



# Übung GSS Blatt 6

SVS – Sicherheit in Verteilten Systemen

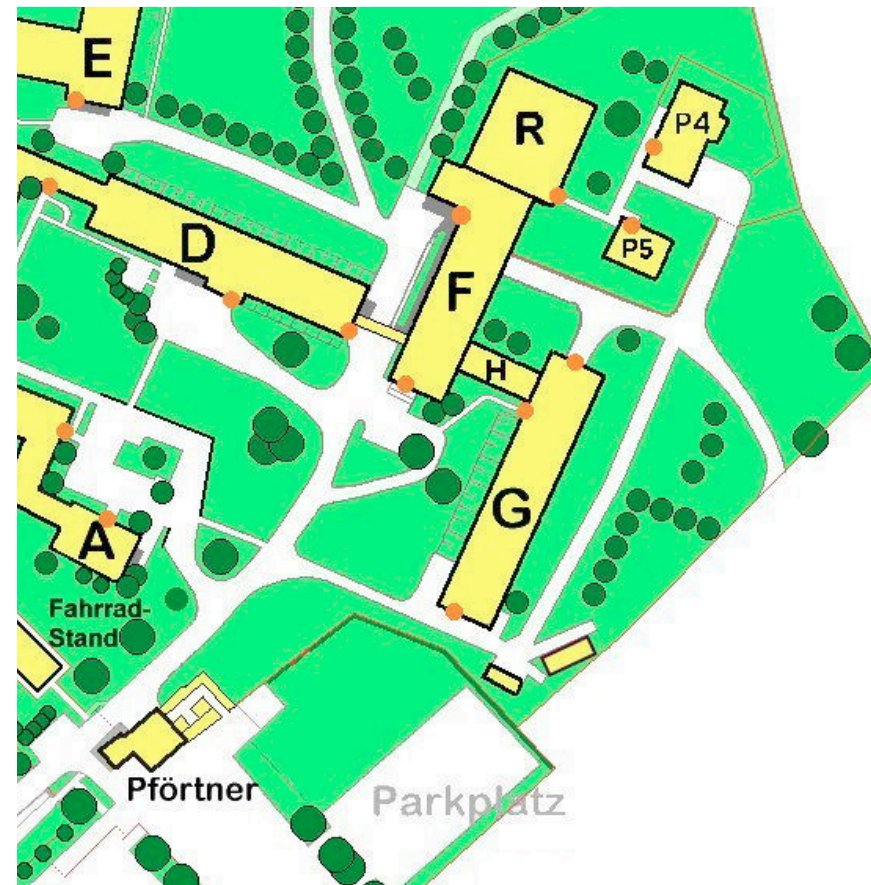


Universität Hamburg

DER FORSCHUNG | DER LEHRE | DER BILDUNG

## Einladung zum SVS-Sommerfest

- SVS-Sommerfest
  - **am 12.07.16 ab 17 Uhr**
  - Ihr seid eingeladen! :-)
- Es gibt
  - Thüringer Bratwürste im Brötchen oder Grillkäse
  - kalte Getränke
- Ort:
  - Campus Stellingen
  - voraussichtlich vor oder hinter Haus G
- Bitte mit E-Mail-Adresse anmelden
  - <http://tinyurl.com/svsbbq16>



## Aufgabe 1: Zentrale Begriffe der Kryptographie

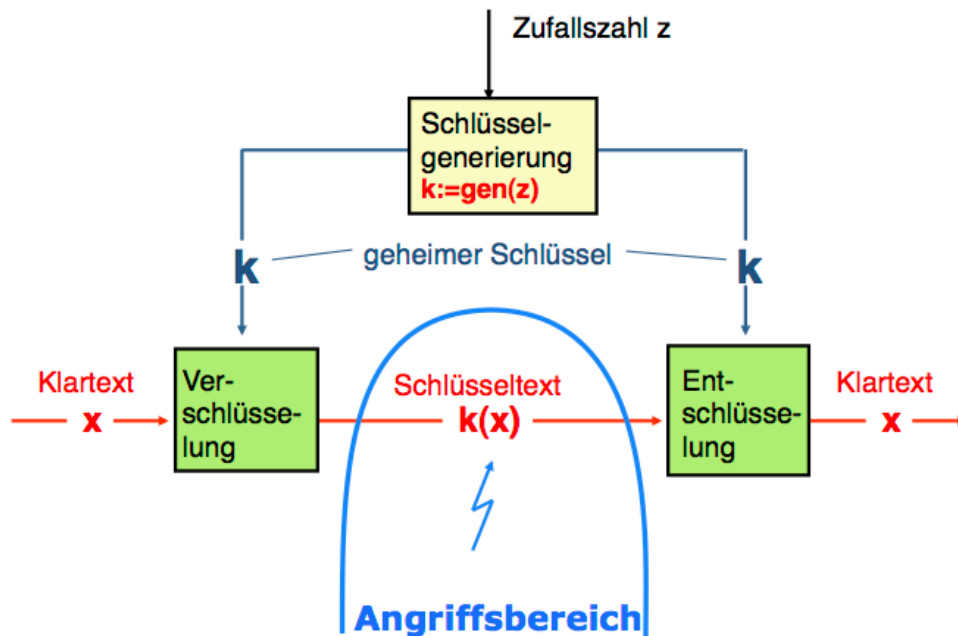
---

- Teilaufgabe 1: Unterschiedliche Chiffren (Optional)  
Was ist der Unterschied zwischen einem symmetrischen und einem asymmetrischen Kryptosystem?

## Aufgabe 1: Zentrale Begriffe der Kryptographie

- Teilaufgabe 1: Unterschiedliche Chiffren (Optional)  
Was ist der Unterschied zwischen einem symmetrischen und einem asymmetrischen Kryptosystem?

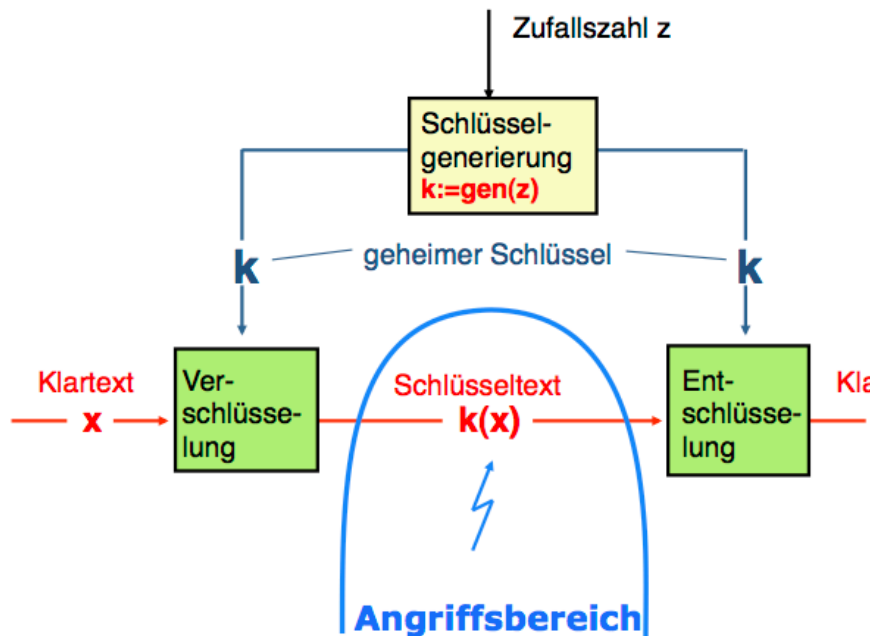
### Symmetrische Verschlüsselung



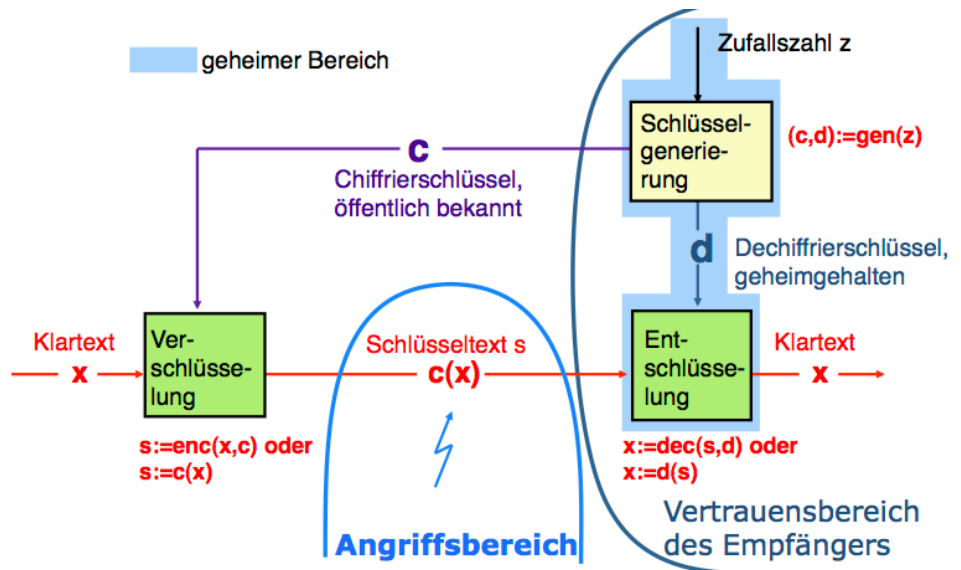
# Aufgabe 1: Zentrale Begriffe der Kryptographie

- Teilaufgabe 1: Unterschiedliche Chiffren (Optional)  
Was ist der Unterschied zwischen einem symmetrischen und einem asymmetrischen Kryptosystem?

## Symmetrische Verschlüsselung



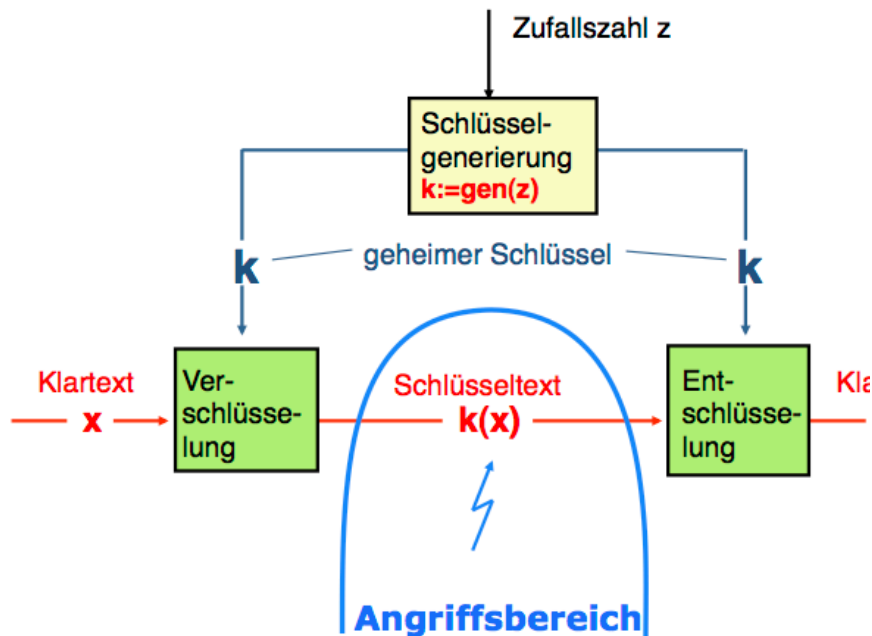
## Asymmetrische Verschlüsselung



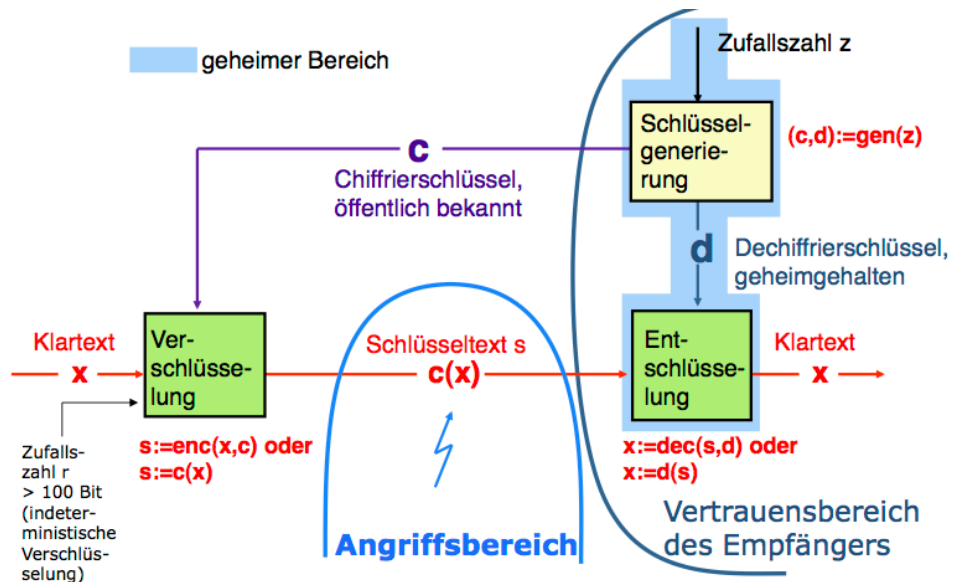
# Aufgabe 1: Zentrale Begriffe der Kryptographie

- Teilaufgabe 1: Unterschiedliche Chiffren (Optional)  
Was ist der Unterschied zwischen einem symmetrischen und einem asymmetrischen Kryptosystem?

## Symmetrische Verschlüsselung



## Asymmetrische Verschlüsselung



## Aufgabe 1: Zentrale Begriffe der Kryptographie

---

- Teilaufgabe 1: Unterschiedliche Chiffren (Optional)  
Was ist der Unterschied zwischen einem symmetrischen und einem asymmetrischen Kryptosystem?

Symmetrisches Kryptosystem:

Sender und Empfänger haben 1 gemeinsamen Schlüssel, der sowohl zum Verschlüsseln als auch zum Entschlüsseln verwendet wird.

Asymmetrisches Kryptosystem:

Zum Verschlüsseln wird ein anderer Schlüssel verwendet als zum Entschlüsseln.

## Aufgabe 1: Zentrale Begriffe der Kryptographie

---

- Teilaufgabe 3: Hybride Kryptosysteme (Pflicht)
  - Warum werden hybride Kryptosysteme eingesetzt, wie werden sie benutzt und wie sehen Nachrichten in diesem Fall aus.

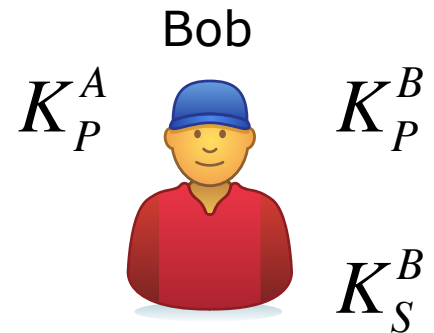
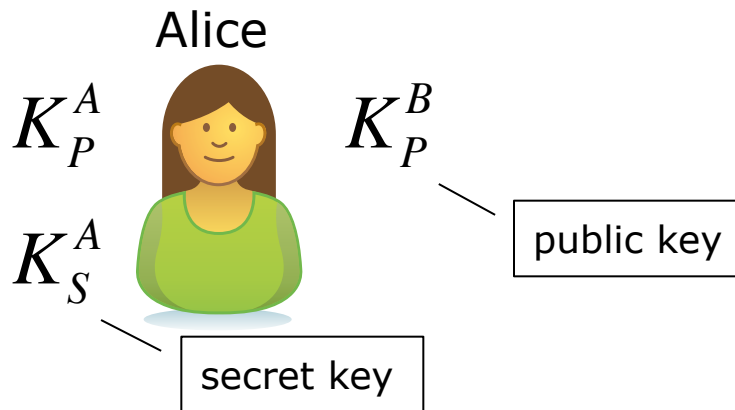


## Aufgabe 1: Zentrale Begriffe der Kryptographie

- Teilaufgabe 3: Hybride Kryptosysteme (Pflicht)
  - Warum werden hybride Kryptosysteme eingesetzt, wie werden sie benutzt und wie sehen Nachrichten in diesem Fall aus.
  - Asymmetrische Kryptosysteme sind **wesentlich langsamer** als symmetrische.
  - Bei symmetrischen Kryptosystemen ist das **Schlüsselmanagement aufwändiger** (bei  $n$  Teilnehmern müssen  $(n * (n-1)) / 2$  gemeinsame Schlüssel erzeugt und ausgetauscht werden!).
  - **Hybride Systeme** vereinen die Vorteile beider Systeme und vermeiden dennoch ihre Nachteile.

## Aufgabe 1: Zentrale Begriffe der Kryptographie

- Teilaufgabe 3: Hybride Kryptosysteme (Pflicht)
  - Warum werden hybride Kryptosysteme eingesetzt, wie werden sie benutzt und wie sehen Nachrichten in diesem Fall aus.



# Aufgabe 1: Zentrale Begriffe der Kryptographie

- Teilaufgabe 3: Hybride Kryptosysteme (Pflicht)
  - Warum werden hybride Kryptosysteme eingesetzt, wie werden sie benutzt und wie sehen Nachrichten in diesem Fall aus.



- generiert sym. Schlüssel  $K_M$
- verschlüsselt  $M$  symmetrisch mit  $K_M \rightarrow M'$
- verschlüsselt  $K_M$  asymmetrisch mit  $K_P^B \rightarrow K_M'$
- sendet  $(M', K_M')$  an Bob

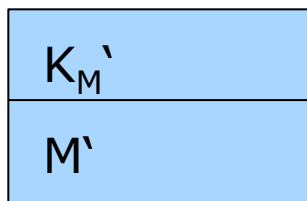


# Aufgabe 1: Zentrale Begriffe der Kryptographie

- Teilaufgabe 3: Hybride Kryptosysteme (Pflicht)
  - Warum werden hybride Kryptosysteme eingesetzt, wie werden sie benutzt und wie sehen Nachrichten in diesem Fall aus.



- generiert sym. Schlüssel  $K_M$
- verschlüsselt  $M$  symmetrisch mit  $K_M \rightarrow M'$
- verschlüsselt  $K_M$  asymmetrisch mit  $K_P^B \rightarrow K_M'$
- sendet  $(M', K_M')$  an Bob



- entschlüsselt  $K_M'$  mit  $K_S^B \rightarrow K_M$
- entschlüsselt  $M'$  mit  $K_M \rightarrow M$

## Aufgabe 3: Authentifizierungsprotokolle

---

- Teilaufgabe 1: Verschlüsselte Passwortübermittlung (Optional)

## Aufgabe 3: Authentifizierungsprotokolle

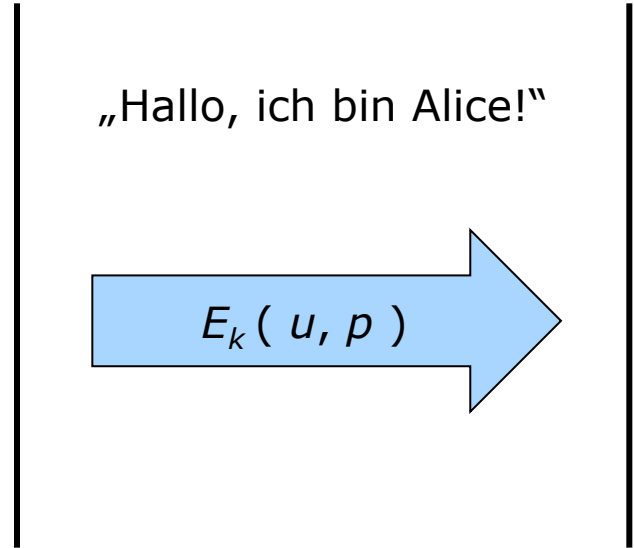
- Teilaufgabe 1: Verschlüsselte Passwortübermittlung (Optional)  
Nutzer  $u$  authentisiert sich bei einem Server mit einem Passwort  $p$ .  
Die Übertragung wird mit symmetrischem Schlüssel  $k$  verschlüsselt:  
 $c = E_k(u, p)$  und  $c$  wird an den Server geschickt.
  - Welche Schwäche weist dieses Protokoll auf?

**ALICE**

**BOB**

„Hallo, ich bin Alice!“

$E_k(u, p)$



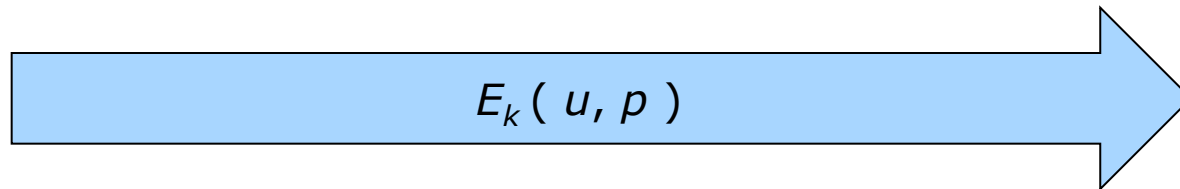
## Aufgabe 3: Authentifizierungsprotokolle

- Teilaufgabe 1: Verschlüsselte Passwortübermittlung (Optional)
  - Welche Schwäche weist dieses Protokoll auf?

- Aktiver Angreifer kann **Replay-Angriff** durchführen und sich am Server anmelden

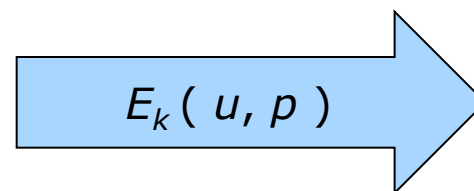
**ALICE**

**BOB**



**TRUDY**

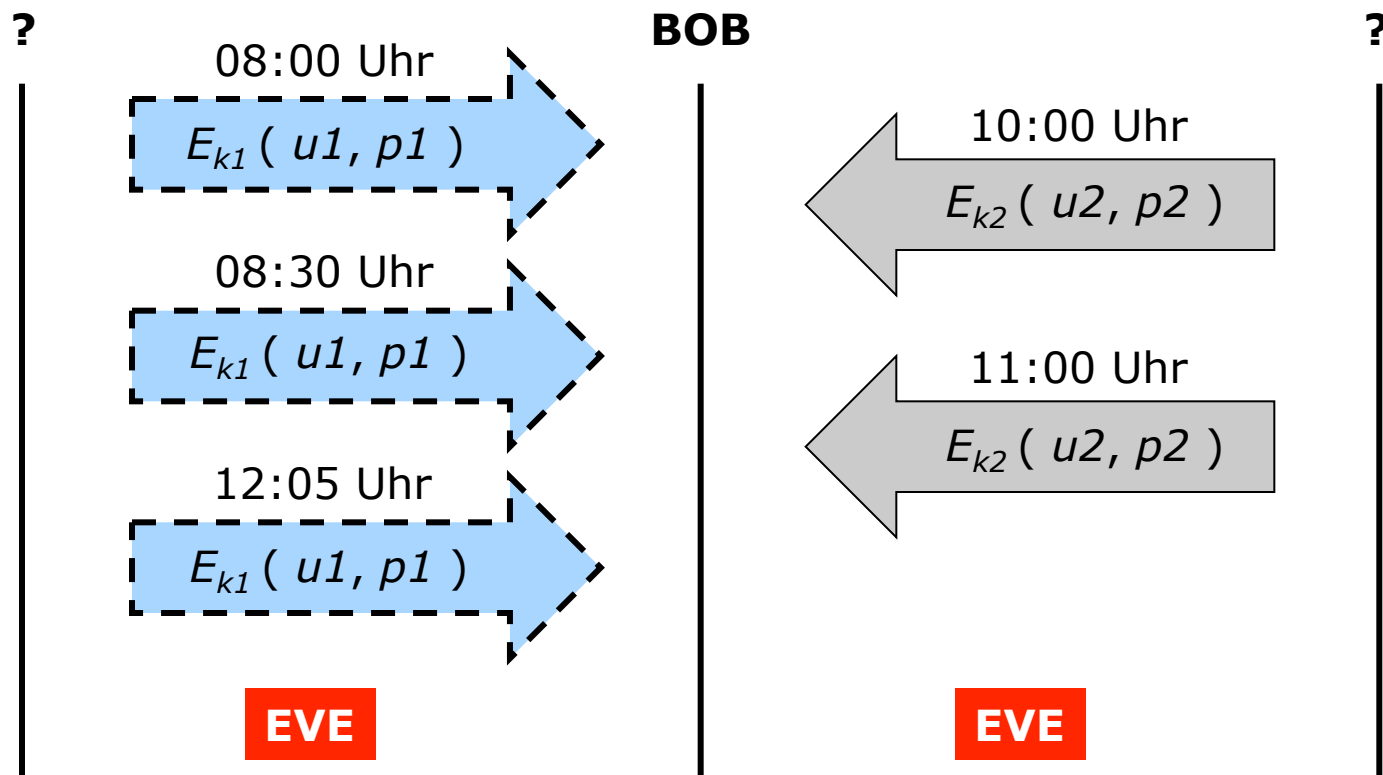
„Hallo, ich bin Alice!“



## Aufgabe 3: Authentifizierungsprotokolle

- Teilaufgabe 1: Verschlüsselte Passwortübermittlung (Optional)
  - Welche Schwäche weist dieses Protokoll auf?

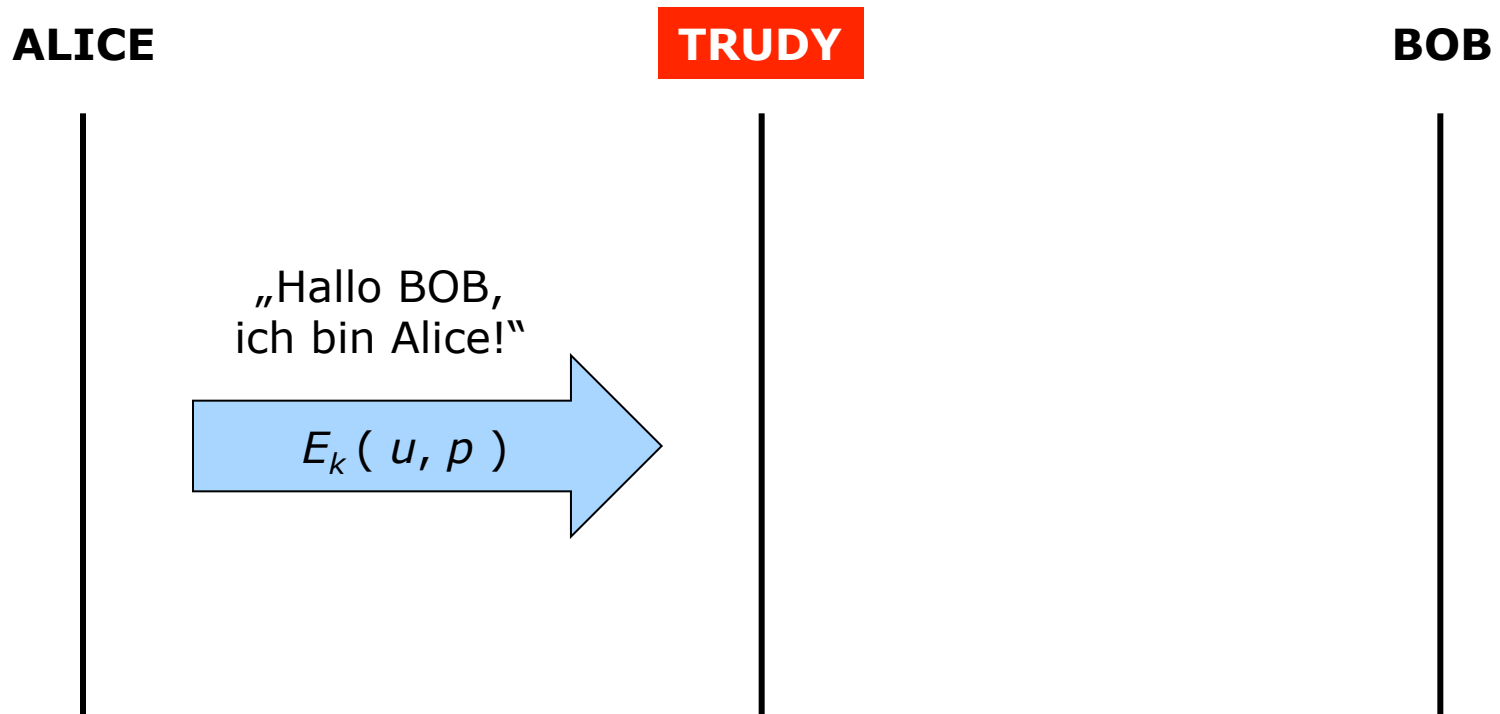
2. Passiver Angreifer kann **Verkehrsanalyse** durchführen und Nachrichten verketten





## Aufgabe 3: Authentifizierungsprotokolle

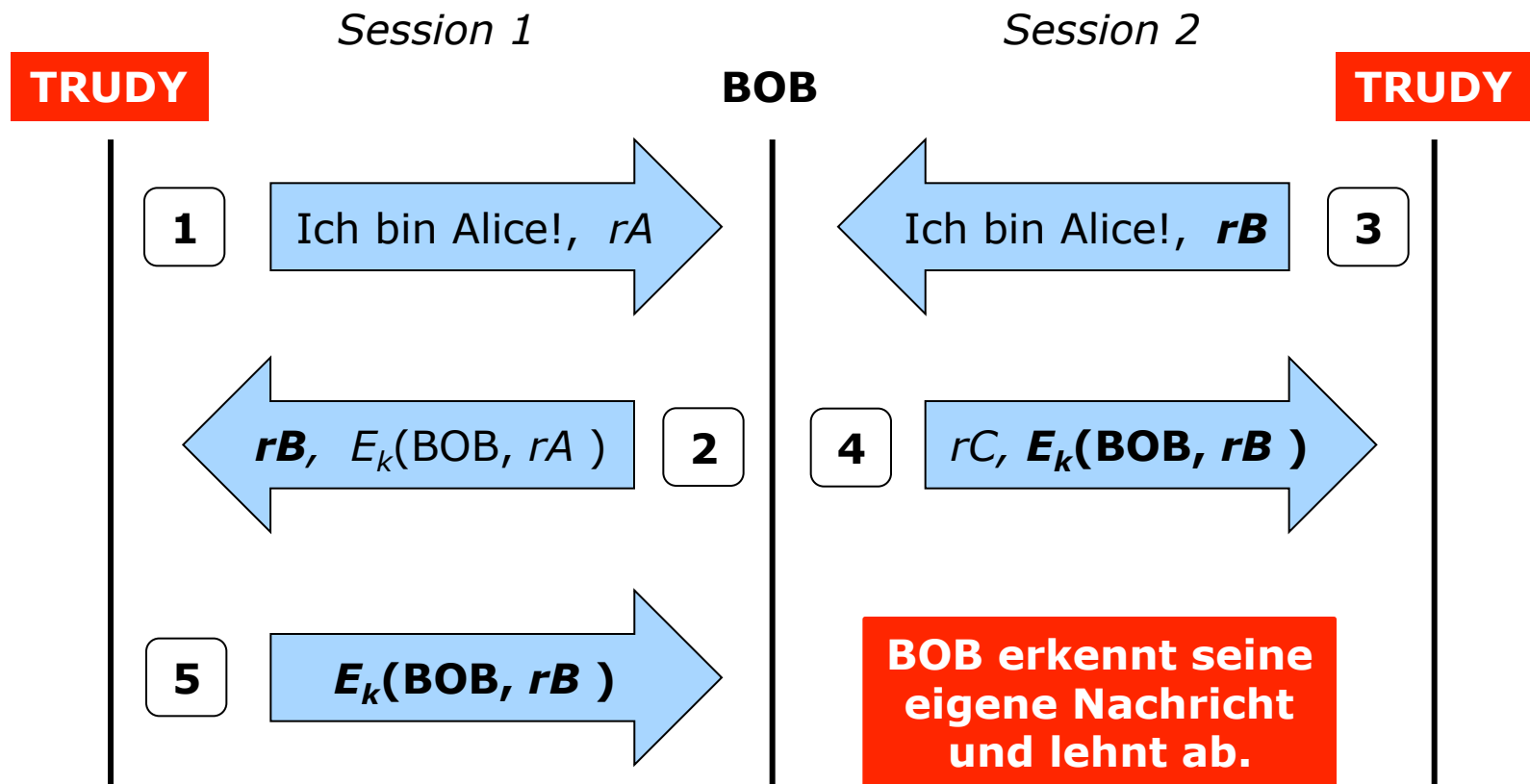
- Teilaufgabe 1: Verschlüsselte Passwortübermittlung (Optional)
  - Welche Schwäche weist dieses Protokoll auf?
  
- 3. Aktiver Angreifer kann sich **als Server ausgeben** und dadurch den Nutzer täuschen (und kann evtl. alle Nachrichten, die danach ausgetauscht werden, mitlesen)



## Aufgabe 3: Authentifizierungsprotokolle

- Teilaufgabe 4: Sichere Challenge-Response-Auth. (Optional)

### Sichere gegenseitige Challenge-Response-Authentisierung



## Aufgabe 5: RSA-Verfahren

- Teilaufgabe 1: Wie funktioniert RSA? Bei Lösung welcher Probleme gilt das RSA-Verfahren als gebrochen? Was ist die häufigste Anwendung in der Praxis? (Optional)
  - Für die Verschlüsselung wird die Nachricht in Zahlenwerte kleiner  $n$  umgewandelt
  - Verschlüsselung eines Zeichens (Block  $i$ )

$$c_i = m_i^e \bmod n$$

- Entschlüsselung von Block  $i$

$$m_i = c_i^d \bmod n$$

$$(m^e)^d = m^{e \cdot d} \equiv m \bmod n \text{ falls } e \cdot d \equiv 1 \bmod \Phi(n)$$

## Aufgabe 5: RSA-Verfahren

- Teilaufgabe 1: Wie funktioniert RSA? Bei Lösung welcher Probleme gilt das RSA-Verfahren als gebrochen? Was ist die häufigste Anwendung in der Praxis? (Optional)

### Schlüsselerzeugung

1. Erzeugung zweier ausreichend großer Primzahlen  $p$  und  $q$
2. Berechnung des RSA-Moduls:  $n = p * q$
3. Erzeugen des Eulerwertes von  $N$ :  $\Phi(n) = (p-1) * (q-1)$
4. Es wird ein  $e$  teilerfremd und kleiner als  $\Phi(n)$  gewählt, d.h.  $\text{ggT}(e, \Phi(n)) = 1$
5. Bestimmung von  $d$  (= multiplikatives Inverses zu  $e$ ):  

$$e * d + k * \Phi(n) = 1$$

(mit dem erweiterten Euklidischen Algorithmus)

## Aufgabe 5: RSA-Verfahren

- Teilaufgabe 1: Wie funktioniert RSA? Bei Lösung welcher Probleme gilt das RSA-Verfahren als gebrochen? Was ist die häufigste Anwendung in der Praxis? (Optional)

### Sicherheit des Verfahrens

- Gegeben einen öffentlichen Schlüssel  $(e, n)$  soll es schwierig sein, auf  $(d, n)$  zu schließen
- Um  $d$  zu berechnen ist Kenntnis der beiden Primzahlen  $p$  und  $q$  notwendig ( $\Phi(n)$ )

→ Angriff durch Primfaktorzerlegung von  $n$  (zwei Primfaktoren)

### „Faktorisierungsannahme“:

- Primfaktorzerlegung großer Zahlen ist äußerst aufwändig
- derzeit gelten RSA-Schlüssel mit einer Länge ab 2048 bit als sicher

## Aufgabe 5: RSA-Verfahren

- Teilaufgabe 1: Wie funktioniert RSA? Bei Lösung welcher Probleme gilt das RSA-Verfahren als gebrochen? Was ist die häufigste Anwendung in der Praxis? (Optional)

### Sicherheit des Verfahrens (Zusatz)

- Die Sicherheit des geheimen Schlüssels bedingt noch nicht die Sicherheit des RSA-Verfahrens selbst
- Effizientes Ziehen der  $e$ -te Wurzel bricht RSA
- Unbekannt:  $e$ -te Wurzel ziehen ohne geheimen Schlüssel möglich?

### Stand der Forschung

- Ob Faktorisierung wirklich schwierig ist, ist unbekannt
- Wer aus dem öffentlichen Schlüssel den geheimen Schlüssel berechnen kann, kann auch faktorisieren
- Ziehen der  $e$ -ten Wurzel für kleines  $e$  vmtl. einfacher als Faktorisierung (einfacher  $\neq$  einfach!)

## Aufgabe 5: RSA-Verfahren

- Teilaufgabe 2: Entschlüsseln Sie den gegebenen Schlüsseltext, unter Verwendung der Basiswerte  $p = 271$ ,  $q = 379$ ,  $e = 47$ . (Pflicht)
  - $\Phi(n) = (p-1) * (q-1) = 270 * 378 = 102060$

$$\begin{aligned} e \cdot d &\equiv 1 \pmod{\Phi(n)} \\ e \cdot d + k \cdot \Phi(n) &= 1 \\ 67 \cdot d + k \cdot 102060 &= 1 \end{aligned}$$

**Hier nur Teilproblem  
„d ermitteln“  
dargestellt**

Euklidischer Algorithmus zur Bestimmung des ggT

$$\begin{aligned} 102060 &= 2171 \cdot 47 + 23 \\ 47 &= 2 \cdot 23 + 1 \\ 23 &= 23 \cdot 1 + 0 \end{aligned}$$

$$\text{ggT}(102060, 47) = 1$$

Erweiterter Euklidischer Algorithmus

$$\begin{aligned} 1 &= 47 - 2 \cdot 23 \\ &= 47 - 2 \cdot (102060 - 2171 \cdot 47) \\ &= 1 \cdot 47 - 2 \cdot 102060 + (2 \cdot 2171) \cdot 47 \\ &= 4343 \cdot 47 - 2 \cdot 102060 \end{aligned}$$

$$47^{-1} \equiv 4343 \pmod{102060}$$

## Aufgabe 5: RSA-Verfahren

- Teilaufgabe 2: Entschlüsseln Sie den gegebenen Schlüsseltext, unter Verwendung der Basiswerte  $p = 271$ ,  $q = 379$ ,  $e = 47$ . (Pflicht)

- Ergebnis:

**Fuer die GSS-Klausur sind folgende Themen wichtig:  
Angreifermodelle, Schutzziele, Rainbow Tables, die  
(Un-)Sicherheit von Passwoertern und dazugehoerige  
Angriffe, Zugangs- und Zugriffskontrolle, Timing-Attack  
und Power-Analysis, Biometrische Verfahren, Grundlagen  
der Kryptographie, das RSA-Verfahren,  
Authentifikationsprotokolle und natuerlich alle anderen  
Inhalte, die wir in der Uebung und der Vorlesung  
behandelt haben :-)**