VI. Public-Key Kryptographie

Definition 2.1 Ein Verschlüsselungsverfahren ist ein 5-Tupel (P,C,K,E,D), wobei

1. P die Menge der Klartexte ist.
2. C die Menge der Chiffretexte ist.
3. K die Menge der Schlüssel ist.
4. $E=\{E_k : k \in K\}$ eine Menge von Verschlüsselungsfunktionen $E_k : P \to C$ ist.
5. $D=\{D_k : k \in K\}$ eine Menge von Entschlüsselungsfunktionen $D_k : C \to P$ ist.
6. Zu jedem $e \in K$ existiert ein $d \in K$, so dass für alle $m \in P$

$$D_d(E_e(m)) = m.$$

Schlüssel e,d mit dieser Eigenschaft heißen **Schlüsselpaare**.

Symmetrische & asymmetrische Verfahren

auch Private-Key-Verfahren & Public-Key-Verfahren

Gilt für $e,d \in K$, dass $D_d(E_e(m)) = m$ für alle $m \in P$, so heißt (e,d) ein Schlüsselpaar.

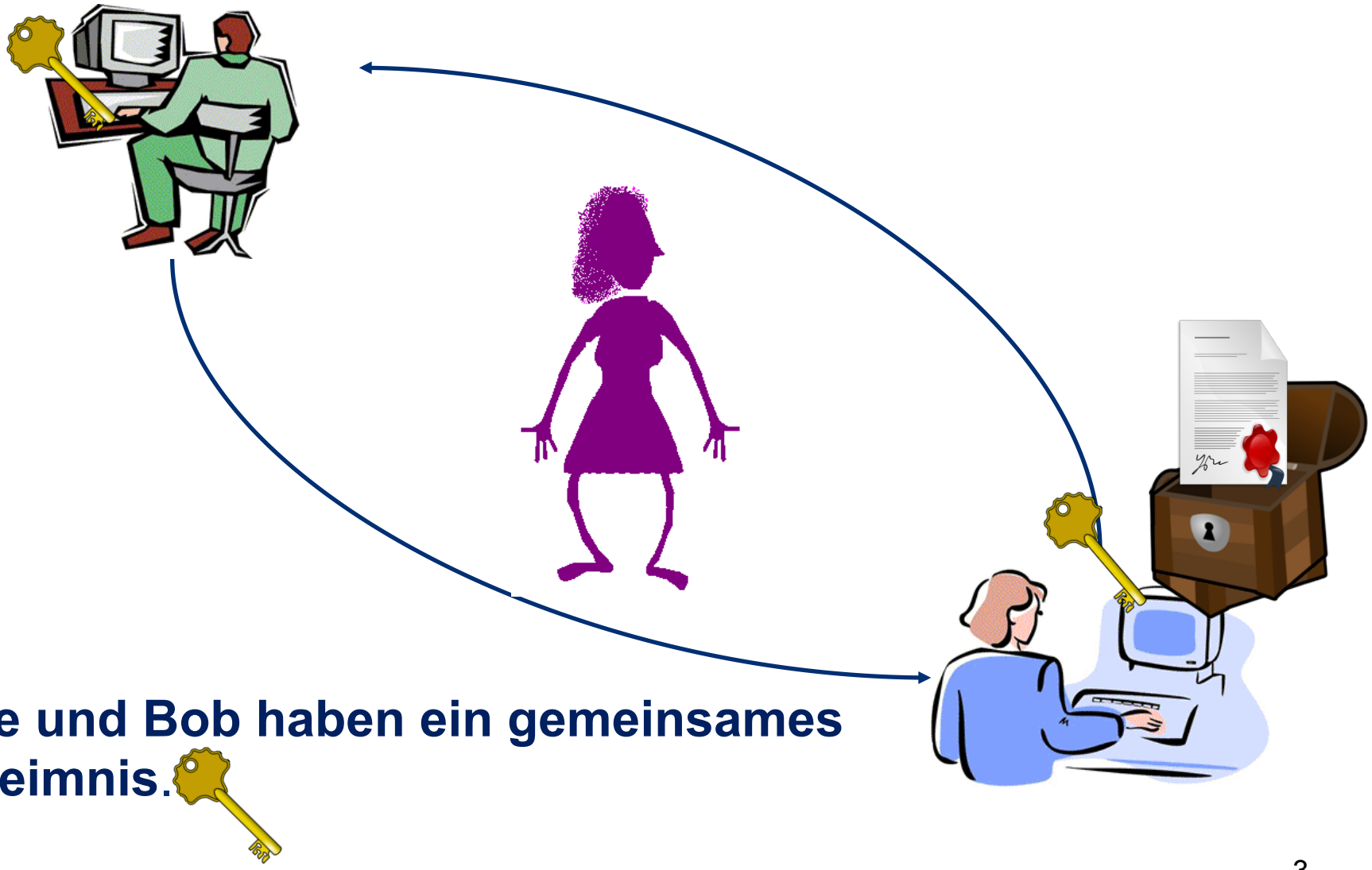
Symmetrische Verfahren Für alle Schlüsselpaare (e,d)

- e = d oder
- d kann aus e leicht berechnet werden.

Asymmetrische Verfahren Für alle Schlüsselpaare (e,d)

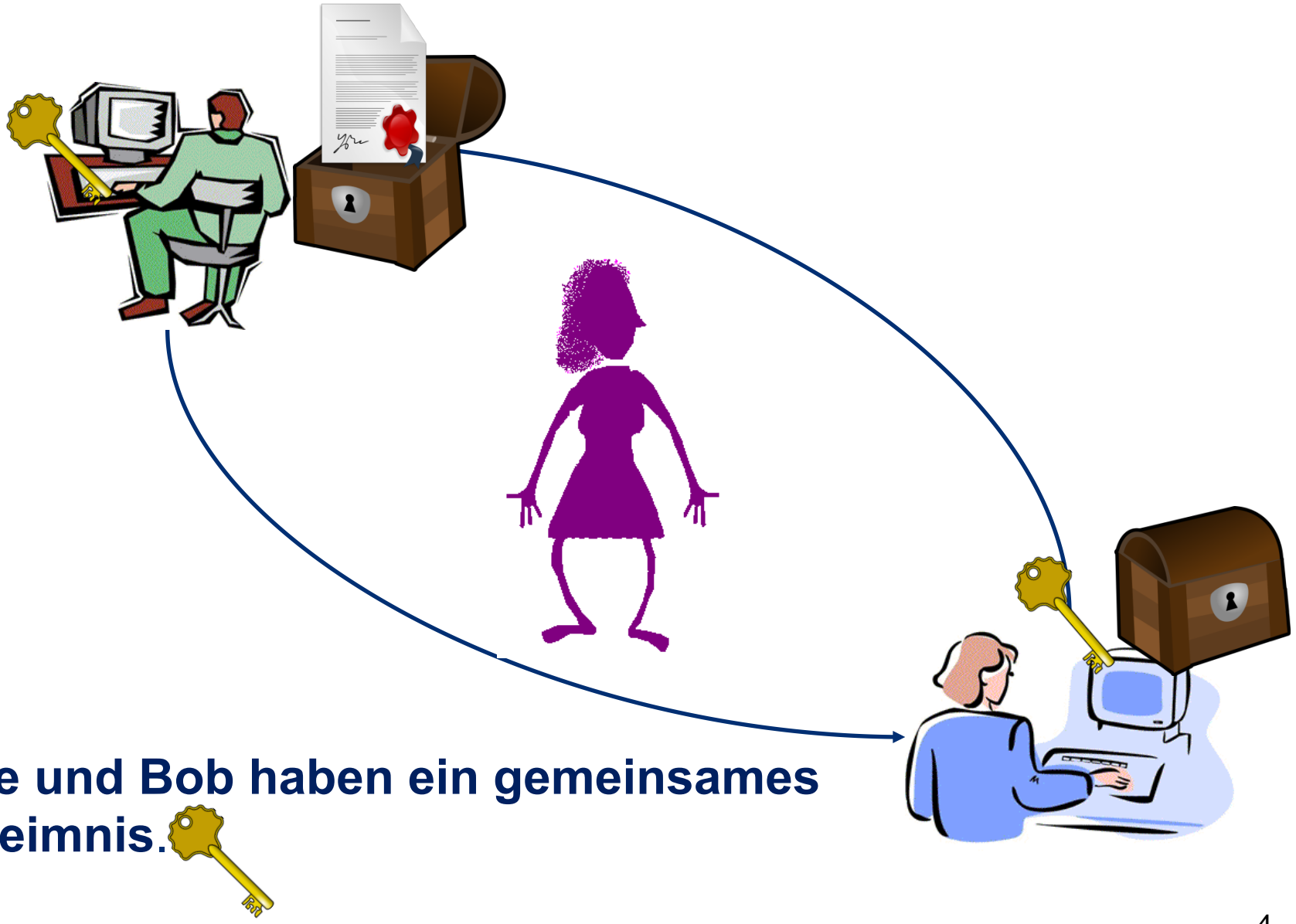
- d kann aus e nicht mit vertretbarem Aufwand berechnet werden.

Verschlüsselung (symmetrisch)



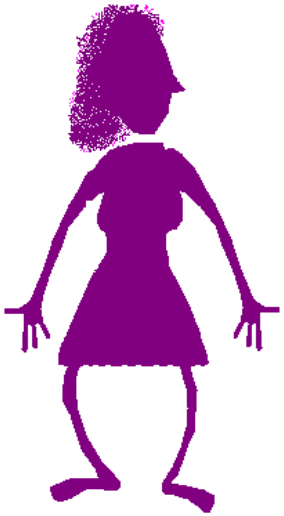
Alice und Bob haben ein gemeinsames Geheimnis.

Verschlüsselung (symmetrisch)



Alice und Bob haben ein gemeinsames Geheimnis.

Verschlüsselung (symmetrisch)

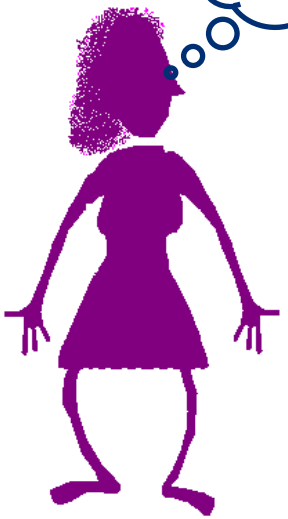


Meine Kontozugangsdaten sind xyz.

Alice und Bob haben ein gemeinsames Geheimnis.

Verschlüsselung (symmetrisch)

Meine Konto-
zugangsda-
ten sind xyz.



hertgnslhgw
glrkgjrhhrwg
grkw

Alice und Bob haben ein gemeinsames Geheimnis.

VI.1 Probleme und Idee

Hauptprobleme symmetrischer Verschlüsselung

- A(lice) und B(ob) benötigen gemeinsamen geheimen Schlüssel.
- Wie erhalten sie diesen Schlüssel?

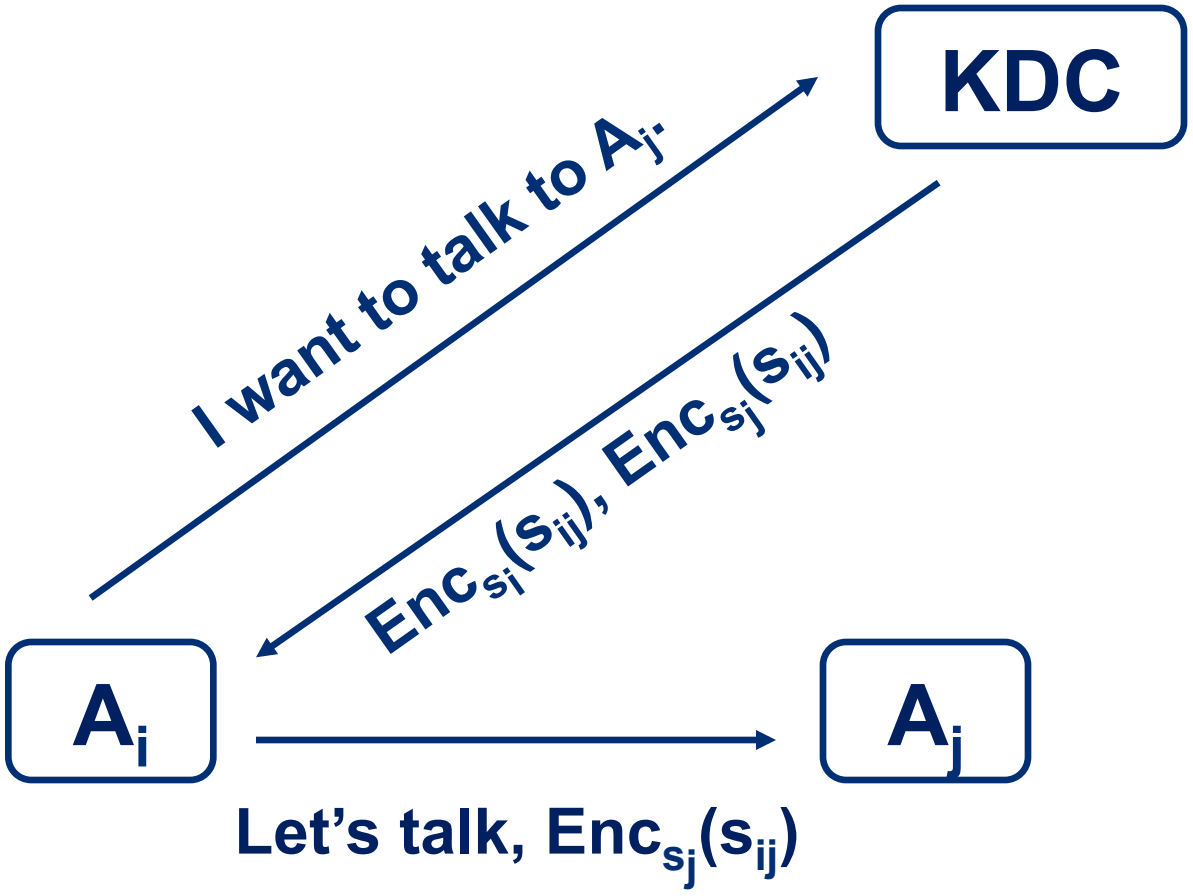
Zwei zusätzliche Probleme

- Wollen sichere Kommunikation zwischen je 2 aus n Parteien $A_1,\ldots, A_n$ ermöglichen.
- Wie speichert A_i n-1 geheime Schlüssel?
- Wie werden Schlüssel für neue Teilnehmer erzeugt und verteilt?

Zentrale Instanzen

- Wollen sichere Kommunikation ziwschen je zwei aus n Parteien $A_1,\ldots, A_n$ ermöglichen.
- Zentrale Instanz KDC (key distribution center) zusätzliche Partei.
- Jedes A_i besitzt geheimen Schlüssel s_i mit KDC.
- A_i möchte mit A_j kommunizieren: A_i erbittet bei KDC geheimen Schlüssel s_{ij} für diese Kommunikation.
- KDC sendet s_{ij} verschlüsselt zunächst mit s_i und mit s_j an A_i.
- A_i leitet s_{ij} verschlüsselt mit s_j an A_j.

Rolle von KDCs



Problems with KDCs

- Nur möglich in zentralisierten Systemen.
- KDC ist single-point-of-failure, d.h., KDC muss stets verfügbar sein.
- KDC ist single-point-of-attack, d.h., wird KDC erfolgreich angegriffen, ist jede Kommunikation unsicher.

VI. Public-Key Kryptographie

Definition 2.1 Ein Verschlüsselungsverfahren is ein 5-Tupel (P,C,K,E,D), wobei

1. P die Menge der Klartexte ist.
2. C die Menge der Chiffretexte ist.
3. K die Menge der Schlüssel ist.
4. $E=\{E_k : k \in K\}$ eine Menge von Verschlüsselungsfunktionen $E_k : P \to C$ ist.
5. $D=\{D_k : k \in K\}$ eine Menge von Entschlüsselungsfunktionen $D_k : C \to P$ ist.
6. Zu jedem $e \in K$ existiert ein $d \in K$, so dass für alle $m \in P$

$$D_d(E_e(m)) = m.$$

Schlüssel e,d mit dieser Eigenschaft heißen **Schlüsselpaare**.

Symmetrische & asymmetrische Verfahren

auch Private-Key-Verfahren & Public-Key-Verfahren

Gilt für $e,d \in K$, dass $D_d(E_e(m)) = m$ für alle $m \in P$, so heißt (e,d) ein Schlüsselpaar.

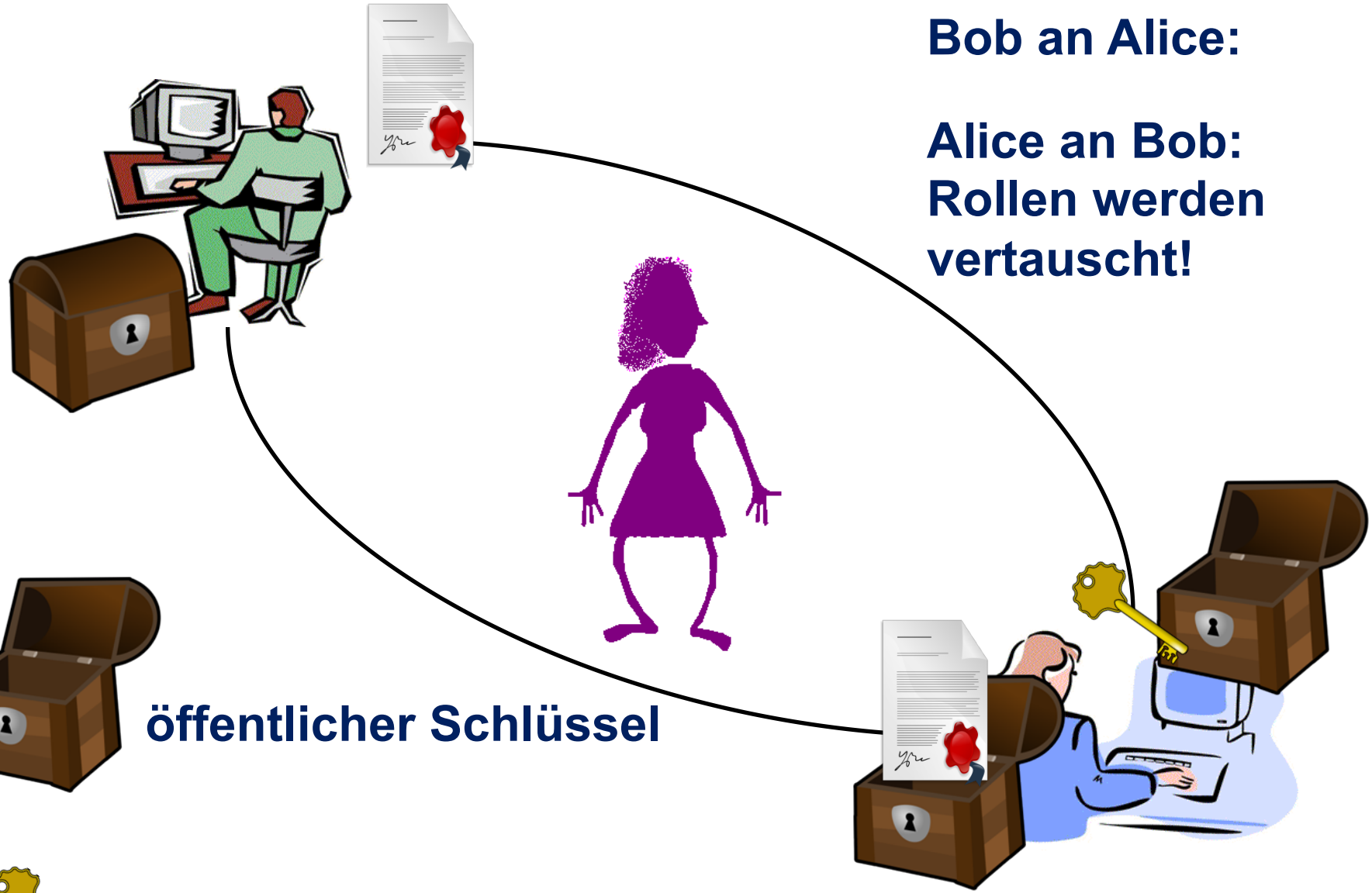
Symmetrische Verfahren Für alle Schlüsselpaare (e,d)

- e = d oder
- d kann aus e leicht berechnet werden.

Asymmetrische Verfahren Für alle Schlüsselpaare (e,d)

- d kann aus e nicht mit vertretbarem Aufwand berechnet werden.

Verschlüsselung (asymmetrisch)



Bob an Alice:

Alice an Bob:
Rollen werden vertauscht!

öffentlicher Schlüssel

geheimer Schlüssel

Konsequenzen

Symmetrische Verfahren

- e muss über sicheren Kanal ausgetauscht werden.
- e muss geheim gehalten werden.

Asymmetrische Verfahren

- e kann öffentlich sein.
- Kommunikation von A zu B benötigt anderes Schlüsselpaar als Kommunikation von B zu A.
- e heißt öffentlicher Schlüssel (public key).
- d heißt geheimer oder privater Schlüssel (private key).
- e und d häufig leicht unterschiedliches Format, aber Anpassung von Definition 2.1 (unwesentlich).

Das Public-Key Paradigma

- Eingeführt 1976 von Diffie and Hellman.

- Diffie und Hellman schlugen drei Primitiven vor.

  - Public-Key Verschlüsselung
    - ➔ vertrauliche Kommunikation ohne gemeinsame Schlüssel.

  - Digitale Signaturen
    - ➔ Integrität und Authentizität ohne gemeinsame Schlüssel.

  - Interaktiver Schlüsselaustausch
    - ➔ Einigung auf gemeinsame Schlüssel ohne Treffen.

VI.2 Sicherheit von Public-Key Verschlüsselung

Analyse der Sicherheit eines Verfahrens benötigt Wissen über

- Ziele eines Angreifers
- Möglichkeiten eines Angreifers

Ziele eines Angreifers

- Berechnung des Schlüssels d
- Berechnung eines Klartextes m aus einem Chiffretext c
- Berechnung spezieller Informationen über m aus c

Möglichkeiten eines Angreifers

- **Ciphertext-Only Angriff** Angreifer kennt nur Chiffretext c.
- **Known-Plaintext Angriff** Angreifer kennt Chiffretext c und Paare (m_i,c_i) von Klartexten und Chiffretexten unter dem gleichen Schlüssel e
- **Chosen-Plaintext Angriff** Angreifer kann sich zu selbst gewählten Klartexten m_i die Chiffretexte c_i erzeugen.
- **Chosen-Ciphertext Angriff** Angreifer kann sich zu selbst gewählten Chiffretexten c_i die Klartexte m_i erzeugen.

Möglichkeiten eines Angreifers

Ein Angreifer kennt immer auch den öffentlichen Schlüssel, und kann damit einen Chosen-Plaintext Angriff durchführen.

- **Chosen-Plaintext Angriff Angreifer kann sich zu selbst gewählten Klartexten m_i die Chiffretexte c_i erzeugen.**

- **Chosen-Ciphertext Angriff Angreifer kann sich zu selbst gewählten Chiffretexten c_i die Klartexte m_i erzeugen.**

Sicherheit des privaten Schlüssels

Unerläßliche Sicherheitseigenschaft **Der private Schlüssel d kann nicht mit vertretbarem Aufwand aus dem öffentlichen Schlüssel e berechnet werden.**

Umsetzung in der Praxis **Berechnung von privatem Schlüssel d aus öffentlichem Schlüssel e gleichbedeutend mit Lösen eines vermutet schweren Problems (der Zahlentheorie).**