fhwedel
UNIVERSITY OF APPLIED SCIENCES

Grundbegriffe der Kryptographie II

Technisches Seminar SS 2012

Deniz Bilen

Agenda

fhwedel
UNIVERSITY OF APPLIED SCIENCES

1. Kerckhoff‘sches Prinzip
2. Kommunikationsszenario
3. Wichtige Begriffe
4. Sicherheitsmechanismen
    1. Symmetrische Verschlüsselung
    2. Asymmetrische Verschlüsselung
    3. Hybride Verschlüsselung
5. Methoden der Kryptoanalyse
6. Quellen

Agenda

fhwedel
UNIVERSITY OF APPLIED SCIENCES

1. Kerckhoff‘sches Prinzip
2. Kommunikationsszenario
3. Wichtige Begriffe
4. Sicherheitsmechanismen
    1. Symmetrische Verschlüsselung
    2. Asymmetrische Verschlüsselung
    3. Hybride Verschlüsselung
5. Methoden der Kryptoanalyse
6. Quellen

1. Kerckhoffs‘sches Prinzip

fhwedel
UNIVERSITY OF APPLIED SCIENCES

Auguste Kerckhoffs (1835-1903) revolutionierte die Kryptographie

Das Kerckhoffs‘ Prinzip besagt:

- Der Verschlüsselungsalgorithmus darf nicht geheim gehalten werden
- Der Schlüssel muss geheim bleiben

Algorithmen konnten fortan öffentlich von Experten diskutiert werden

1. Kerckhoffs‘sches Prinzip

Ein sicheres Kryptosystem muss 6 Grundsätze befolgen:

1. Das System muss im Wesentlichen (…) unentzifferbar sein
2. Das System darf keine Geheimhaltung erfordern (…)
3. Es muss leicht übermittelbar sein und man muss sich die Schlüssel ohne schriftliche Aufzeichnung merken können (…)
4. Das System sollte mit telegraphischer Kommunikation kompatibel sein
5. Das System muss transportabel sein und die Bedienung darf nicht mehr als eine Person erfordern
6. Das System muss einfach anwendbar sein (…)

Zur Kerckhoffs‘ Zeit gab es solches System nicht

1. Kerckhoffs‘sches Prinzip

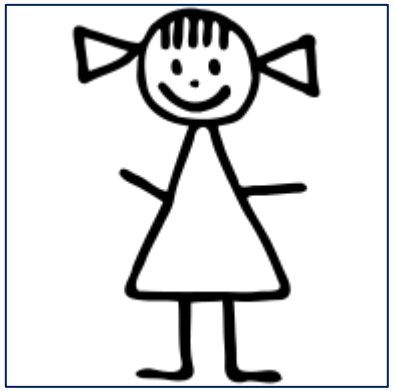
Einige Gründe warum Kerckhoffs‘ Prinzip die Kryptographie revolutioniert hat:

- Einen Algorithmus geheim zu halten ist schwerer, als einen Schlüssel
- Kompromittierte Algorithmen sind schwer zu ersetzen, Schlüssel hingegen einfach
- Algorithmen können durch Reverse-Engineering rekonstruiert werden
- Öffentliche Diskussionen über Algorithmen führen durch Fehlerentdeckungen zu erhöhter Sicherheit und Verbesserung der Kryptosysteme

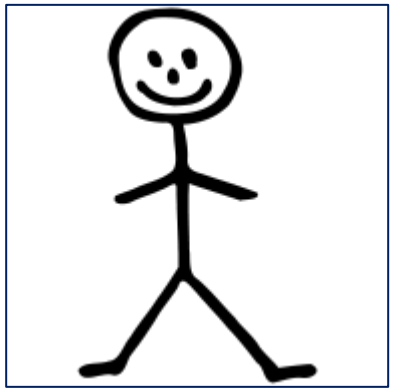
Agenda

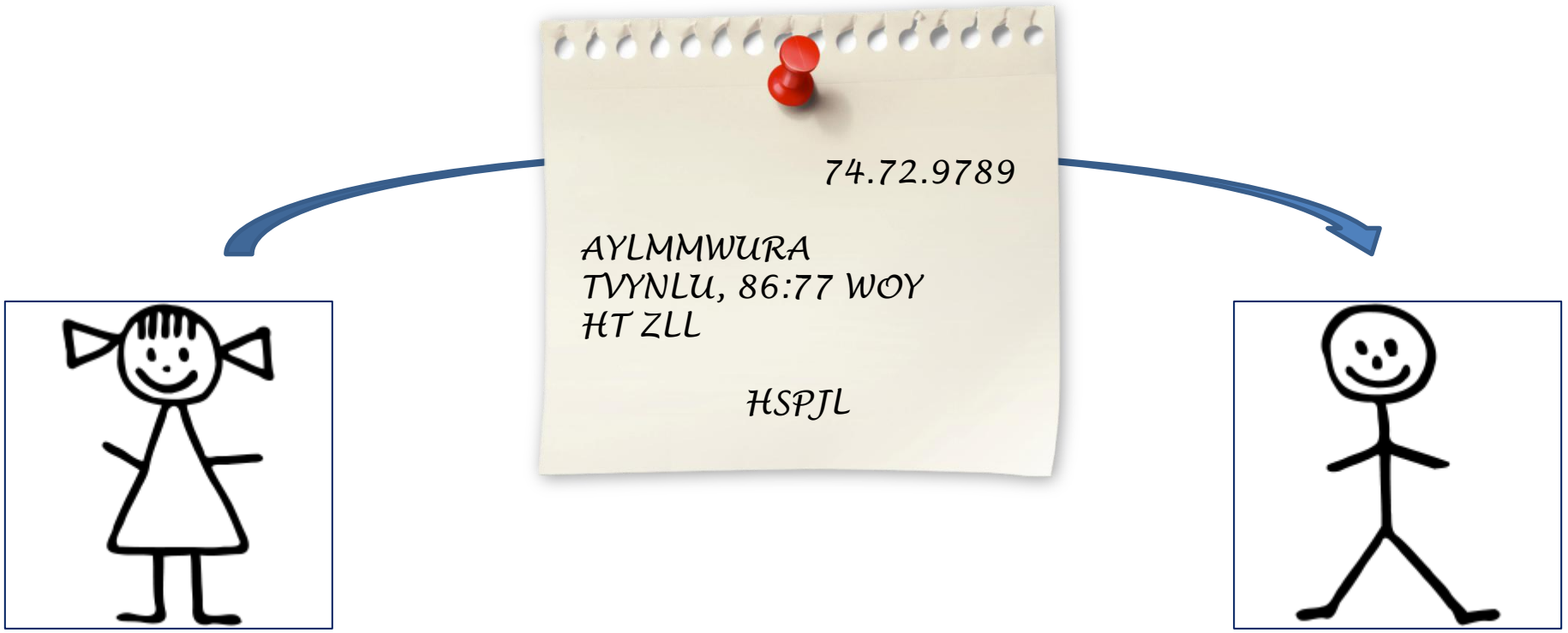
fhwedel
UNIVERSITY OF APPLIED SCIENCES

1. Kerckhoff‘sches Prinzip
2. Kommunikationsszenario
3. Wichtige Begriffe
4. Sicherheitsmechanismen
    1. Symmetrische Verfahren
    2. Asymmetrische Verschlüsselung
5. Methoden der Kryptoanalyse
6. Quellen



Alice möchte mit Bob auf geheimen Wege kommunizieren, weil sie nicht möchte, dass andere den Inhalt ihrer Nachricht mitbekommen

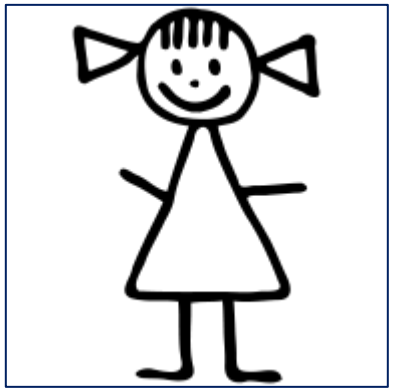


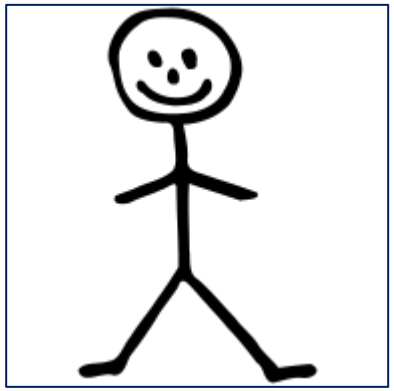


1. Alice pinnt eine Notiz an Bobs Pinnwand

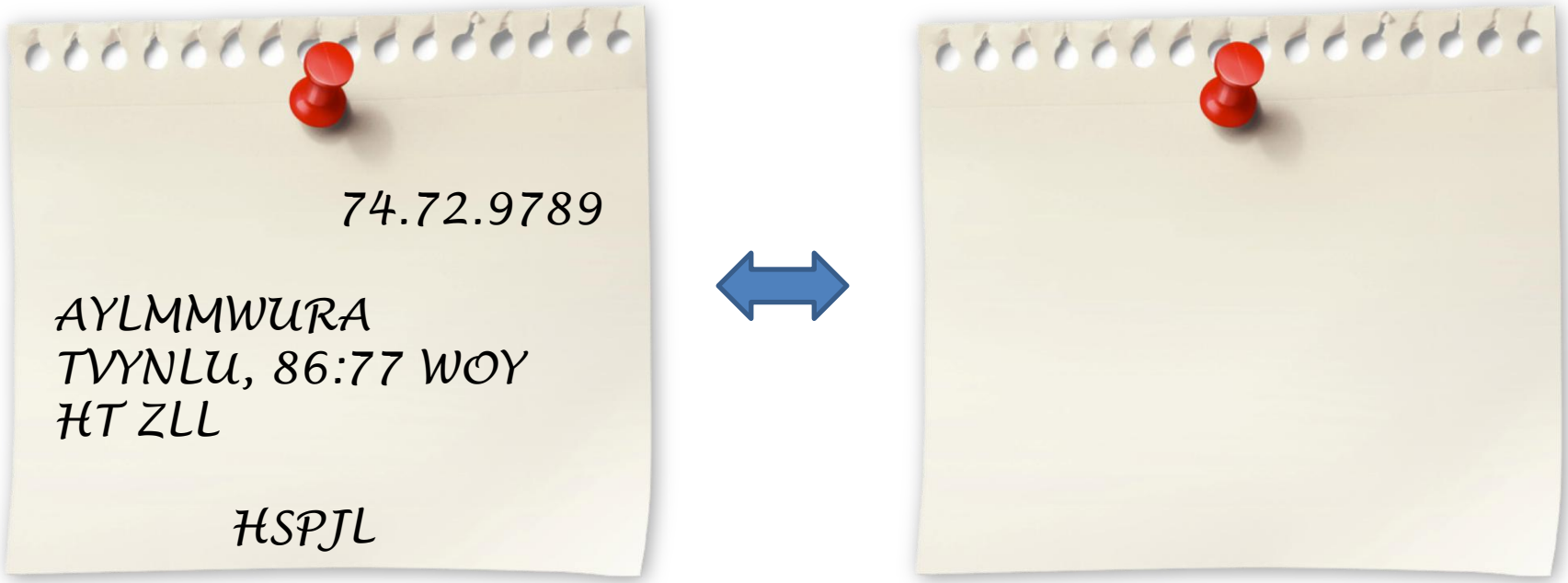
fhwedel
UNIVERSITY OF APPLIED SCIENCES

2. Alice schreibt Bob eine SMS

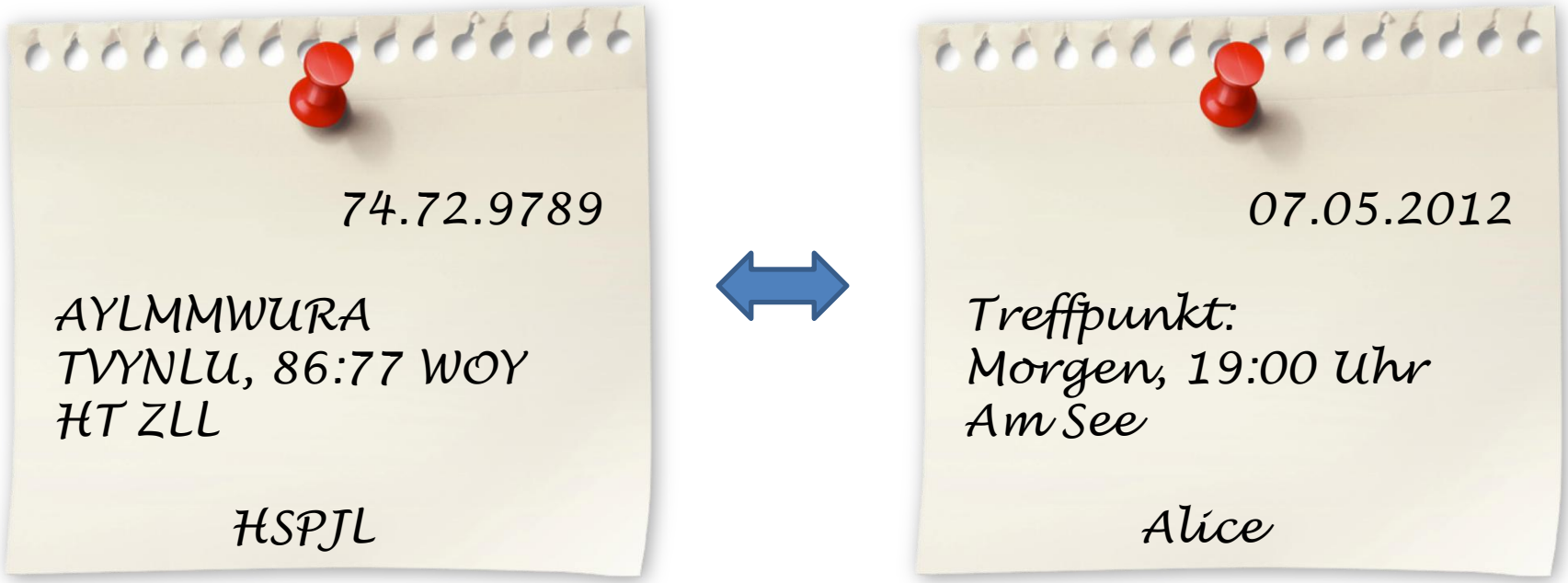




Mit Kenntnis des Schlüssels C7 ist die Nachricht sehr einfach zu entschlüsseln



Mit Kenntnis des Schlüssels C7 ist die Nachricht sehr einfach zu entschlüsseln



Jeder Buchstabe wurde durch den 7. Nachfolger im Alphabet substituiert.
Diese Verschlüsselungsmethode nennt man Caesar-Chiffre.

Agenda

fhwedel
UNIVERSITY OF APPLIED SCIENCES

1. Kerckhoff‘sches Prinzip
2. Zeitreise durch die Geschichte der Kryptographie ab 19. Jahrhundert
3. Kommunikationsszenario
4. Wichtige Begriffe
5. Sicherheitsmechanismen
    1. Symmetrische Verschlüsselung
    2. Asymmetrische Verschlüsselung
    3. Hybride Verschlüsselung
6. Methoden der Kryptoanalyse

3. Wichtige Begriffe

Klartext / plaintext

Geheimtext / ciphertext

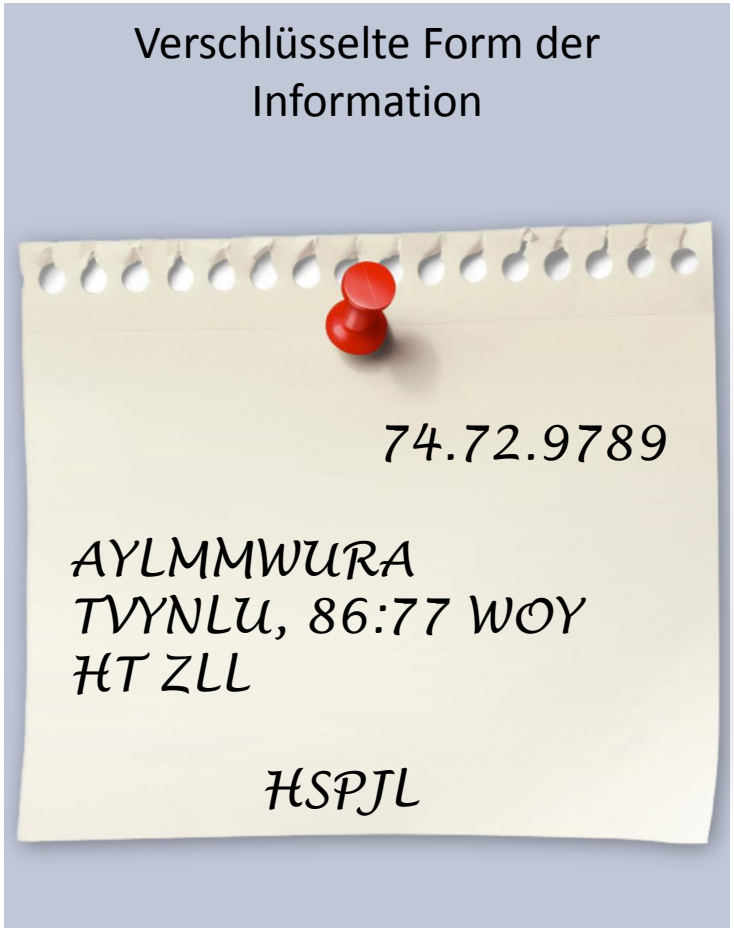
Schlüssel / key

3. Wichtige Begriffe

Klartext / plaintext

Geheimtext / ciphertext

Schlüssel / key



3. Wichtige Begriffe

Klartext / plaintext

Geheimtext / ciphertext

Schlüssel / key

Entscheidende Information für die Entschlüsselung des Geheimtextes

Agenda

fhwedel
UNIVERSITY OF APPLIED SCIENCES

1. Kerckhoff‘sches Prinzip
2. Kommunikationsszenario
3. Wichtige Begriffe
4. Sicherheitsmechanismen
    1. Symmetrische Verfahren
    2. Asymmetrische Verschlüsselung
    3. Hybride Verschlüsselung
5. Methoden der Kryptoanalyse
6. Quellen

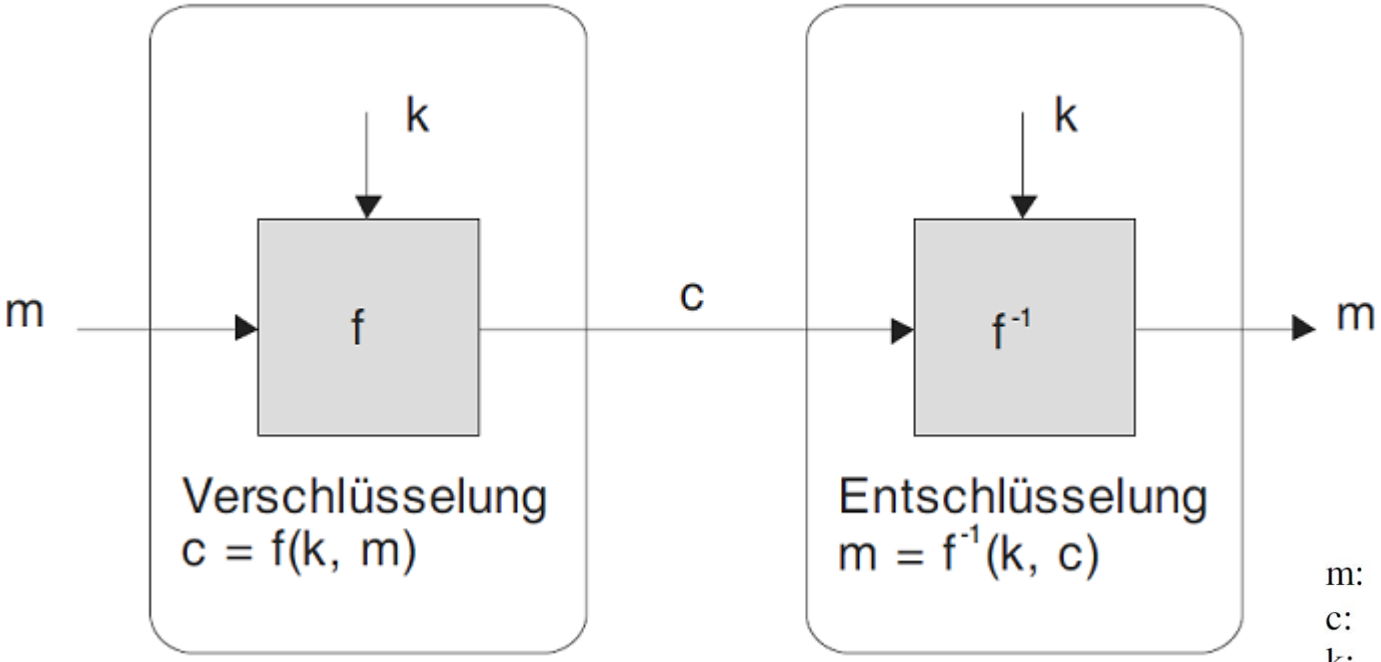
4. Sicherheitsmechanismen

Man unterscheidet hier zwischen:

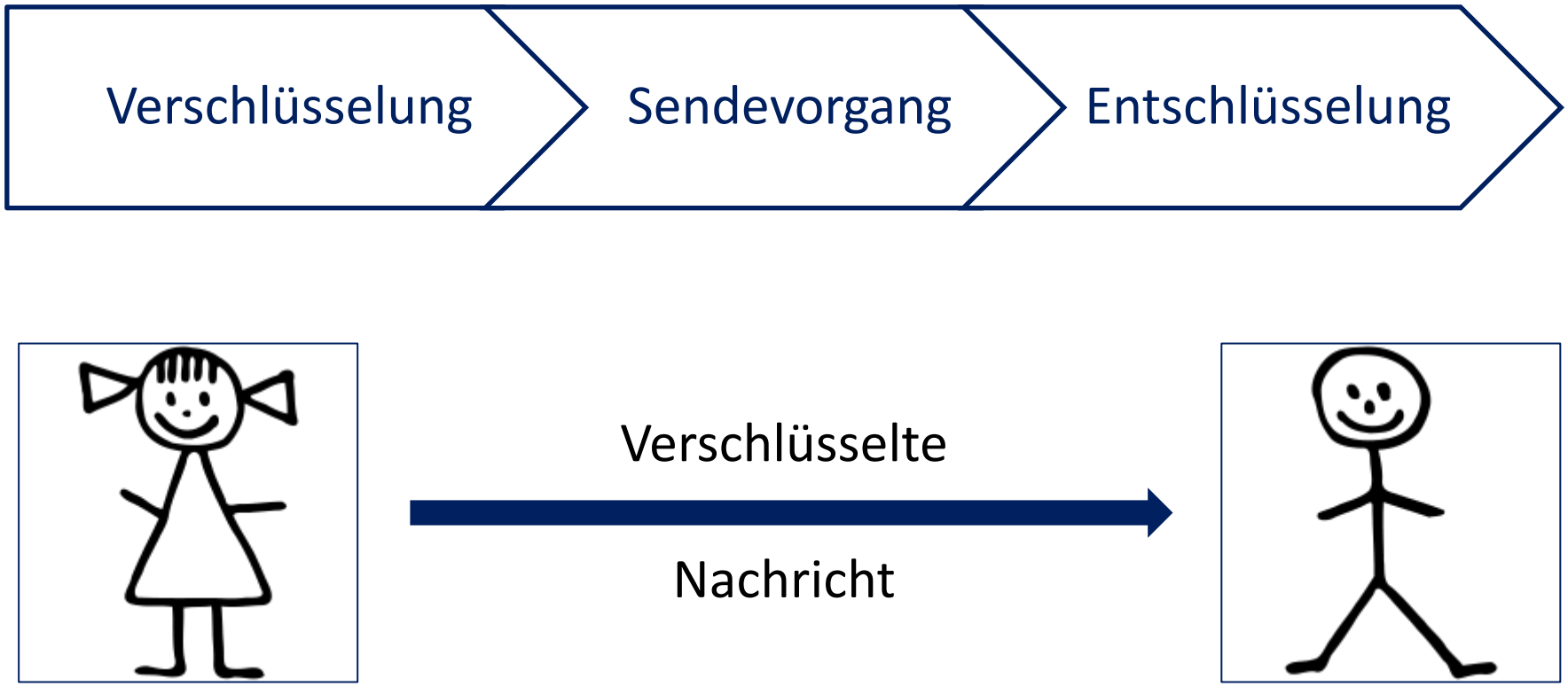
Symmetrischen,
Asymmetrischen
und
Hybriden Verfahren

fhwedel
UNIVERSITY OF APPLIED SCIENCES

Jede Ver- und Entschlüsselung besitzt einen Schlüssel **k**

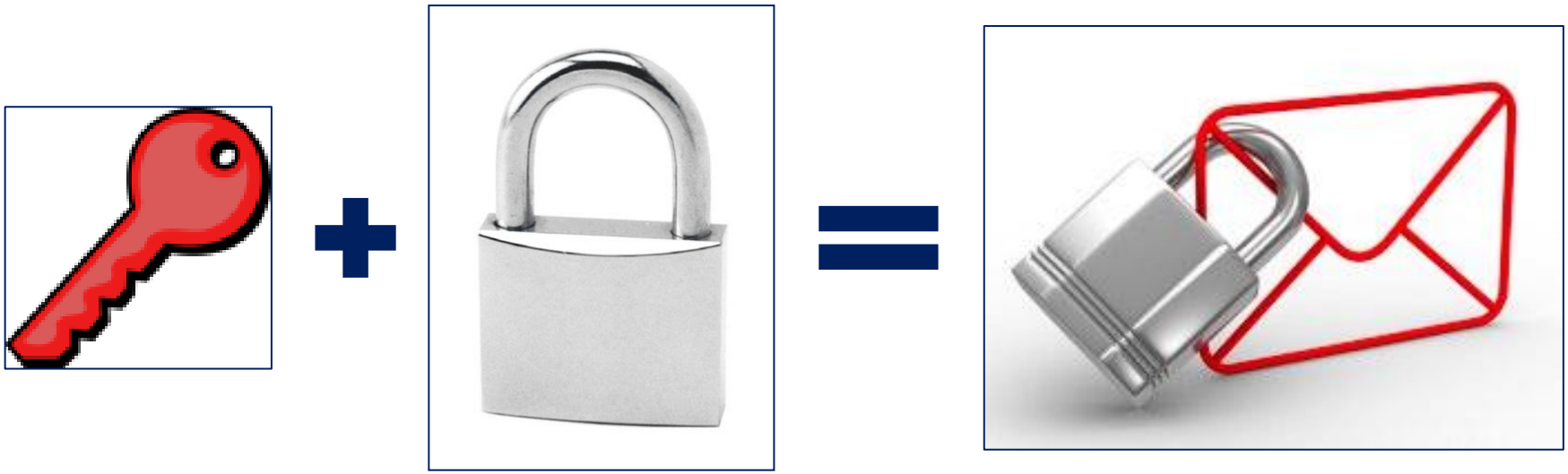


m:	Klartext-Nachricht
c:	Chiffretext-Nachricht
k:	Schlüssel
f:	Verschlüsselungsfunktion
f^{-1}:	Entschlüsselungsfunktion


Verschlüsselung
Sendevorgang
Entschlüsselung
Verschlüsselte
Nachricht

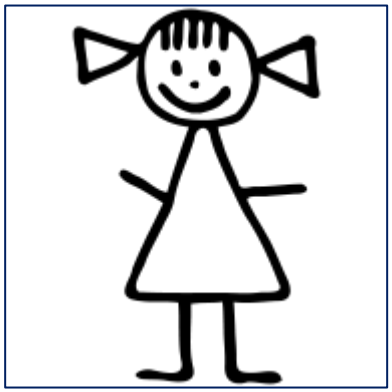
fhwedel
UNIVERSITY OF APPLIED SCIENCES

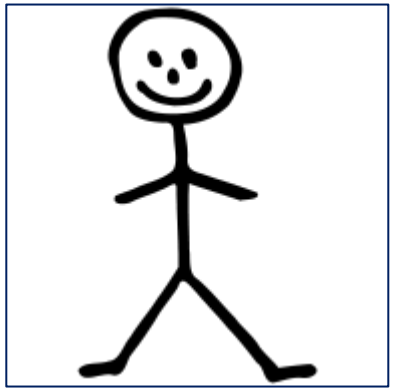
Verschlüsselung | Sendevorgang | Entschlüsselung



fhwedel
UNIVERSITY OF APPLIED SCIENCES

Verschlüsselung | Sendevorgang | Entschlüsselung



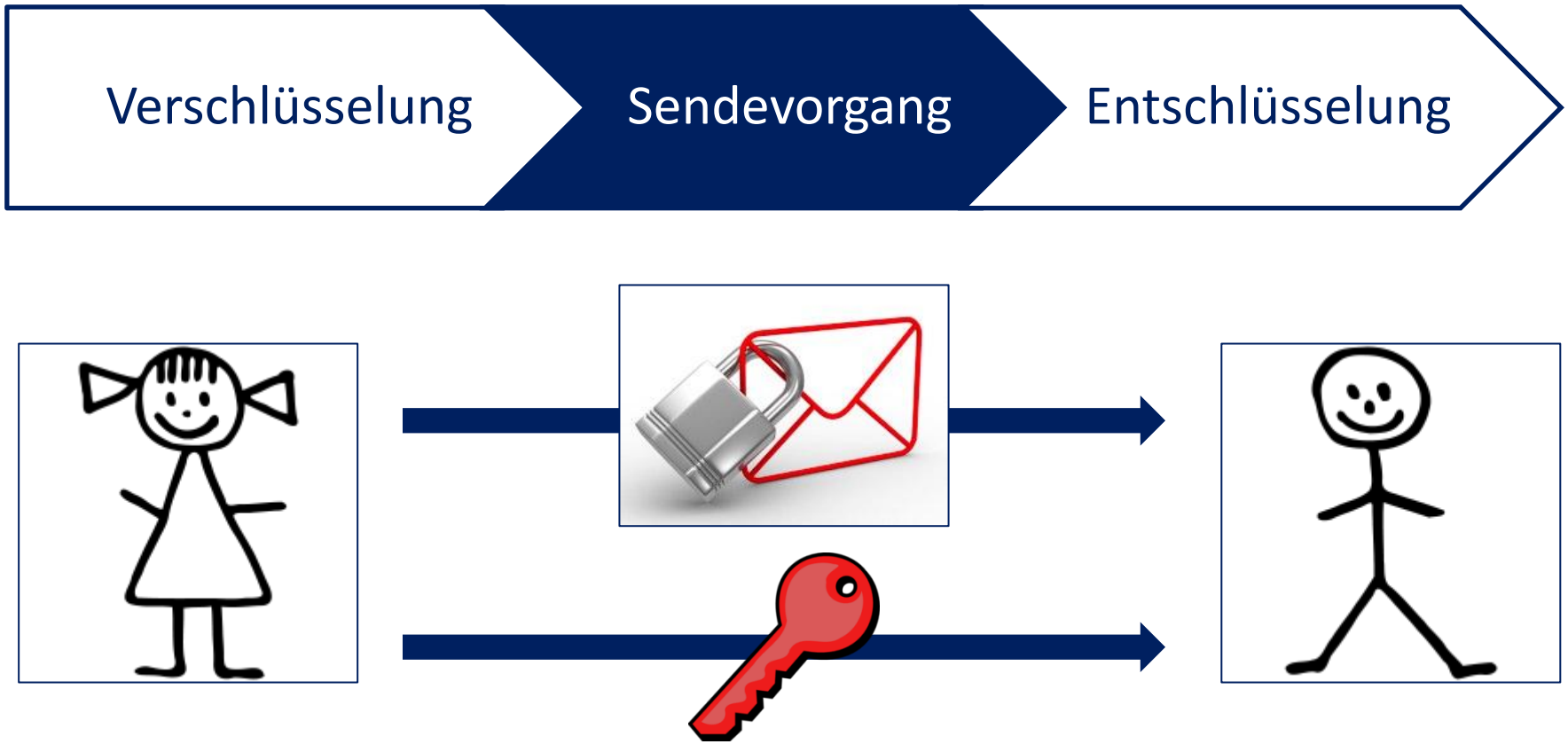


fhwedel
UNIVERSITY OF APPLIED SCIENCES

Verschlüsselung → Sendevorgang → **Entschlüsselung**

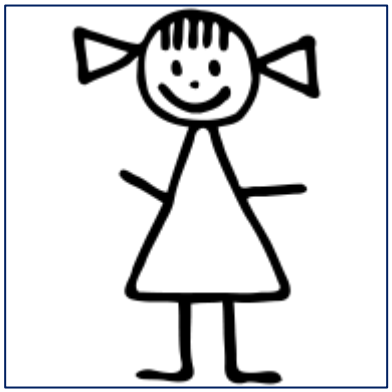
fhwedel
UNIVERSITY OF APPLIED SCIENCES

Verschlüsselung → Sendevorgang → Entschlüsselung


Verschlüsselung
Sendevorgang
Entschlüsselung

fhwedel
UNIVERSITY OF APPLIED SCIENCES

V[illegible]devorgang Entschlüsselung

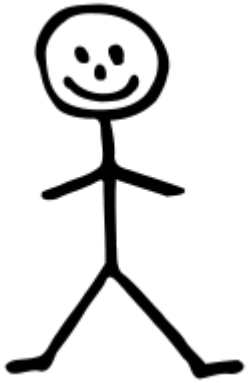


UNSICHER

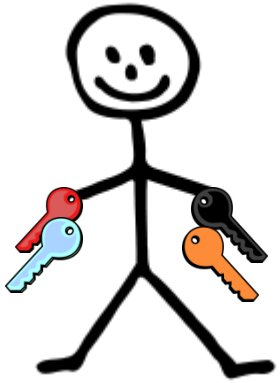
fhwedel
UNIVERSITY OF APPLIED SCIENCES

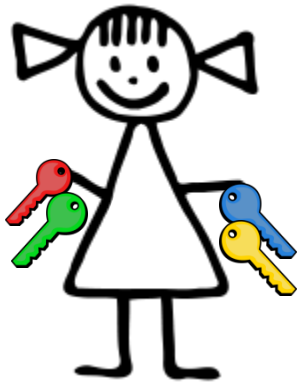
Verschlüsselung | Sendevorgang | Entschlüsselung

Der symmetrische Schlüssel muss auf einem sicheren Kanal mitgesendet werden

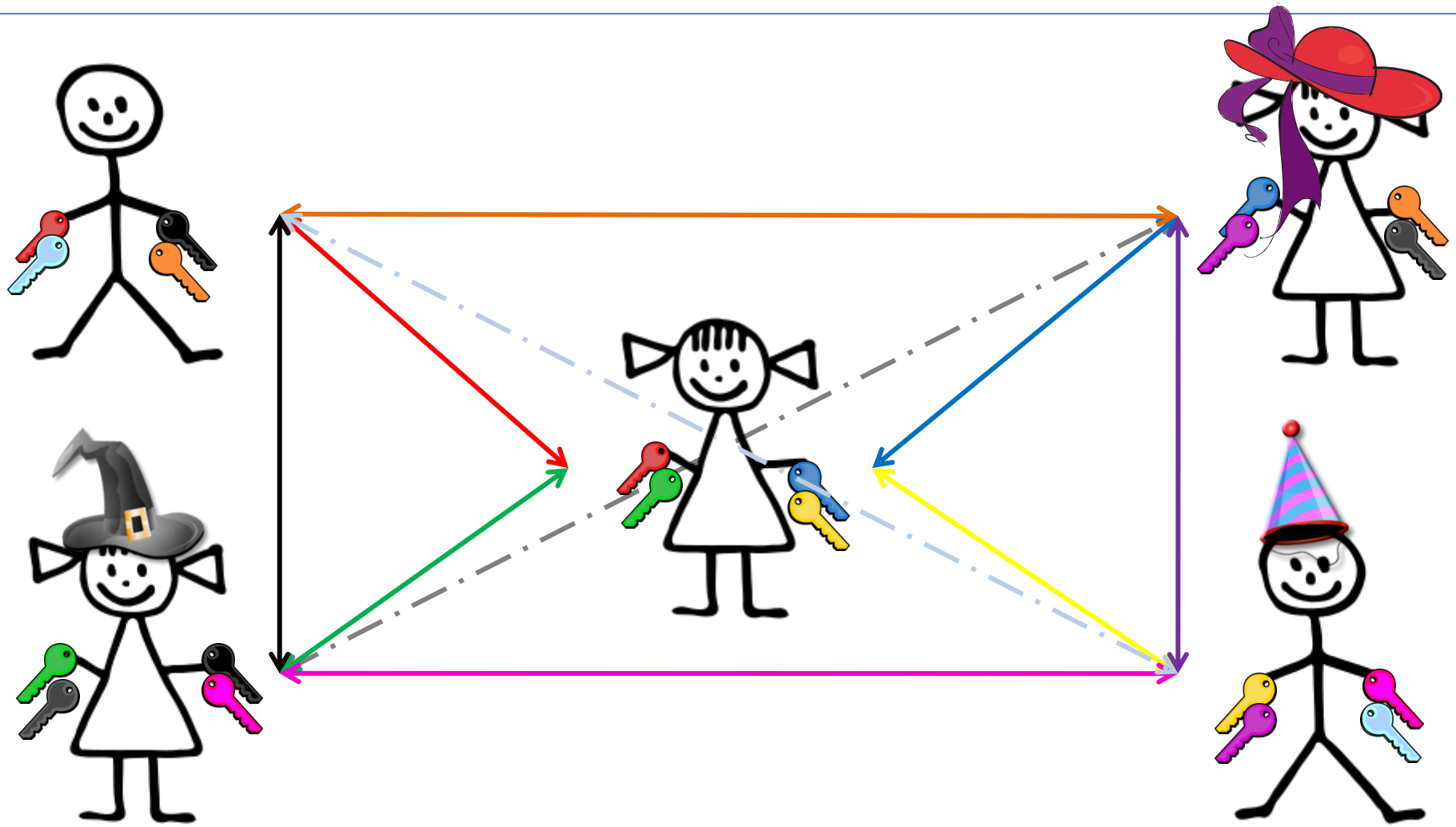


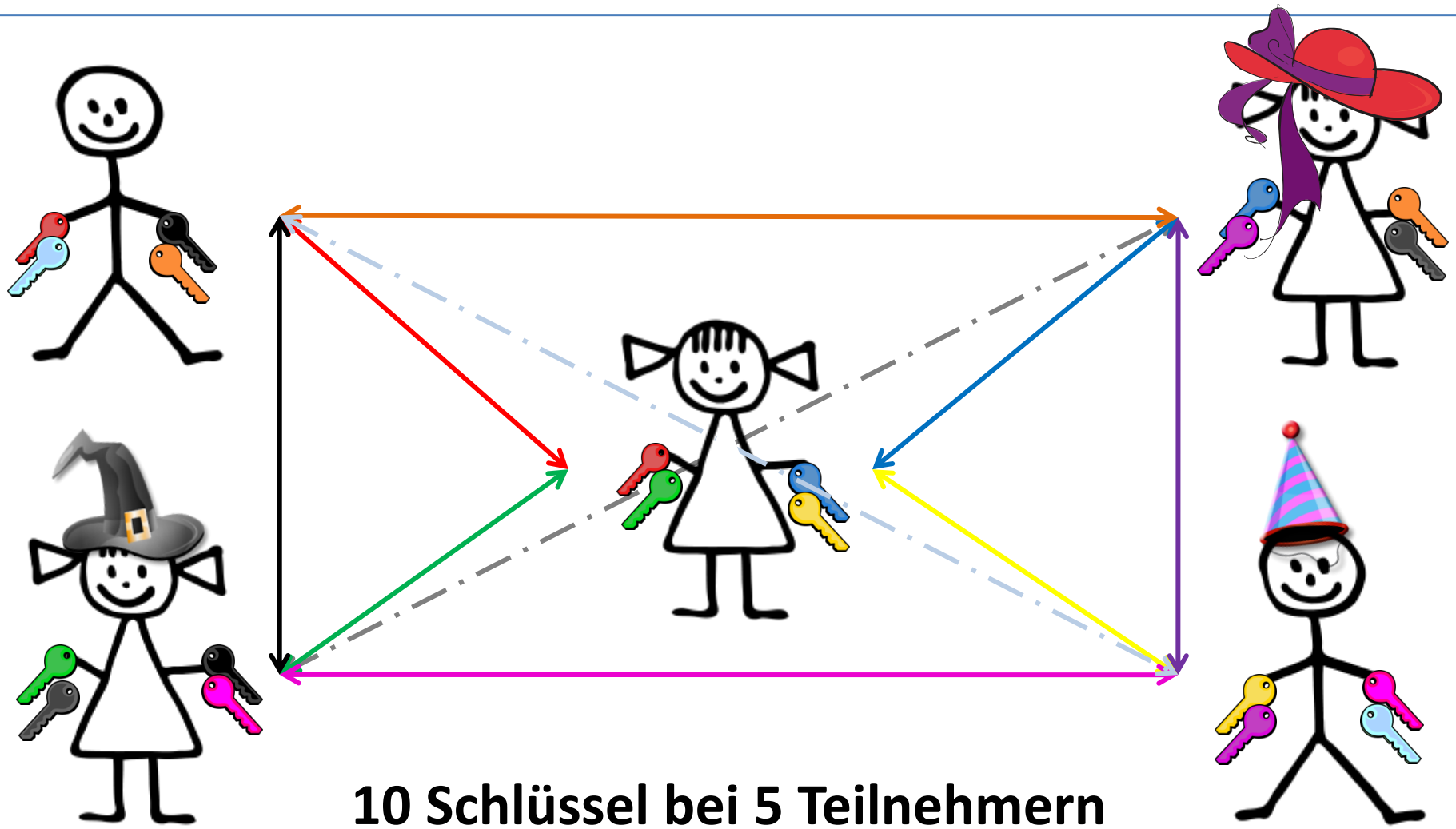
fhwedel
UNIVERSITY OF APPLIED SCIENCES



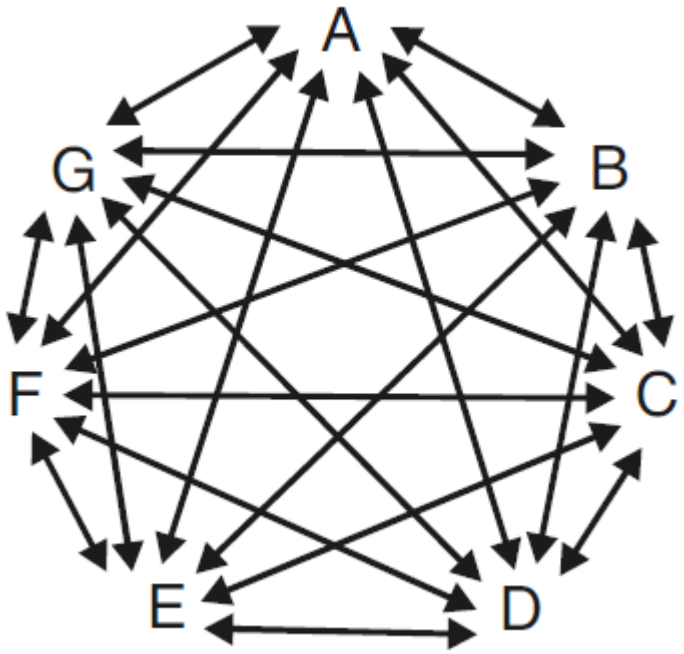


fhwedel
UNIVERSITY OF APPLIED SCIENCES



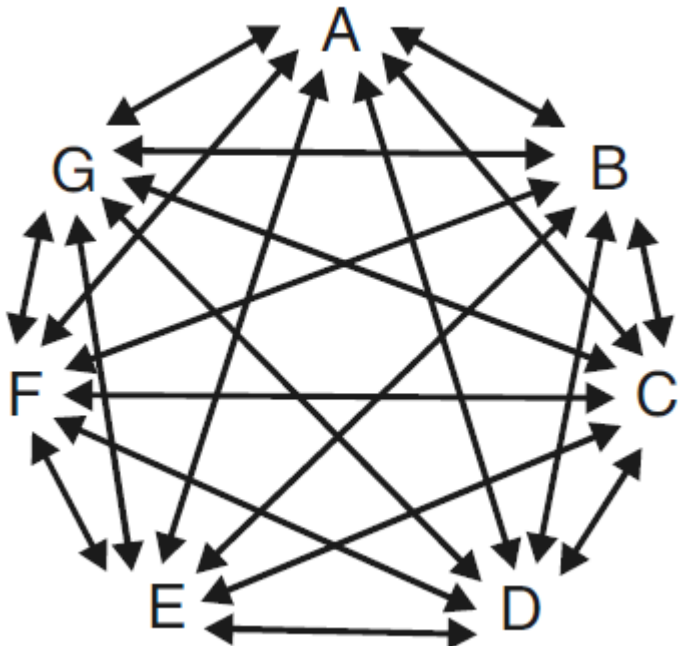


10 Schlüssel bei 5 Teilnehmern



7 Teilnehmer ergeben schon eine enorme Anzahl von Schlüssel

Wie viele Schlüssel benötigt man für die Kommunikation zwischen 1000 Teilnehmer?



7 Teilnehmer ergeben schon eine enorme Anzahl von Schlüssel

Wie viele Schlüssel benötigt man für die Kommunikation zwischen 1000 Teilnehmer?

Ca. eine halbe Millionen

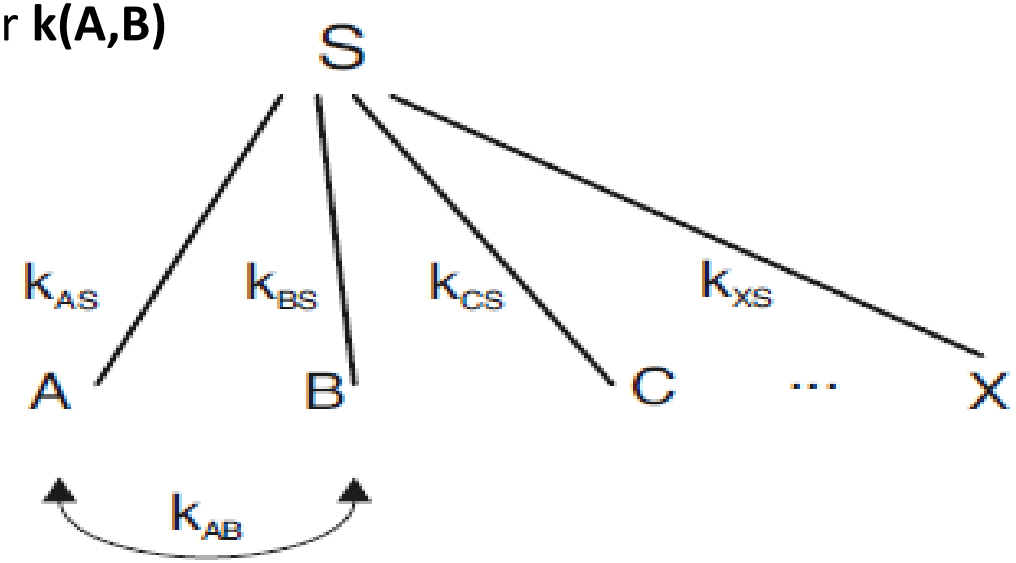
Anzahl der symmetrischen Schlüssel

$$\binom{N}{2} = \frac{N \cdot (N-1)}{2}$$

Problem: Verwaltung von symmetrischen Schlüsseln ist unmöglich handzuhaben

Lösung: Sichere Instanz **S**, erstellt und vergibt Schlüsselpaare erst bei Bedarf (TTP, Trust Third Party)

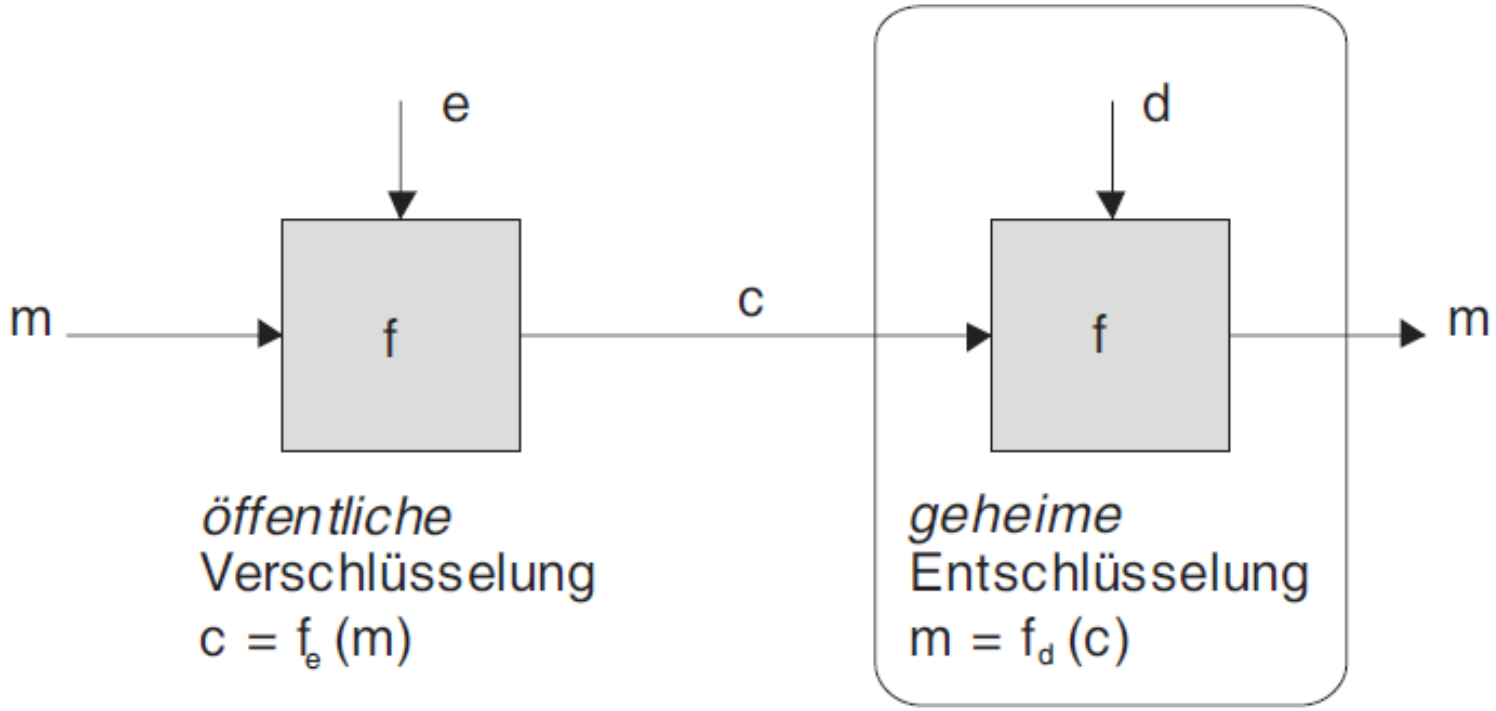
Auf die Initiative von **Alice** mit **Bob** kommunizieren zu wollen, erstellt **S** das Schlüsselpaar **k(A,B)**



Agenda

fhwedel
UNIVERSITY OF APPLIED SCIENCES

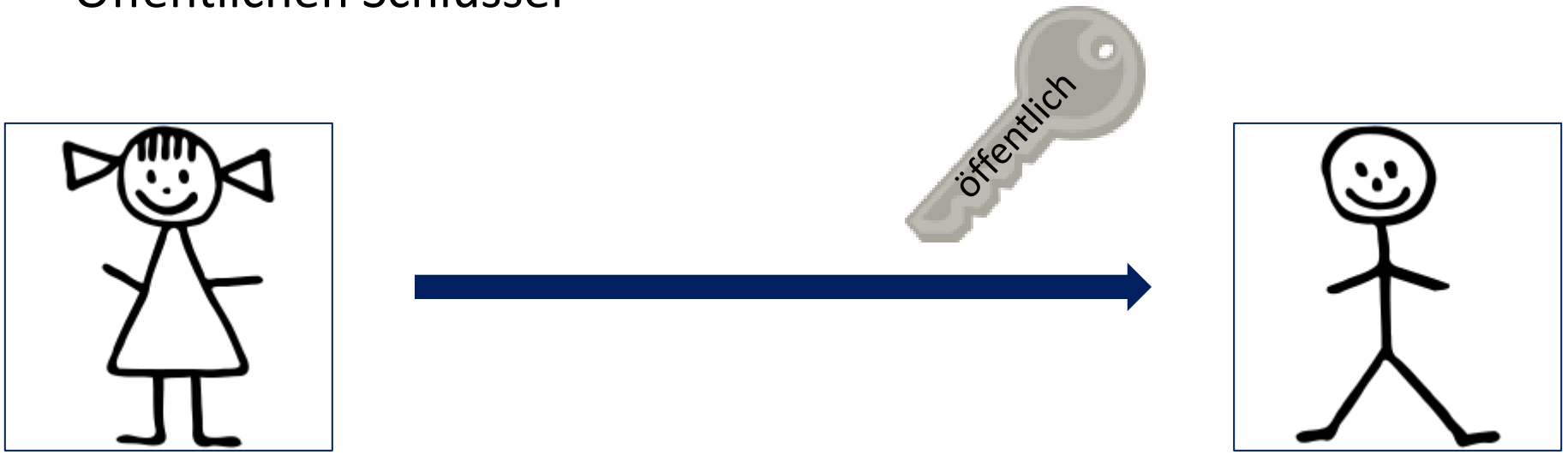
1. Kerckhoff‘sches Prinzip
2. Kommunikationsszenario
3. Wichtige Begriffe
4. Sicherheitsmechanismen
    1. Symmetrische Verschlüsselung
    2. Asymmetrische Verschlüsselung
    3. Hybride Verschlüsselung
5. Methoden der Kryptoanalyse
6. Quellen



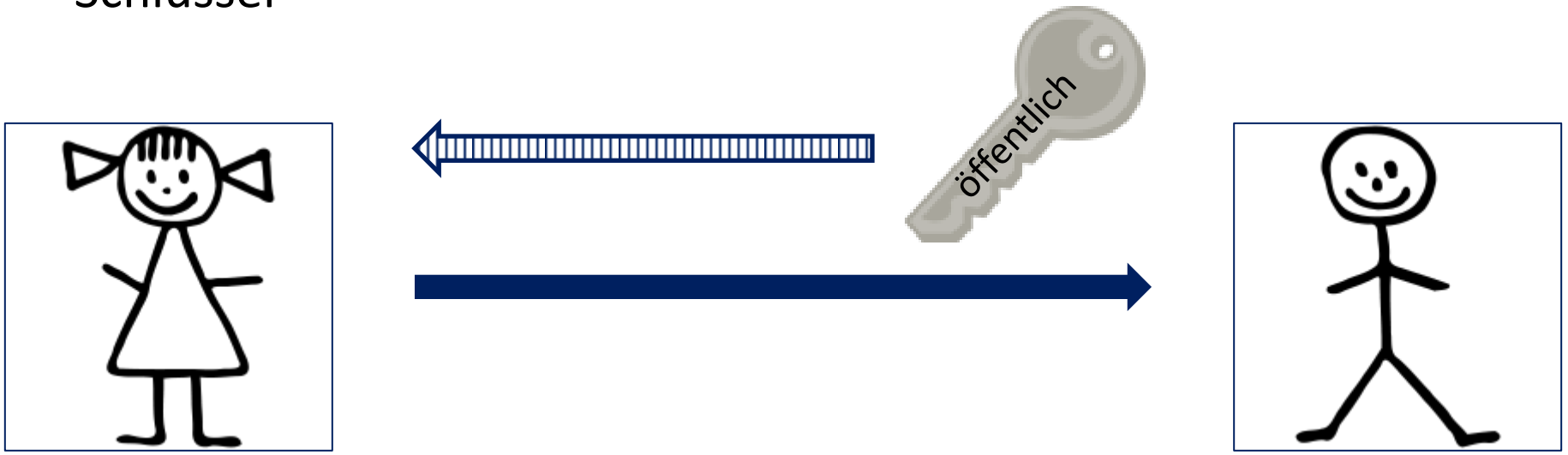
m: Klartext-Nachricht
c: Chiffretext-Nachricht
e: öffentlicher Verschlüsselungs-Schlüssel
d: privater Entschlüsselungs-Schlüsssel
f: Verschlüsselungs- und Entschlüsselungsfunktion

Alice möchte erneut mit Bob kommunizieren und ihm eine Nachricht übermitteln

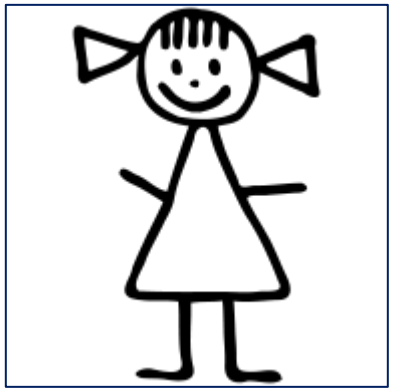
Um die Nachricht verschlüsseln zu können, braucht Alice Bobs Öffentlichen Schlüssel



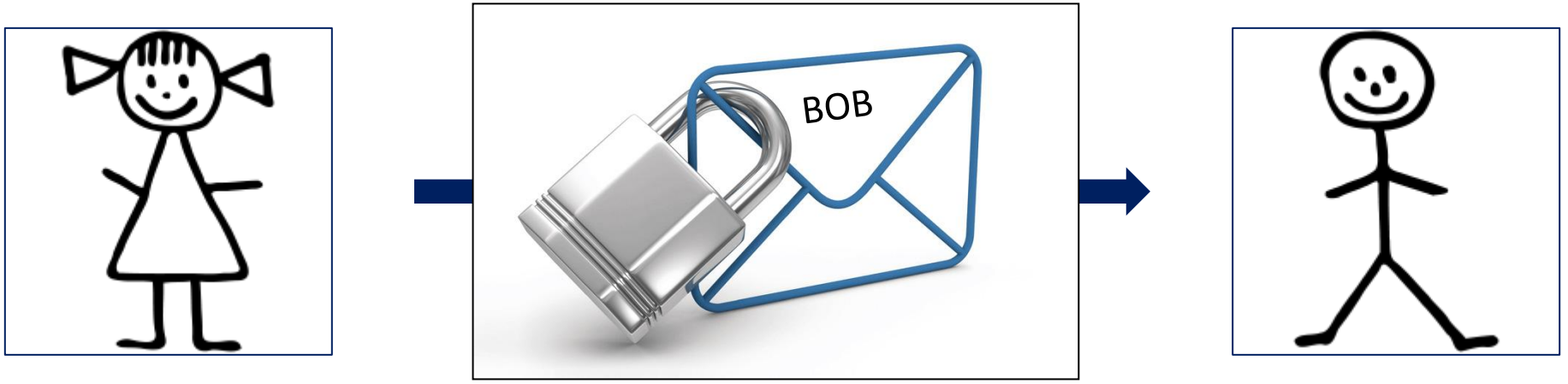
Dafür beschafft sich Alice einfach Bobs öffentlich zugänglichen Schlüssel



Mit Bobs öffentlichem Schlüssel verschlüsselt Alice nun die Nachricht an Bob

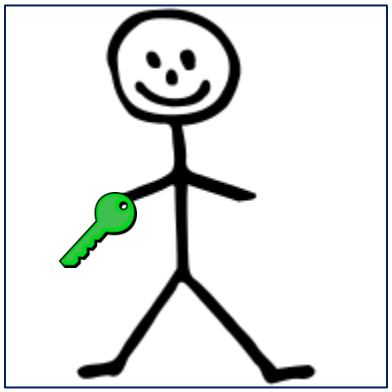


Die verschlüsselte Nachricht wird anschließend einfach an Bob verschickt



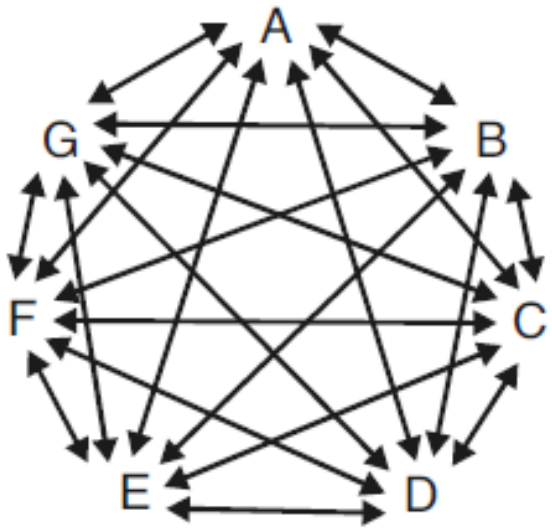
Wie kann die Nachricht sicher verschlüsselt sein, wenn jeder Zugang zu Bobs öffentlichen Schlüssel hat?

Hier kommt Bobs privater Schlüssel zur Geltung



Nur Bobs privater Schlüssel ist in der Lage, die durch seinen öffentlichen Schlüssel verschlüsselte Nachricht zu entschlüsseln

Fazit: Bei der asymmetrischen Verschlüsselung sind deutlich weniger Schlüssel notwendig



symmetrische Schlüssel

e_A, d_A

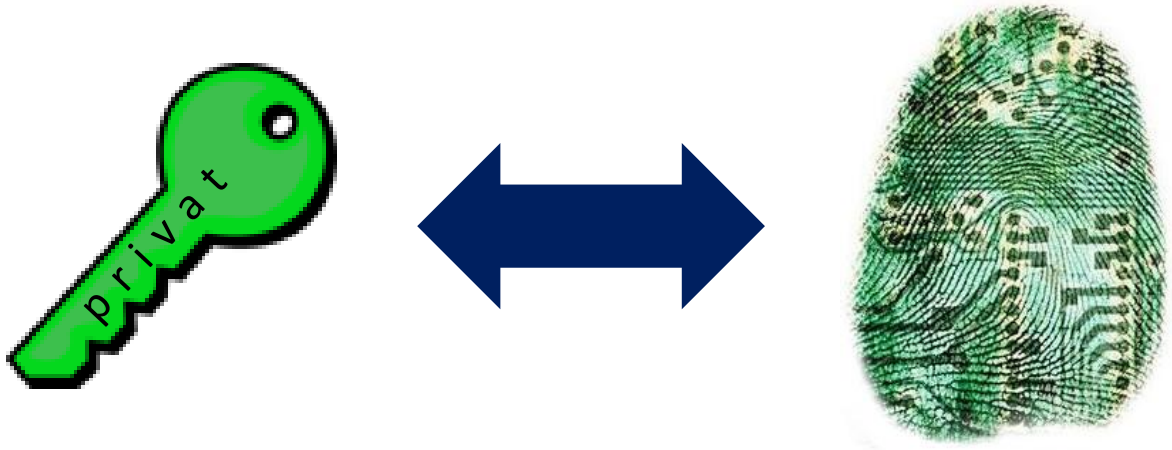
e_G, d_G e_B, d_B

e_F, d_F e_C, d_C

e_E, d_E e_D, d_D

asymmetrische Schlüssel

Der **private Schlüssel** bei asymmetrischer Verschlüsselung bietet weiterhin die Möglichkeit zur Authentifizierung



Der private Schlüssel von Bob ist ihm eindeutig zuzuordnen und gleicht daher einem **digitalen Fingerabdruck**

Agenda

fhwedel
UNIVERSITY OF APPLIED SCIENCES

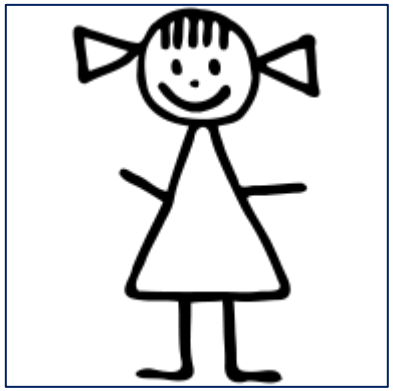
1. Kerckhoff‘sches Prinzip
2. Zeitreise durch die Geschichte der Kryptographie ab 19. Jahrhundert
3. Kommunikationsszenario
4. Wichtige Begriffe
5. Sicherheitsmechanismen
    1. Symmetrische Verschlüsselung
    2. Asymmetrische Verschlüsselung
    3. Hybride Verschlüsselung
6. Methoden der Kryptoanalyse

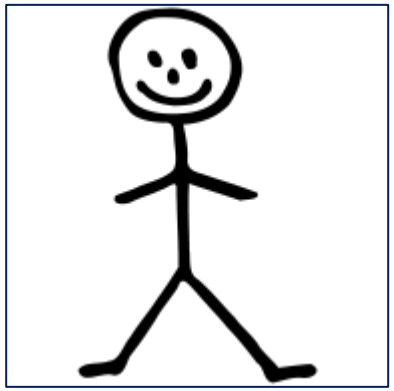
fhwedel
UNIVERSITY OF APPLIED SCIENCES

	Symmetrisch	Asymmetrisch
Schlüsselmenge	Groß	Klein
Geschwindigkeit	Schnell	Langsam
Sicherheit	Gering	Hoch
Authentifizierung	Nein	Ja
Datenmenge	Groß	Klein

Hybride Verfahren

Alice möchte erneut mit Bob kommunizieren und ihm eine Nachricht übermitteln, diesmal per **Hybrid-Verschlüsselung**.

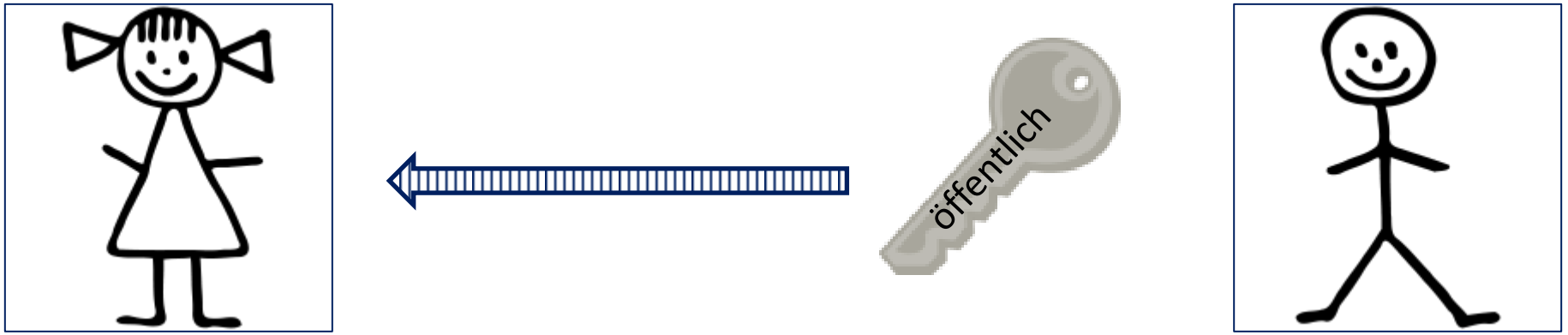




Für die Verschlüsselung wird ein symmetrischer Schlüssel k(A,B) erzeugt.

Mit diesem wird die Nachricht m verschlüsselt (**symmetrische Verschlüsselung**)

Jetzt beschafft sich Alice wieder den öffentlichen Schüssel von Bob, wie bei der asymmetrischen Verschlüsselung



Mit dem öffentlichen Schlüssel von Bob verschlüsselt Alice nun den symmetrischen Schlüssel k(A,B)

Jetzt werde der verschlüsselte symmetrische Schlüssel k(A,B) und die mittels k(A,B) verschlüsselte Nachricht m versendet

Zuerst entschlüsselt Bob mithilfe seines privaten Schlüssels den verschlüsselten symmetrischen Schlüssel k(A,B)

Anschließend entschlüsselt er mithilfe des Schlüssels k(A,B) die Nachricht m

Das Hybride Verschlüsselungsverfahren kombiniert die Vorteile der symmetrischen und asymmetrischen Verfahren und vereint sie in einem

- Sicheren
- Schnellen
- Große Daten umfassenden

Kryptosystem.

Hybride Verfahren werden vor Allem im **E-Mail-Verkehr** genutzt.

Agenda

fhwedel
UNIVERSITY OF APPLIED SCIENCES

1. Kerckhoff‘sches Prinzip
2. Zeitreise durch die Geschichte der Kryptographie ab 19. Jahrhundert
3. Kommunikationsszenario
4. Wichtige Begriffe
5. Sicherheitsmechanismen
    1. Symmetrische Verschlüsselung
    2. Asymmetrische Verschlüsselung
    3. Hybride Verschlüsselung
6. Methoden der Kryptoanalyse

5. Kryptoanalyse

Analyse von Verschlüsselungsverfahren mit dem Ziel das System zu entschlüsseln

Freundliche Kryptoanalyse:
Überprüfung der Sicherheit des Kryptosystems

Feindliche Kryptoanalyse:
Versuch einer unbefugten Entschlüsselung

fhwedel
UNIVERSITY OF APPLIED SCIENCES

Brute Force Angriff / Holzhammermethode / Vollständige Suche

ALLE Schlüssel werden systematisch nach Wahrscheinlichkeit ausprobiert.

Heutige Rechner können Millionen verschiedene Schlüssel pro Sekunde eingeben

Wie lange braucht ein Rechner heutzutage um einen Schlüssel zu entschlüsseln?

Es kommt auf die Schlüssellänge an, die in Bits angeben wird.

Caesar-Chiffre:

DES:

AES:

fhwedel
UNIVERSITY OF APPLIED SCIENCES

Es kommt auf die Schlüssellänge an, die in Bits angeben wird.

Caesar-Chiffre: 26 Schlüssel
ca. 5 bit

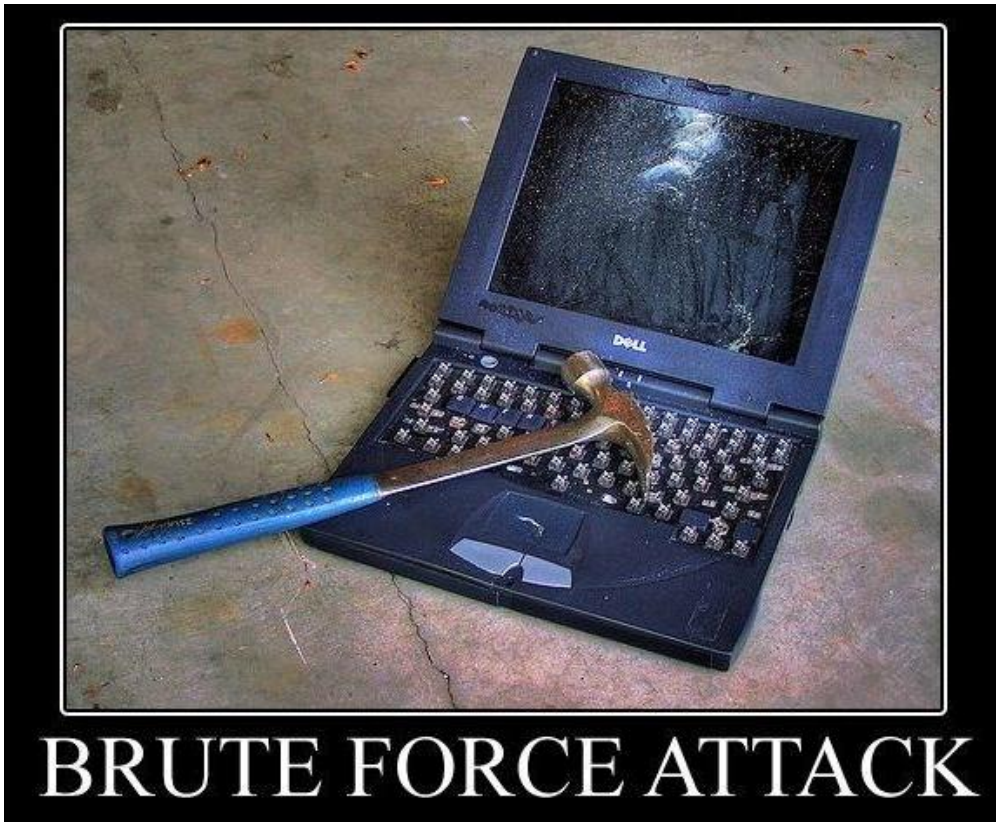
DES: 2^{56} = 72.057.594.037.927.936 Schlüssel
56 bit

AES: 2^{256} =
115.792.089.237.316.195.423.570.985.008.687.907.853.269.984.665.640.564.039.457.584.007.913.129.639.936
256 bit

Man braucht Millionen Jahre um einen 256 Bit Schlüssel zu knacken

fhwedel
UNIVERSITY OF APPLIED SCIENCES

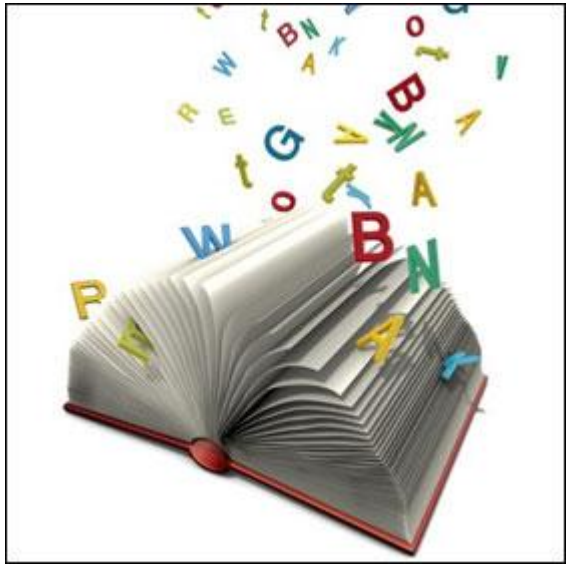
So sollte man es nicht machen



fhwedel
UNIVERSITY OF APPLIED SCIENCES

Wörterbuchangriff

ALLE Passwörter werden systematisch nach Wahrscheinlichkeit ausprobiert.



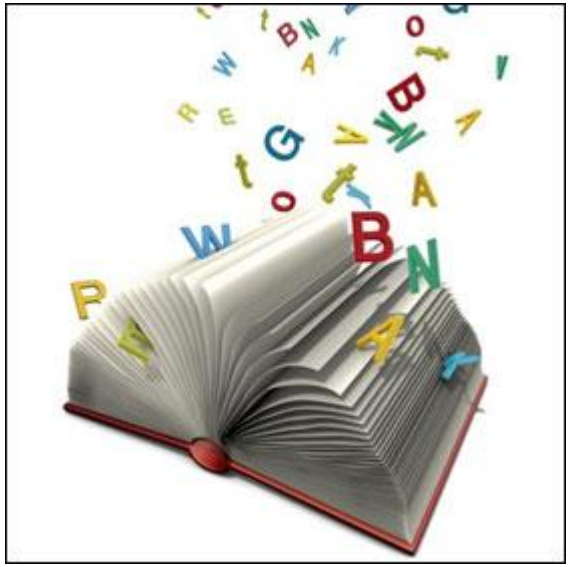
Heutige Rechner können Millionen verschiedene Schlüssel pro Sekunde eingeben

Alle Wörter einer Sprache werden innerhalb von einer Sekunde getestet

fhwedel
UNIVERSITY OF APPLIED SCIENCES

Wörterbuchangriff

Ein Kennwort was aus einem Wort einer Sprache besteht ist daher sehr unsicher



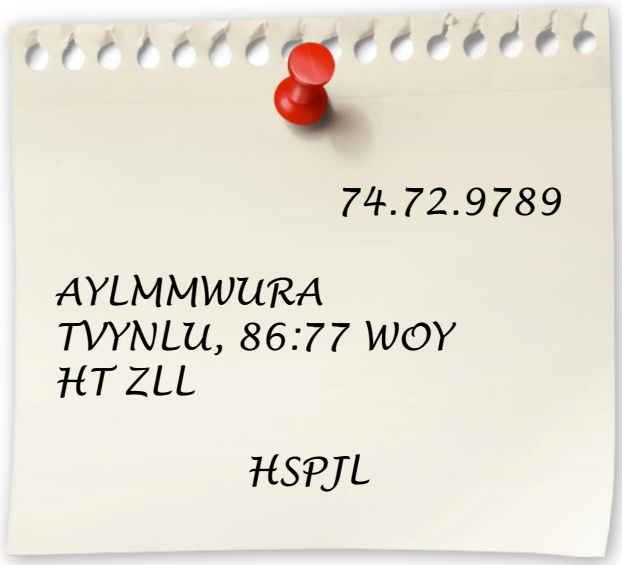
Schutz vor Angriff:

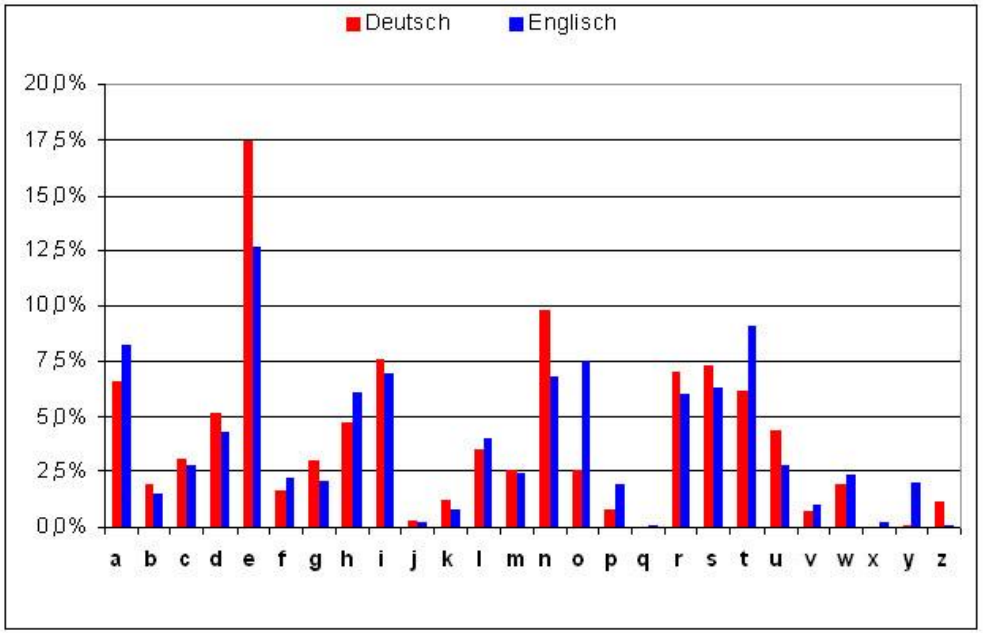
- Sinnlose Buchstabenfolge
- Sätze
- Buchstaben und Zahlen gemischt

fhwedel
UNIVERSITY OF APPLIED SCIENCES

Cipher text only

Angreifer verfügt über den Geheimtext (cipher text)





Chosen cipher text

Der Angreifer hat temporär die Möglichkeit, Geheimtexte seiner Wahl zu entschlüsseln

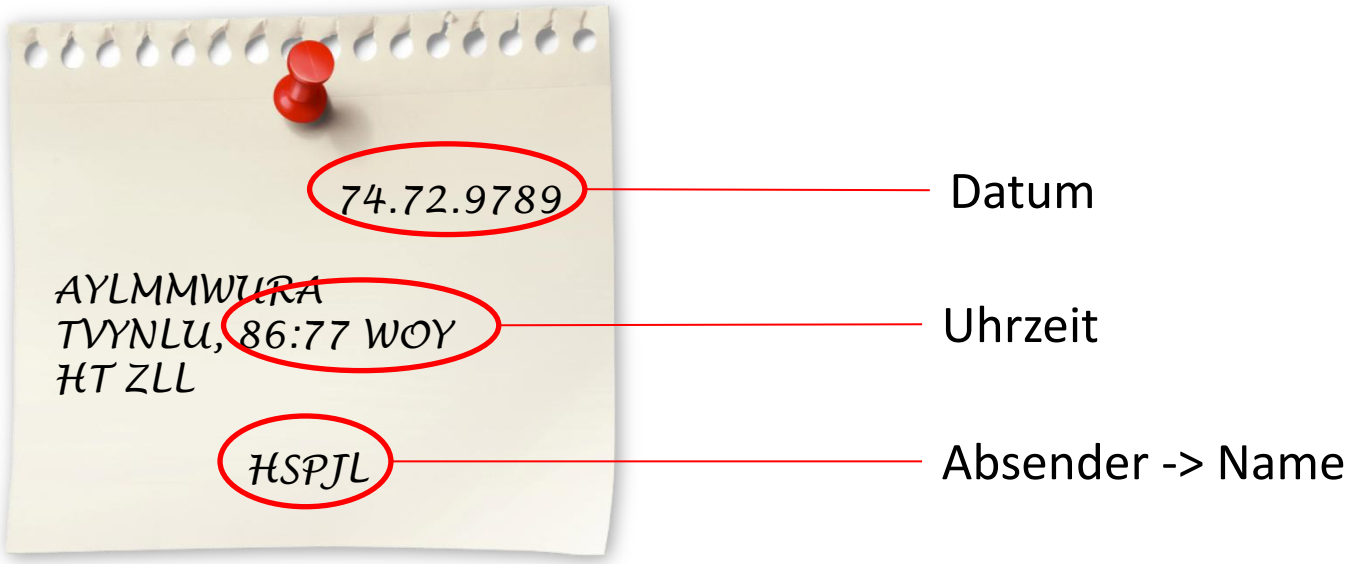
Chosen plain text

Der Angreifer kann die zu verschlüsselnden Klartexte frei wählen und hat Zugang zu den entsprechenden Geheimtexten.

fhwedel
UNIVERSITY OF APPLIED SCIENCES

Known plain text

Aus Kenntnis (oder Vermutung) über einen Teil des Klartexts wird versucht Informationen über den Schlüssel zu gewinnen



fhwedel
UNIVERSITY OF APPLIED SCIENCES

Seitenkanalattacke

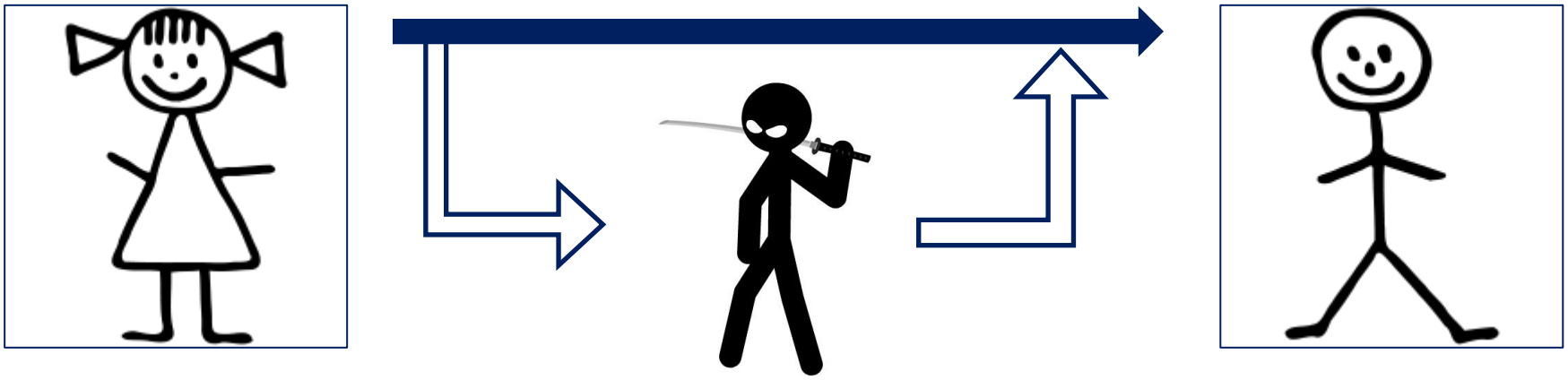
Der Angreifer versucht, außer dem Klartext, dem Chiffrat oder dem Schlüssel zunächst **auch andere Daten** zu erfassen und daraus Informationen über den verwendeten Algorithmus und Schlüssel zu gewinnen

- Dauer der Verschlüsselung
- zeitliche Verlauf des Stromverbrauchs eines Chips
- Berechnungsfehler aufgrund extremer Umgebungsbedingungen

fhwedel
UNIVERSITY OF APPLIED SCIENCES

Man-in-the-middle-Angriff

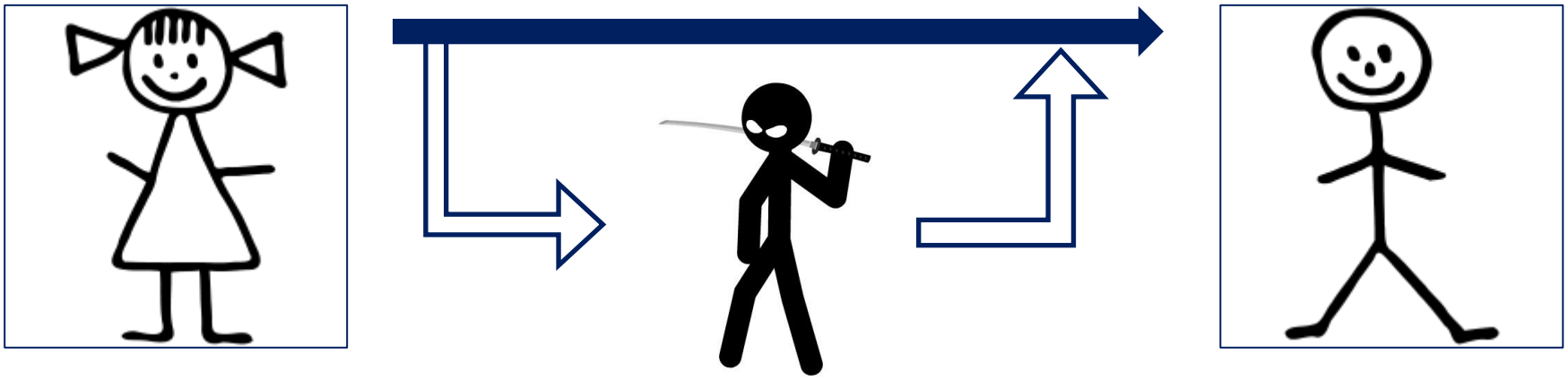
Mallory (der Angreifer) befindet sich zwischen Alice und Bob und kann alle Nachrichten mithören und sogar verändern oder neue Nachrichten einfügen



fhwedel
UNIVERSITY OF APPLIED SCIENCES

Man-in-the-middle-Angriff

Schutz: durch sicher verschlüsselte Nachrichten



6. Quellen

- www.wikipedia.de
- http://www.staff.uni-mainz.de/pommeren/DSVorlesung/KryptoBasis/KryptAnal.html
- www.kryptowissen.de
- http://ddi.cs.uni-potsdam.de/Lehre/e-commerce/elBez2-5/page05.html
- Kryptographie und IT Sicherheit; Vieweg + Teubner Verlag; 2008

Vielen Dank für Ihre Aufmerksamkeit

fhwedel
UNIVERSITY OF APPLIED SCIENCES

Haben Sie noch Fragen?

Möchten Sie die eine oder andere Folie nochmal betrachten?

Falls Ihnen doch noch Fragen einfallen:

Deniz Bilen
wing9197@stud.fh-wedel.de
denizbilen@gmx.de

Vielen Danke für Ihre Aufmerksamkeit