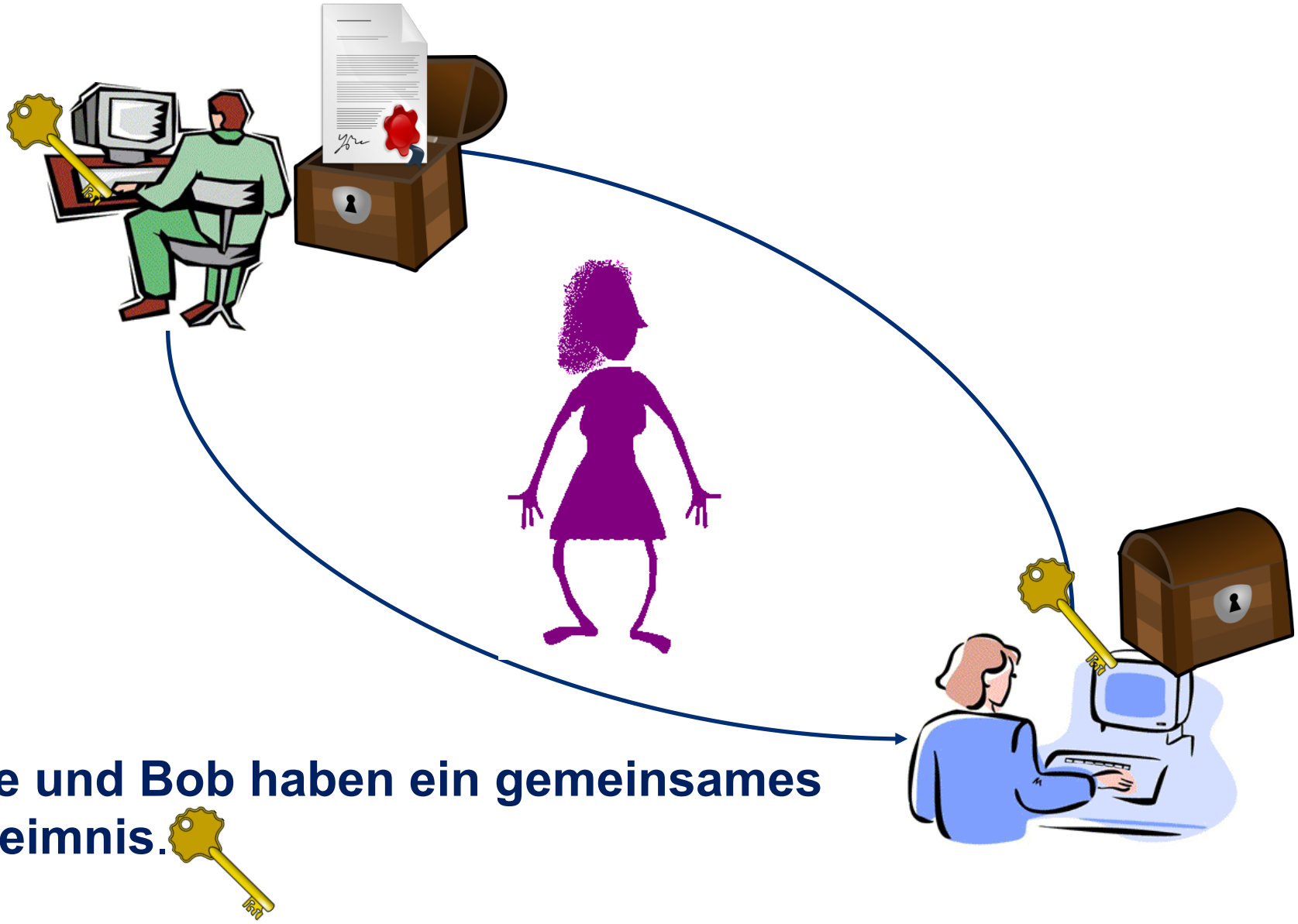
- Verschlüsselungsverfahren ≙ Vertraulichkeit
- Authentifzierungscodes (MACs) ≙ Authentifizierung
- Hashfunktionen ≙ Integrität
- Digitale Signaturen ≙ Authentifizierung & Zurechenbarkeit

Verschlüsselung (symmetrisch)



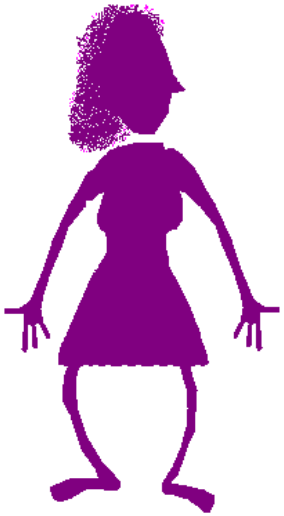
Alice und Bob haben ein gemeinsames Geheimnis.

Verschlüsselung (symmetrisch)



Alice und Bob haben ein gemeinsames Geheimnis.

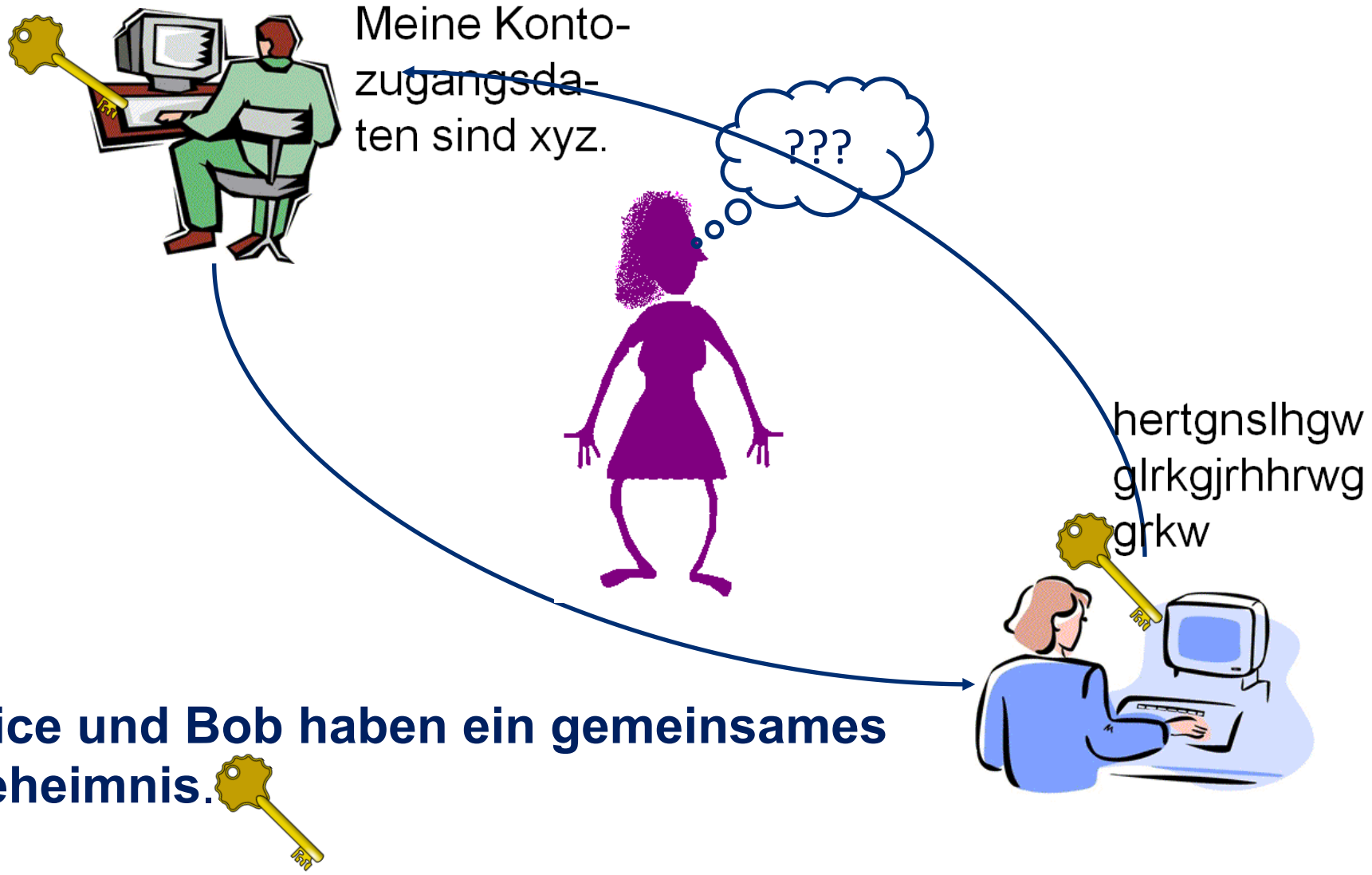
Verschlüsselung (symmetrisch)



Meine Kontozugangsdaten sind xyz.

Alice und Bob haben ein gemeinsames Geheimnis.

Verschlüsselung (symmetrisch)



Alice und Bob haben ein gemeinsames Geheimnis.

Verschlüsselungsverfahren

- Symmetrische Verschlüsselungsverfahren
  - Klassische Verfahren – Caesar, Vigenère
  - One-Time-Pad
  - DES (data encryption standard)
  - AES (advanced encryption standard)

- Asymmetrische Verschlüsselungsverfahren
  - RSA
  - Elgamal

Sicherheit

- Formale Sicherheitskonzepte
  - ununterscheidbare Verschlüsselung
  - perfekte Sicherheit

- Heuristische Sicherheit
  - besten bekannten Angriffe sind ineffizient

- Formale Sicherheit in Masterveranstaltungen

Informationen

Informationen zur Vorlesung unter

http://www-old.cs.uni-paderborn.de/fachgebiete/ag-bloemer/lehre/2015/ws/krypto111.html

Hier finden Sie

- **Übungsblätter**
- **Folien**
- **Literatur**
- **Ankündigungen**

Übungsblätter

- erscheinen zweiwöchentlich auf der Webseite, jeweils freitags
- Abgabe 10 Tage später; montags 14:00 Uhr
- Gruppenabgabe bis maximal drei Personen erwünscht
- 40% der Übungspunkte notwendig zum Bestehen der Veranstaltung
- Verbesserung der Prüfungsnote durch gute Übungsleistungen möglich
- Verbesserung der Prüfungsnote 5 nicht möglich
- Übungen beginnen kommende Woche
- in den ersten beiden Wochen jeweils ein Übungsblatt
- erstes Blatt Wiederholung, Abgabe Montag, 26. Oktober

Literatur

- Es wird kein Skript zur Vorlesung geben.
- Vorlesung richtet sich weitgehend nach
  - J.Buchmann, Einführung in die Kryptographie
- Das Buch ist auf den Seiten der Uni-Bibliothek aus den internen Uni-Netz frei verfügbar.