

9. TUTORIUM

DATENKOMMUNIKATION UND SICHERHEIT

TUTORIUMSGRUPPE 18

MATTHIS FRANZGROTE

COMSYS

RWTH AACHEN

14.07.2021

1 Fragen

- Übung 1.3
- Shannon-Theorem
- IP-Fragmentierung
- TCP/UDP Ports

2 Aufgabe 9.1: Symmetrische und asymmetrische Verschlüsselung

3 Aufgabe 9.2: Diffie-Hellman

4 Aufgabe 9.3: Schlüsselvereinbarung

FRAGEN

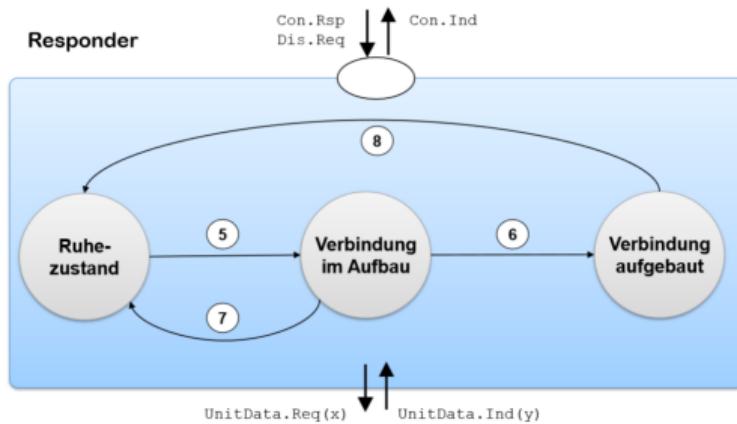
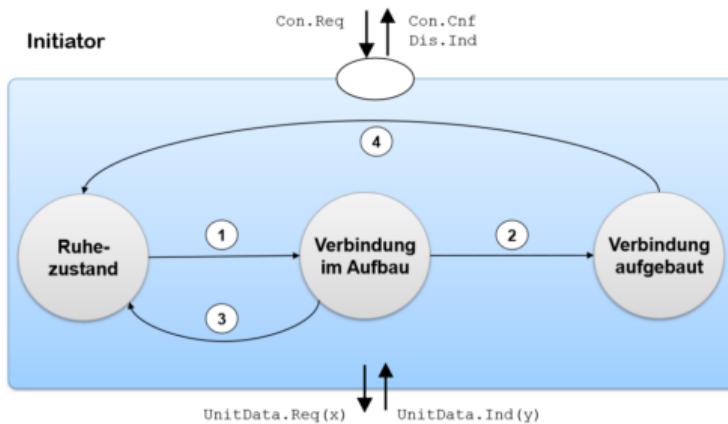
FRAGEN

ÜBUNG 1.3

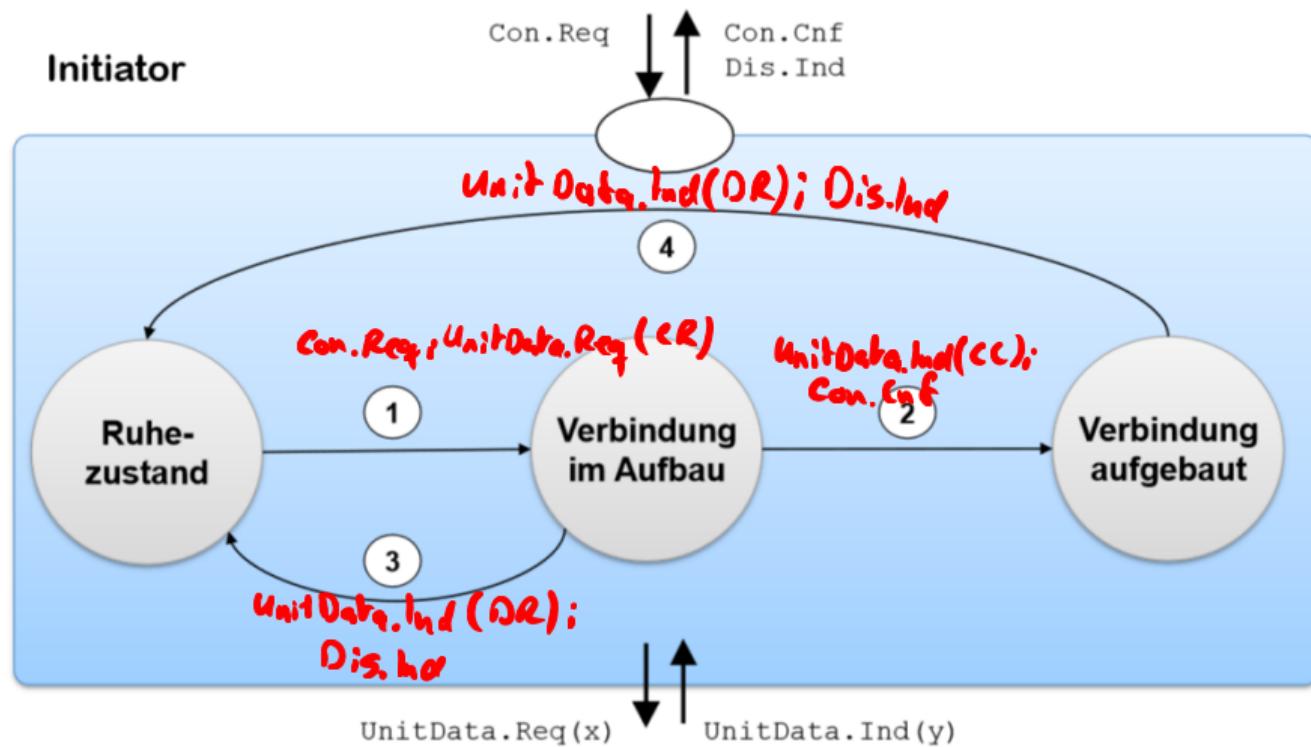
ÜBUNG 1.3

Aufgabe

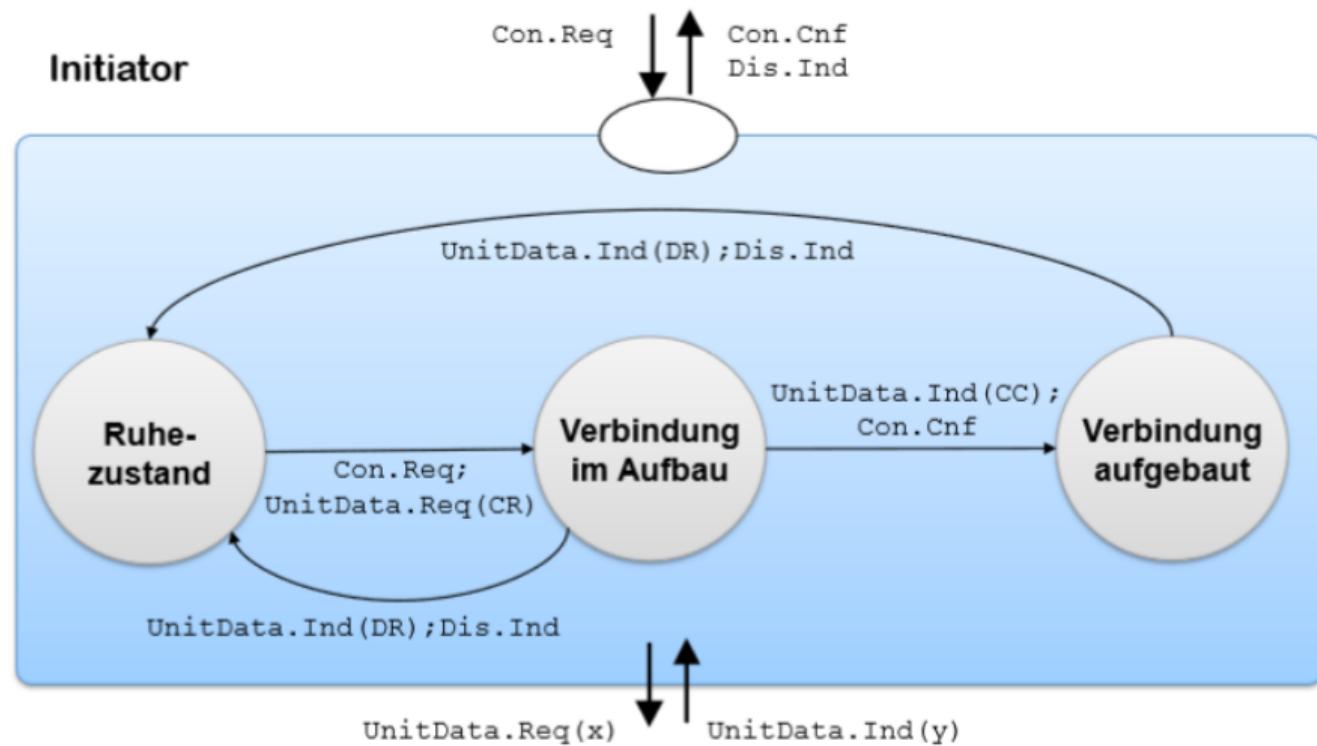
Beschriften Sie die Zustandsübergänge korrekt. Geben Sie dabei bei Verwendung von UnitData.Req und UnitData.Ind in Klammern an, welcher Inhalt übergeben wird. (Z.B. CR für ConnectionRequest, DR für DisconnectRequest oder CC für ConnectionConfirmation)



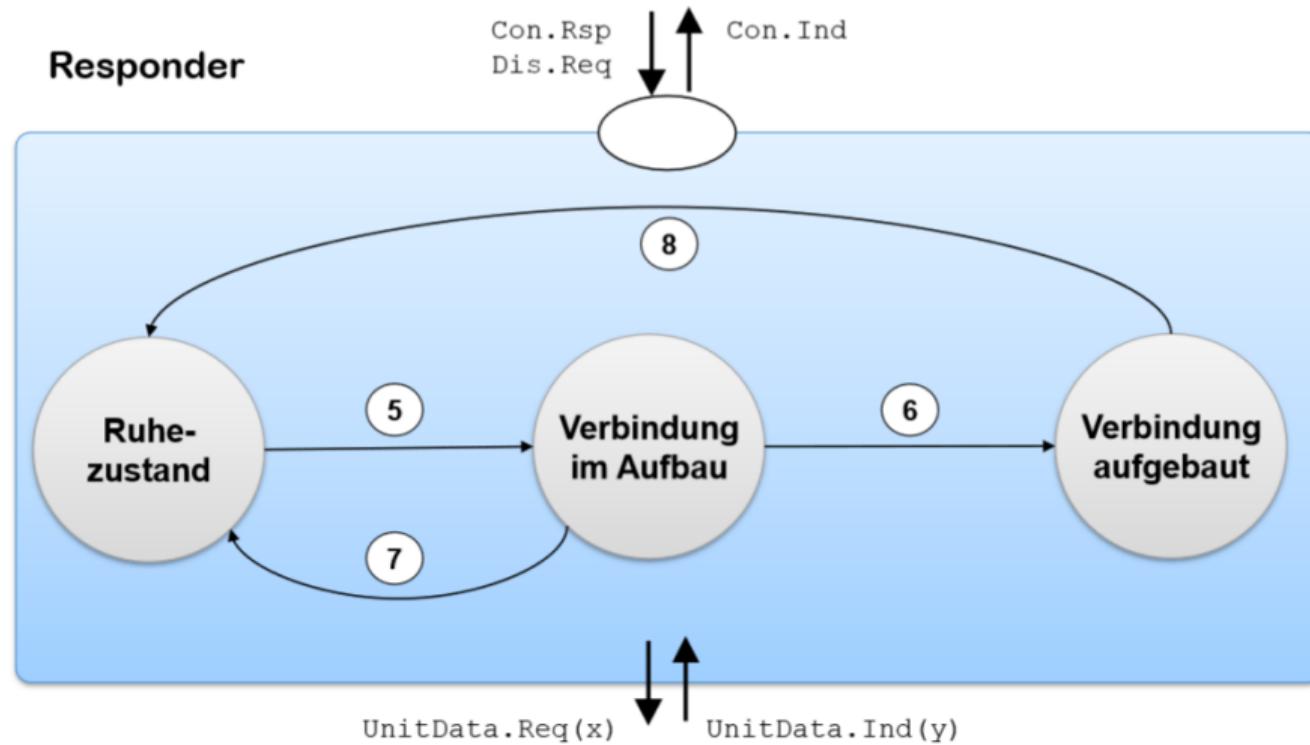
ÜBUNG 1.3



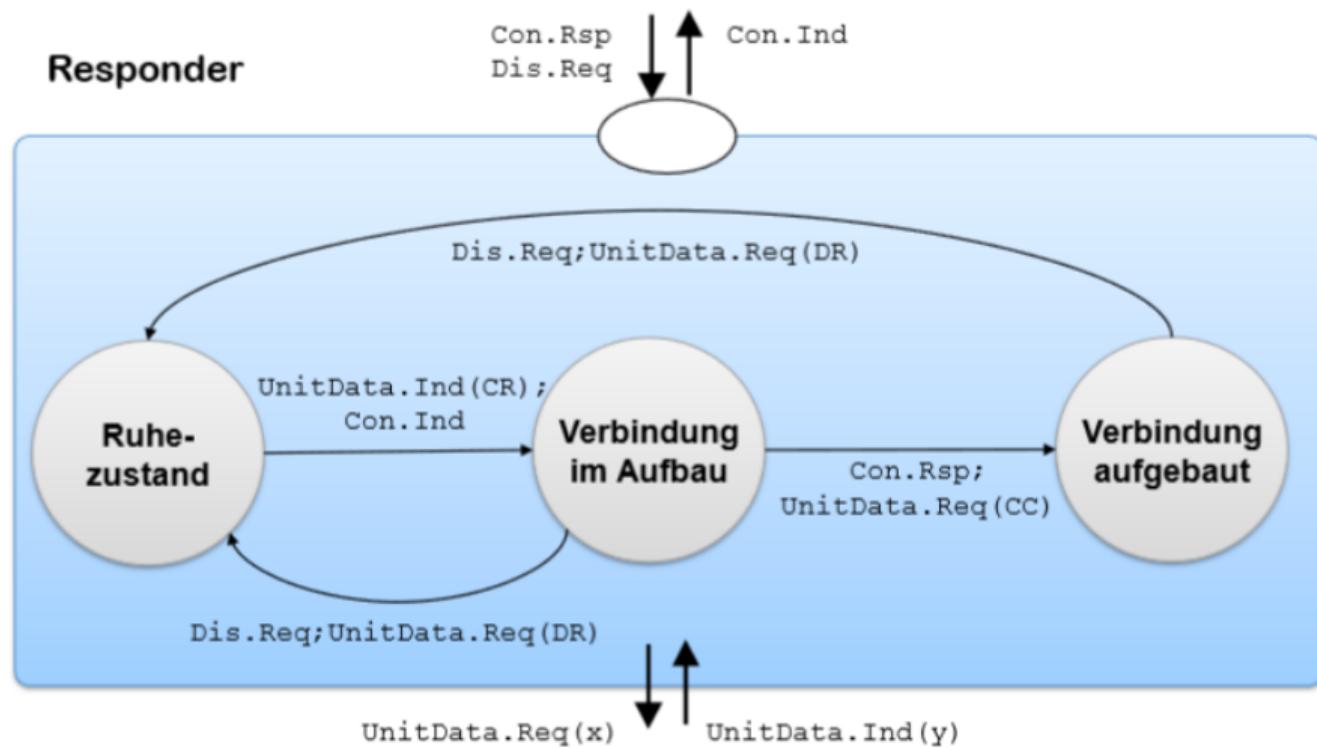
ÜBUNG 1.3



ÜBUNG 1.3



ÜBUNG 1.3



FRAGEN

SHANNON-THEOREM

SHANNON-THEOREM: S/N - SNR

Shannon-Theorem

$$R_{max}^{Sh} = B \cdot \ln(1 + S/N)$$

$S/N \leftarrow$ absoluter Maßstab, Verhältnis der Sende- zur Rauschleistung

$SNR \leftarrow$ logarithmischer Maßstab

Da i.d.R. die Sendeleistung **deutlich** größer ist, als die Rauschleistung, ist S/N zumeist sehr groß → Verwendung vom logarithmischen Maßstab (dB)

Umrechnung

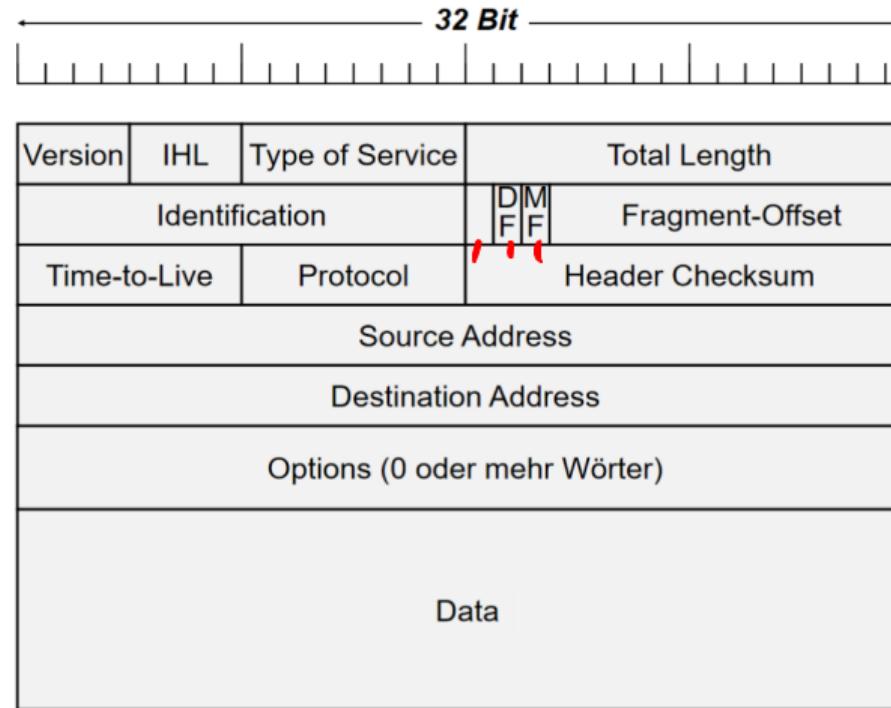
$$S/N = 100 \rightarrow SNR = 20 \quad SNR_{dB} = 10 \cdot \log_{10}(S/N) \Leftrightarrow S/N = 10^{\frac{SNR_{dB}}{10}}$$

$S/N = 1000 \rightarrow SNR = 70$
Bei jeder **verzehnfachung** von S/N erhöht sich SNR um 10

FRAGEN

IP-FRAGMENTIERUNG

IP FRAGMENTIERUNG



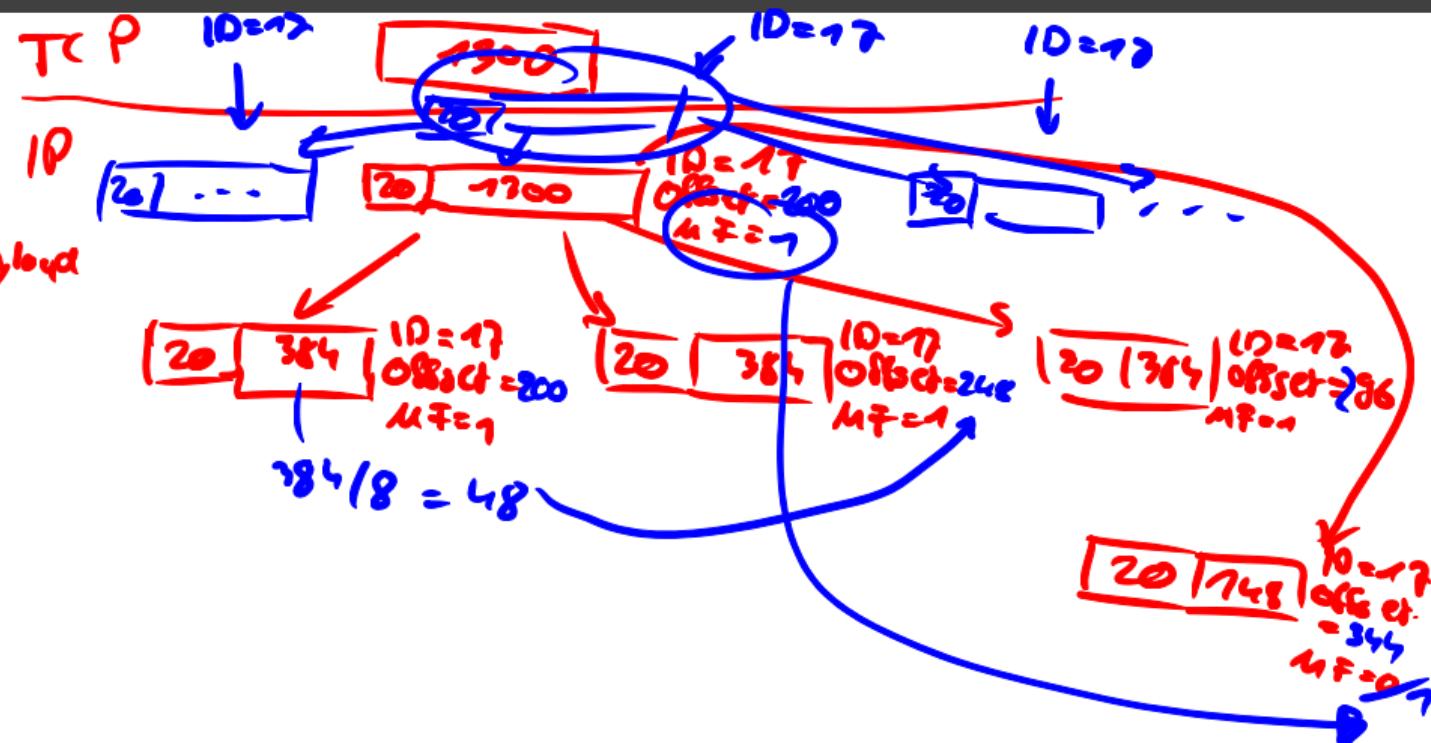
Wichtig (auch für die Klausur!)

- ID ist bei allen Fragmenten gleich
- Offset wird immer in 8 Byte (~~40 Bit~~^{64 Bit}) angegeben ⇒ Also sind auch nur Vielfache von 8 Byte als Payloadgrößen zulässig! (außer im letzten Fragment natürlich)
→ Offset 100 bedeutet also, dass das Fragment einen Teil des originalen Payloads ab Byte 800 enthält (also ab dem 801. Byte)
- MF = 0 nur im allerletzten Fragment

IP FRAGMENTIERUNG

MTU 405

$$\begin{aligned} & 405 - 20 \text{ Payload} \\ & = 385 \\ & 384 \end{aligned}$$



Übung 6.3:

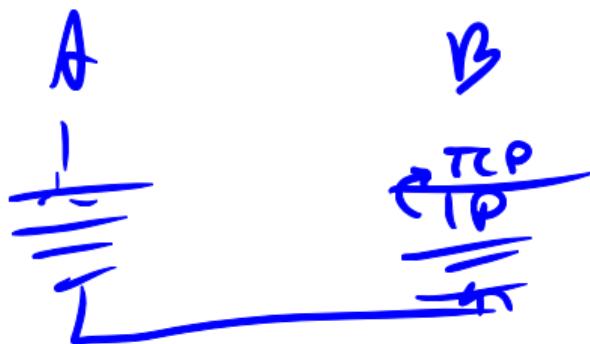
- Das gegebene Paket ist schon selbst Fragment von einem anderen Paket (da $\text{Offset} \neq 0$)
- Fragmentierung funktioniert aber wie sonst auch!
- Das erste neue Fragment bekommt nur dann nicht Offset 0, sondern den vom originalen Paket (In der Aufgabe 744)
- Von da an wie gewohnt hochzählen

FRAGEN

TCP/UDP PORTS

TCP/UDP PORTS

- TCP/UDP Ports sind PCIs!
- TCP/UDP Instanz bekommt ein Segment und ordnet anhand des Ports die Anwendung an, die zu diesem Port gehört
- Irrelevant für IP (IP Instanz reicht Pakete einfach an TCP, der kümmert sich darum das Paket weiter zuzustellen)
- Irrelevant für obere Schichten (wissen oft trotzdem darüber Bescheid)



TCP/UDP PORTS

Beispiel

- Server mit IP 137.137.137.137
- Webserver auf Port 80 (HTTP) und SSH-Server auf Port 22
- IP Pakete gehen beide an die gleiche IP Adresse (Schicht 3 kann und braucht auch nicht zwischen den beiden Anwendungen unterscheiden)
- IP gibt den Payload (TCP Segment) and die TCP Instanz
- Erst TCP sieht dann, an welchen Dienst die Anfrage geht: HTTP oder SSH

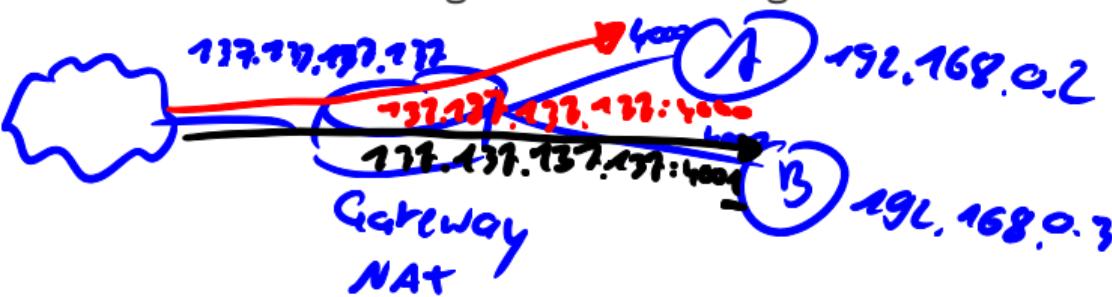
TCP/UDP PORTS

Und wenn NAT verwendet wird?

TCP/UDP PORTS

Und wenn NAT verwendet wird?

- Lokal ändert sich nichts (Hosts bekommen nichts davon mit - außer dass sie IPs aus privaten Adressbereichen haben)
- Am Gateway Übersetzung der lokalen Ports und Adressen auf globale (NAT/Portzuweisung nur hier bekannt)
- Wichtig: Da z.B. nur eine globale IP zur Verfügung steht müssen ggf. gleiche lokale Ports (geöffnet von unterschiedlichen Rechnern im lokalen Netz) auf verschiedene globale Ports abgebildet werden



AUFGABE 9.1: SYMMETRISCHE UND ASYMMETRISCHE VERSCHLÜSSELUNG

AUFGABE 9.1 A)

Aufgabe

Nennen und erläutern Sie einen *wichtigen Unterschied* zwischen *symmetrischen* und *asymmetrischen* Verfahren.

AUFGABE 9.1 A)

Aufgabe

Nennen und erläutern Sie einen *wichtigen Unterschied* zwischen *symmetrischen* und *asymmetrischen* Verfahren.

Bei **symmetrischer** Verschlüsselung verwenden beide Parteien den **gleichen** (geheimen) **Schlüssel** zum Ver- und Entschlüsseln.

Bei **asymmetrischer** werden **unterschiedliche** verwendet. Der Schlüssel zum Verschlüsseln ist dabei allen (auch potenziellen Angreifern) bekannt.

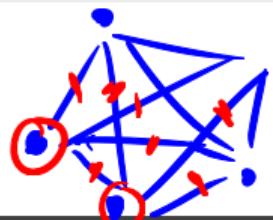
AUFGABE 9.1 B)

Angenommen, N Personen wollen paarweise mittels symmetrischer Verschlüsselung kommunizieren. Alle Kommunikationspartner können die ausgetauschten, verschlüsselten Nachrichten mitlesen, aber keiner außer den zwei kommunizierenden Personen soll in der Lage sein, die mitgelesene Kommunikation zu entschlüsseln.

Aufgabe

- Wie viele Schlüssel werden benötigt?
- Nehmen Sie nun an, dass asymmetrische Verschlüsselung genutzt wird. Wie viele Schlüssel werden dann benötigt?

$$N = 5$$



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

AUFGABE 9.1 B)

Aufgabe

- Wie viele Schlüssel werden benötigt?
- Nehmen Sie nun an, dass *asymmetrische Verschlüsselung* genutzt wird. Wie viele Schlüssel werden dann benötigt?

Symmetrische Verschlüsselung:

- Je ein Schlüssel für ein Paar von Personen
 $\Rightarrow \frac{N \cdot (N-1)}{2}$ Schlüssel

AUFGABE 9.1 B)

Aufgabe

- Wie viele Schlüssel werden benötigt?
- Nehmen Sie nun an, dass *asymmetrische Verschlüsselung* genutzt wird. Wie viele Schlüssel werden dann benötigt?

Asymmetrische Verschlüsselung:

- Jede Person P braucht einen geheimen und einen öffentlichen Schlüssel
 - Mit dem öffentlichen (public key) verschlüsseln andere Nachrichten, die an P gehen sollen
 - P entschlüsselt diese mit dem geheimen Schlüssel (private key)
- ⇒ $2 \cdot N$ Schlüssel

AUFGABE 9.1 C)

Aufgabe

Warum benutzen die meisten Protokolle sowohl *symmetrische* als auch *asymmetrische* Verfahren?

AUFGABE 9.1 C)

Aufgabe

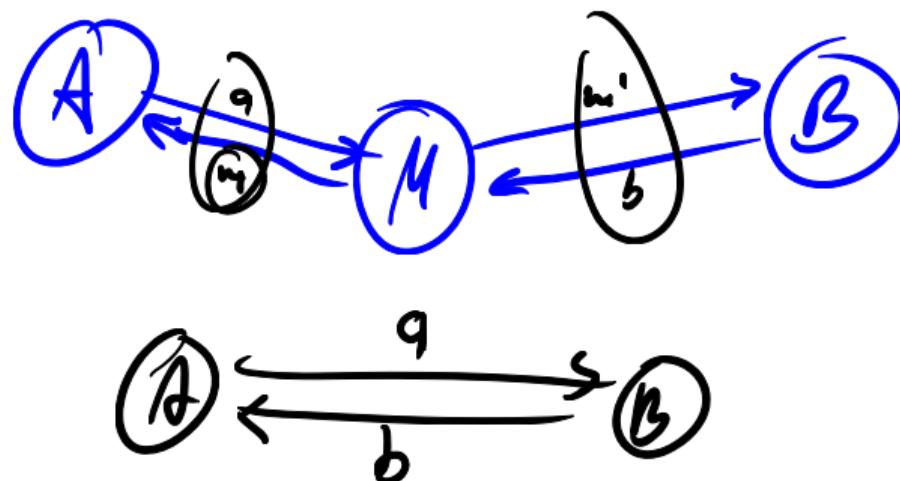
Warum benutzen die meisten Protokolle sowohl *symmetrische* als auch *asymmetrische* Verfahren?

- Bei asymmetrischer Verschlüsselung sind deutlich weniger Schlüssel notwendig und diese können über Zertifikate sehr einfach verteilt werden (via Public Key Infrastructures)
- Aber: **EXTREM** Langsam!
- Daher symmetrische Verschlüsselung zum Übertragen von vielen Daten
⇒ Asymmetrische Verfahren zum Aushandeln symmetrischer Schlüssel (und Authentifizierung)

AUFGABE 9.1 D)

Aufgabe

Was ist ein *Man-in-the-Middle-Angriff (MITM)*? Kann dieser Angriff durchgeführt werden, wenn *symmetrische Schlüssel* benutzt werden?



AUFGABE 9.1 D)

Aufgabe

Was ist ein *Man-in-the-Middle-Angriff (MITM)*? Kann dieser Angriff durchgeführt werden, wenn *symmetrische Schlüssel* benutzt werden?

- Angreifer setzt sich *zwischen* die Kommunikationspartner
 - Er gaukelt beiden Seiten vor, der jeweils andere zu sein
 - MITM-Angriffe sind nicht möglich wenn die Schlüssel schon ausgetauscht sind (dann können sie sich sicher gegeneinander authentifizieren)
 - Aber beim Schlüsselaustausch kann ein MITM je einen Schlüssel mit einem Partner austauschen ohne dass die es bemerken
- ⇒ Zusätzlich Authentifizierung notwendig!

AUFGABE 9.1 E)

Aufgabe

Gegeben sei RSA mit $p = 5$ und $q = 13$

- (i) Was sind n und $\varphi(n)$

extra Schule

$$p \cdot q = n$$

$$n = p \cdot q$$
$$\varphi(n) = (p-1)(q-1)$$

offenlich

AUFGABE 9.1 E)

Aufgabe

Gegeben sei RSA mit $p = 5$ und $q = 13$

- (i) Was sind n und $\varphi(n)$

$$n = p \cdot q = 65$$

$$\varphi(n) = (p - 1) \cdot (q - 1) = 48$$

AUFGABE 9.1 E)

Aufgabe

Gegeben sei RSA mit $p = 5$ und $q = 13$

(ii) Sei $e = 5$. Warum ist dies eine gute Wahl?

$$\langle n, e \rangle \text{ öffentliche Schlüssel}$$
$$c = m^e \pmod{n} \quad \xleftarrow{\text{Verschlüsselungsprozess}} \text{ encryption}$$
$$m = c^d \pmod{n} \quad \xleftarrow{\substack{\text{decryption} \\ \text{Entschlüsselungsprozess}}} \text{ decryption}$$

- e teilerfremd zu $\varphi(n)$
- $e < n$
- e sollte möglichst klein sein

AUFGABE 9.1 E)

Aufgabe

Gegeben sei RSA mit $p = 5$ und $q = 13$

(ii) Sei $e = 5$. Warum ist dies eine *gute* Wahl?

$e = 5$ ist kleiner als n und teilerfremd mit $\varphi(n)$ (erfüllt also die Anforderungen)

Da e sehr klein ist, sind Rechenoperationen schnell (hilfreich, da Signaturen ggf. mehrfach geprüft werden)

AUFGABE 9.1 E)

Aufgabe

Gegeben sei RSA mit $p = 5$ und $q = 13$

(iii) Finden Sie ein d , sodass $d \cdot e = 1 \pmod{\varphi(n)}$

$$\text{ggT}(48, 5)$$

$$\varphi(n)$$

$$e$$

$$29 \cdot 5 = 1 \pmod{48}$$

$$m^{d \cdot e} \pmod{n} = m^1 \pmod{\varphi(n)}$$

$$\begin{aligned} 48 &= 9 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (5 - 1 \cdot 3) = 2 \cdot 3 - 1 \cdot 5 \\ &= 2 \cdot (48 - 9 \cdot 5) - 1 \cdot 5 = 2 \cdot 48 - 19 \cdot 5 \end{aligned}$$

$$2 \cdot 48 - 19 \cdot 5 = -19 \cdot 5 \pmod{48}$$

$$-19 + 48 = 29 = d$$

AUFGABE 9.1 E)

Aufgabe

Gegeben sei RSA mit $p = 5$ und $q = 13$

(iii) Finden Sie ein d , sodass $d \cdot e = 1 \pmod{\varphi(n)}$

Erweiterter euklidischer Algorithmus:

$$\underbrace{48}_{\varphi(n)} = 9 \cdot \underbrace{5}_e + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot \underbrace{1}_{ggT} + 0$$

AUFGABE 9.1 E)

Aufgabe

Gegeben sei RSA mit $p = 5$ und $q = 13$

(iii) Finden Sie ein d , sodass $\underline{d} \cdot \underline{e} = 1 \pmod{\varphi(n)}$

Erweiterter euklidischer Algorithmus:

$$\underbrace{48}_{\varphi(n)} = 9 \cdot \underbrace{5}_e + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot \underbrace{1}_{ggT} + 0$$

$$\begin{aligned} 1 &= 3 - (1 \cdot 2) \\ &= 3 - (1 \cdot (5 - (1 \cdot 3))) = 2 \cdot 3 - 1 \cdot 5 \\ &= 2 \cdot (48 - 9 \cdot 5) - 1 \cdot 5 = 2 \cdot 48 - 19 \cdot 5 \end{aligned}$$

$$\begin{aligned} 1 &= 2 \cdot 48 - 19 \cdot 5, \text{ also } -19 \cdot 5 \pmod{48} = 1 \\ -19 &= 29 \pmod{48}, \text{ also } 29 \cdot 5 \pmod{48} = 1 \end{aligned}$$

AUFGABE 9.1 E)

Aufgabe

Gegeben sei RSA mit $p = 5$ und $q = 13$

(iv) Verschlüsseln Sie die Nachricht $m = 8$ mit dem Schlüssel $\langle e, n \rangle$.

AUFGABE 9.1 E)

Aufgabe

Gegeben sei RSA mit $p = 5$ und $q = 13$

(iv) Verschlüsseln Sie die Nachricht $m = 8$ mit dem Schlüssel $\langle e, n \rangle$.

Verschlüsselung mit $\langle e, n \rangle : c = m^e \bmod n$

Public Key *Message*

$$m^e = 32768, \text{ Ciphertext: } c = m^e \bmod n = 8$$

Entschlüsselung mit $\langle d, n \rangle : m = c^d \bmod n$

AUFGABE 9.2: DIFFIE-HELLMAN

AUFGABE 9.2 A)

Es wird Diffie-Hellman mit den Parametern $p = 31$ und $g = 15$ angewandt. Alice generiert $a = 3$, Bob $b = 4$

Aufgabe

Berechnen Sie den geheimen Schlüssel unter Verwendung des Algorithmus' von Diffie-Hellman. Geben Sie an, welche Berechnungen Alice und Bob jeweils ausführen und welche Informationen an den Kommunikationspartner übermittelt werden.

1. A : $g^a \text{ mod } p = 15^3 \text{ mod } 31 = 27$
2. A schickt 27 an B
3. B : $g^b \text{ mod } p = 2$
4. B schickt 2 an A
5. A : $2^a \text{ mod } p = 2^{3 \cdot b} \text{ mod } p = 8$
6. B : $27^b \text{ mod } p = 8$

AUFGABE 9.2 A)

Es wird Diffie-Hellman mit den Parametern $p = 31$ und $\underline{g = 15}$ angewandt. Alice generiert $a = 3$, Bob $b = 4$

Aufgabe

Berechnen Sie den geheimen Schlüssel unter Verwendung des Algorithmus' von Diffie-Hellman. Geben Sie an, welche Berechnungen Alice und Bob jeweils ausführen und welche Informationen an den Kommunikationspartner übermittelt werden.

1. Alice berechnet $A = g^a \bmod p = 15^3 \bmod 31 = 27$
2. Alice sendet A an Bob
3. Bob berechnet $B = g^b \bmod p = 15^4 \bmod 31 = 2$
4. Bob sendet B an Alice
5. ~~Alice~~^{Bob} berechnet den gemeinsamen Schlüssel $K = A^b \bmod p = 27^4 \bmod 31 = 8$
6. ~~Alice~~^{Bob} berechnet ebenso den Schlüssel $K = B^a \bmod p = 2^3 \bmod 31 = 8$

AUFGABE 9.2 B)

Aufgabe

Die Wahl der Werte in a) war nicht optimal - einer der Werte macht es einem Angreifer einfacher, den geheimen Schlüssel zu ermitteln. *Welcher der Werte war schlecht gewählt, und welche Probleme verursacht diese Wahl?* (Das alle Werte zu klein sind, ist hier nicht gemeint)

AUFGABE 9.2 B)

Aufgabe

Die Wahl der Werte in a) war nicht optimal - einer der Werte macht es einem Angreifer einfacher, den geheimen Schlüssel zu ermitteln. *Welcher der Werte war schlecht gewählt, und welche Probleme verursacht diese Wahl?* (Das alle Werte zu klein sind, ist hier nicht gemeint)

g ist schlecht gewählt

- g ist der Generator, sollte also möglichst einen Großteil der Elemente im Ring mod 31 erzeugen können
- g hat aber nur 10 Potenzen mod 31, es können also weniger Schlüssel überhaupt entstehen
- Ein Angreifer kann somit einen Schlüssel schneller ermitteln

AUFGABE 9.3: SCHLÜSSELVEREINBARUNG

AUFGABE 9.3

Es soll ein einfaches, zu Diffie-Hellman alternatives, Protokoll zum Austausch geheimer Schlüssel auf seine Sicherheit analysiert werden. Das Protokoll arbeitet wie folgt:

1. Alice wählt zufällig $k, a \in \{0, 1\}^n$ und sendet $s = k \oplus a$ an Bob
2. Bob wählt zufällig $b \in \{0, 1\}^n$ und sendet $u = s \oplus b$ an Alice
3. Alice berechnet $w = u \oplus a$ und sendet w an Bob
4. Alice nutzt k und Bob $w \oplus b$ als geheimen Schlüssel

$$\begin{aligned} w \oplus b &= (u \oplus a) \oplus b = ((s \oplus b) \oplus a) \oplus b = (((k \oplus a) \oplus b) \oplus a) \oplus b \\ &= k \end{aligned}$$

AUFGABE 9.3 A)

Aufgabe

Zeigen Sie, dass Alice und Bob im Besitz des gleichen Schlüssels sind.

AUFGABE 9.3 A)

Aufgabe

Zeigen Sie, dass Alice und Bob im Besitz des gleichen Schlüssels sind.

$$s = k \oplus a$$

$$u = s \oplus b = (k \oplus a) \oplus b$$

$$w = u \oplus a = ((k \oplus a) \oplus b) \oplus a = k \oplus b$$

$$\Rightarrow w \oplus b = (k \oplus b) \oplus b = k$$

AUFGABE 9.3 B)

Aufgabe

Bietet das Protokoll einen sicheren Schlüsselaustausch, falls ein Angreifer die Nachrichten zwar mitlesen, aber nicht modifizieren kann?

$$s = k \oplus q$$

$$u = s \oplus b = (k \oplus q) \oplus b$$

$$w = u \oplus q = ((k \oplus q) \oplus b) \oplus q = k \oplus b$$

$$s \oplus w = (k \oplus q) \oplus (k \oplus b) = q \oplus b$$

$$u \oplus (q \oplus b) = k$$

AUFGABE 9.3 B)

Aufgabe

Bietet das Protokoll einen sicheren Schlüsselaustausch, falls ein Angreifer die Nachrichten zwar mitlesen, aber nicht modifizieren kann?

Angreifer kennt s, u, w

$$s = k \oplus a$$

$$u = (k \oplus a) \oplus b$$

$$w = k \oplus b$$

Berechne

$$1. s \oplus u = (k \oplus a) \oplus (k \oplus a) \oplus b = b$$

$$2. w \oplus b = (k \oplus b) \oplus b = k$$

KEIN ÜBUNGSBLATT MEHR!

VIEL ERFOLG BEI DER KLAUSUR!

