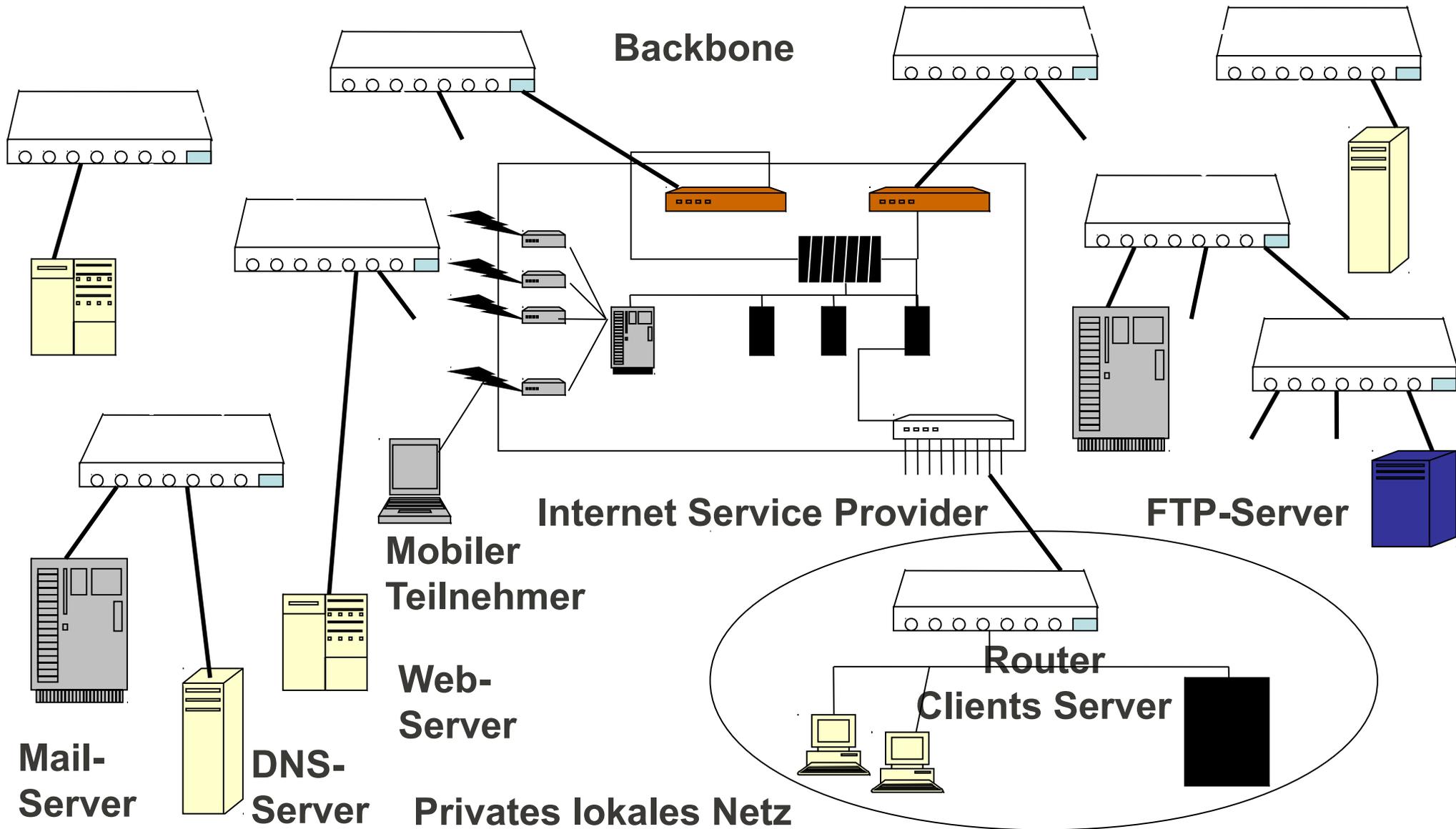


Willkommen zur Vorlesung
*Softwarearchitekturen im Finanz- und
Versicherungsbereich*
im Sommersemester 2010
Prof. Dr. Jan Jürjens

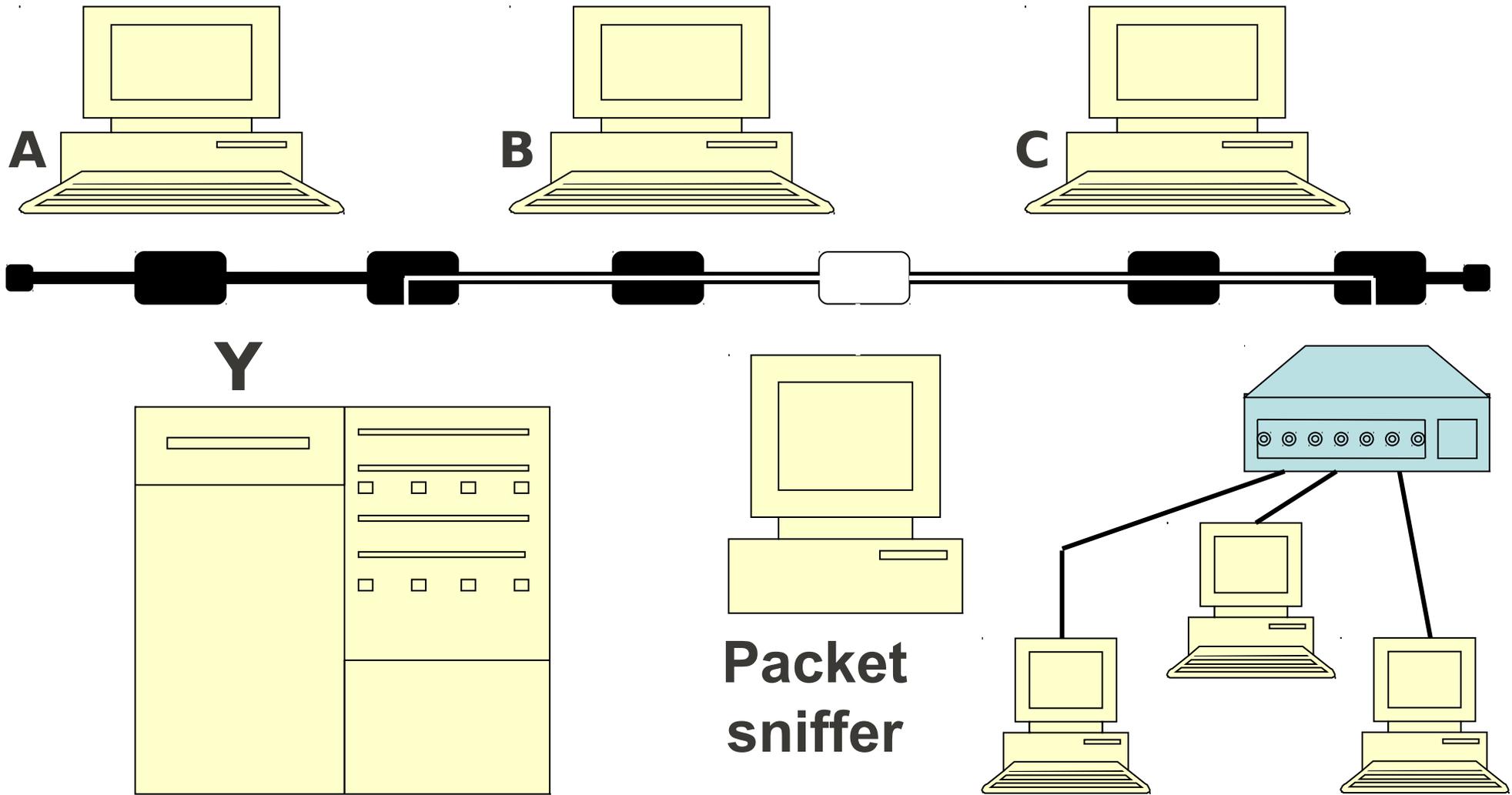
TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

3. Netzwerksicherheit und Kryptographie

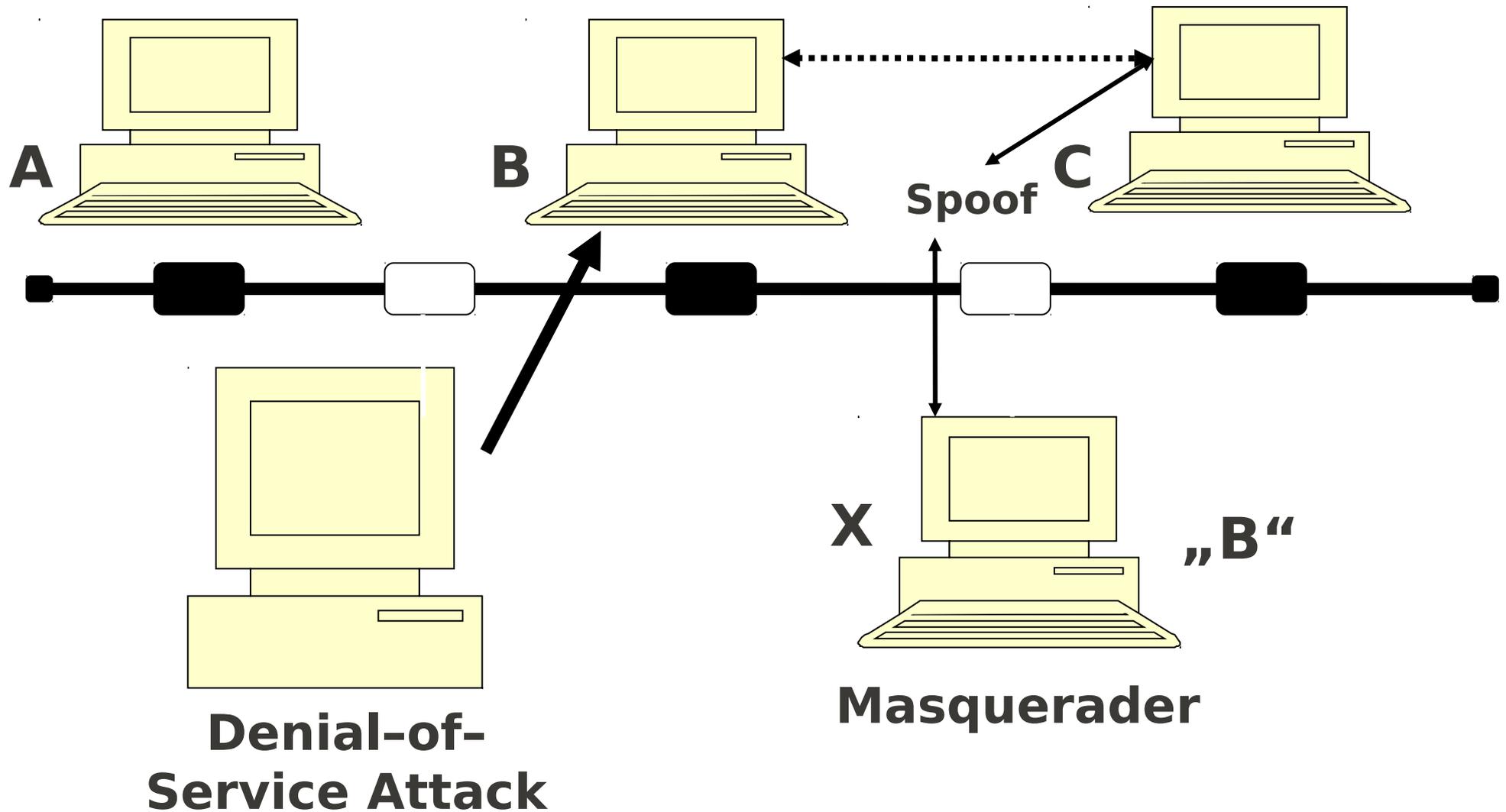
Das Internet



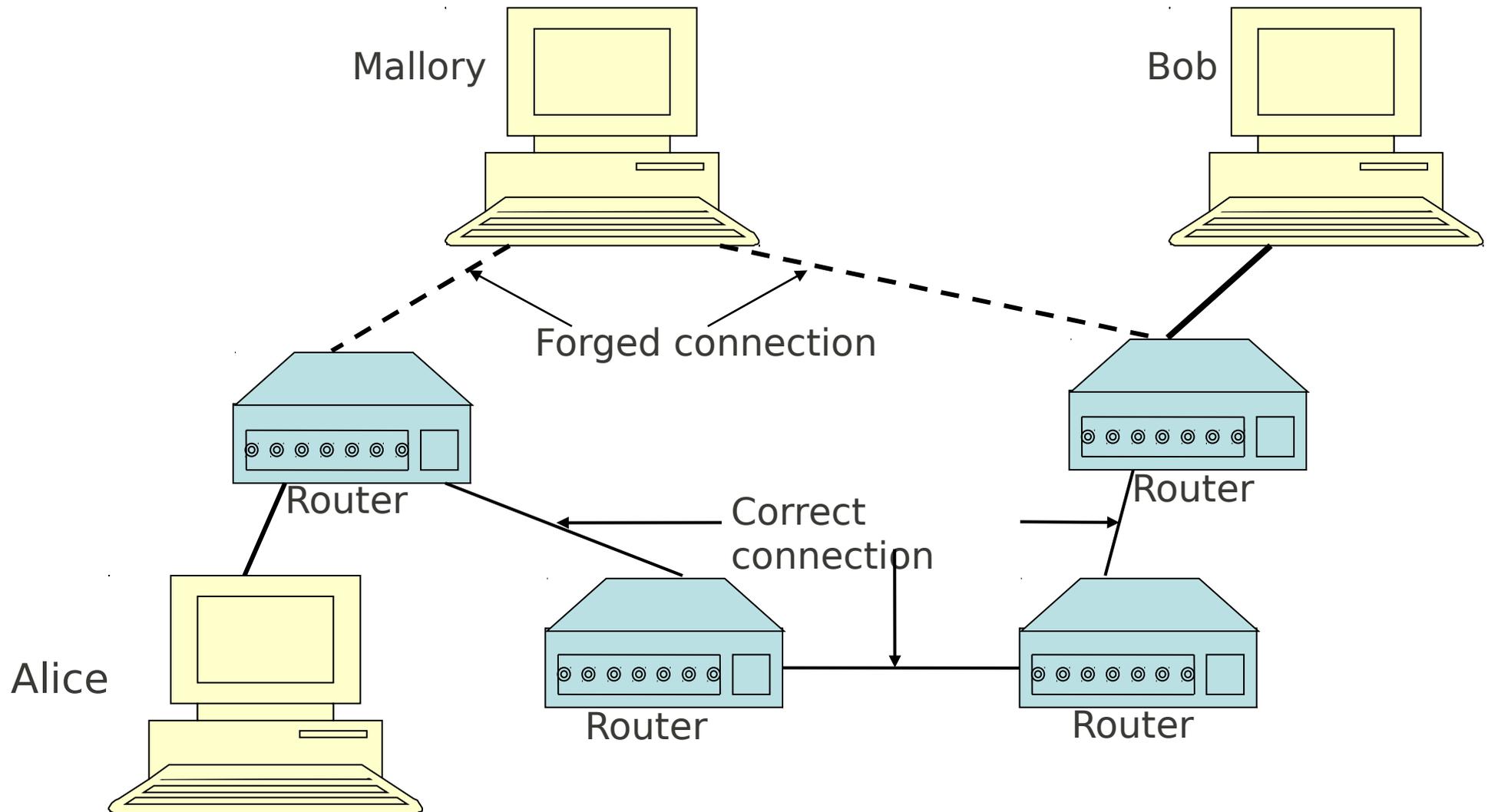
Internet Angriffe: Abhören



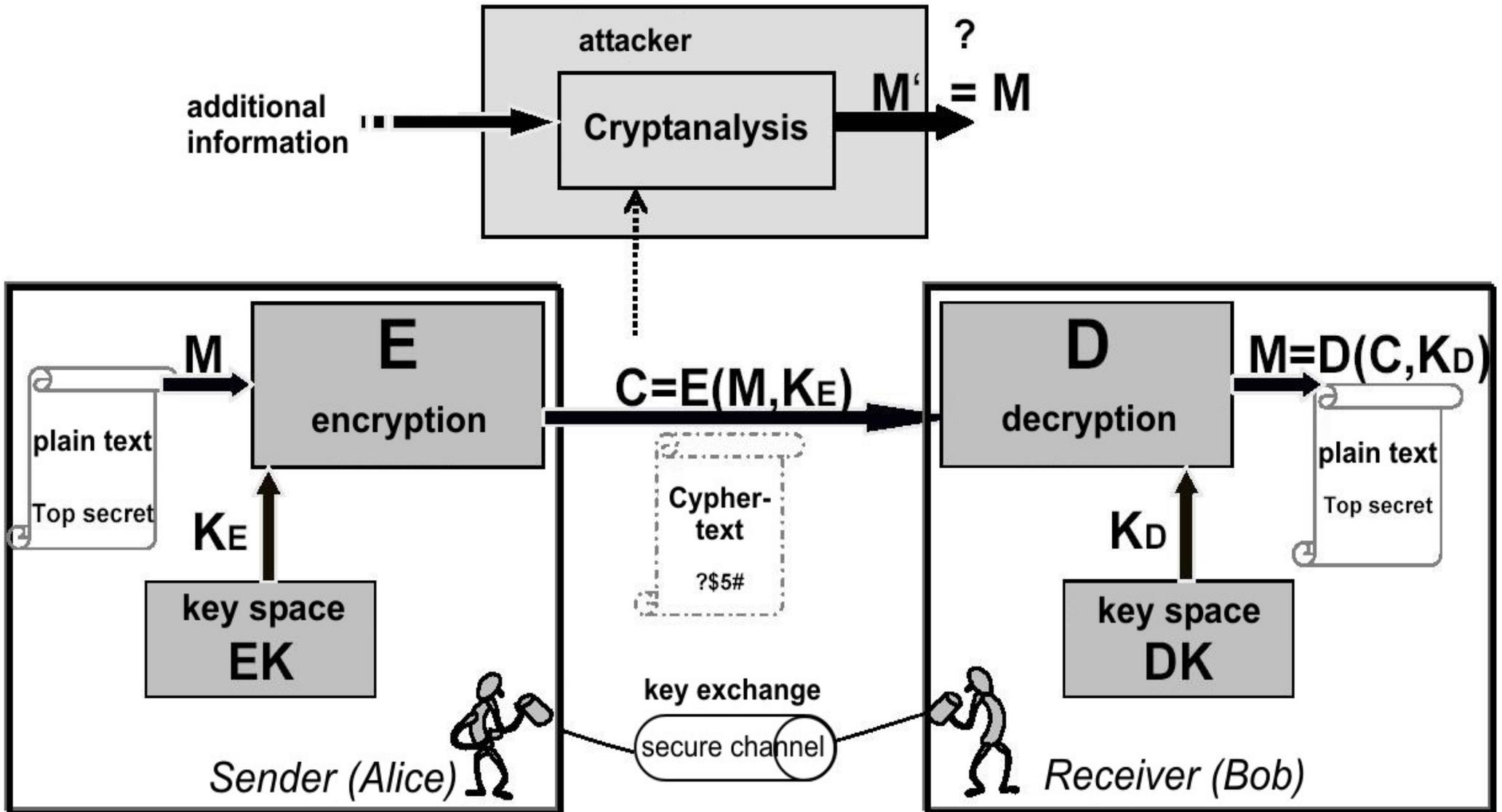
Internet II: Masquerading (Spoofing)

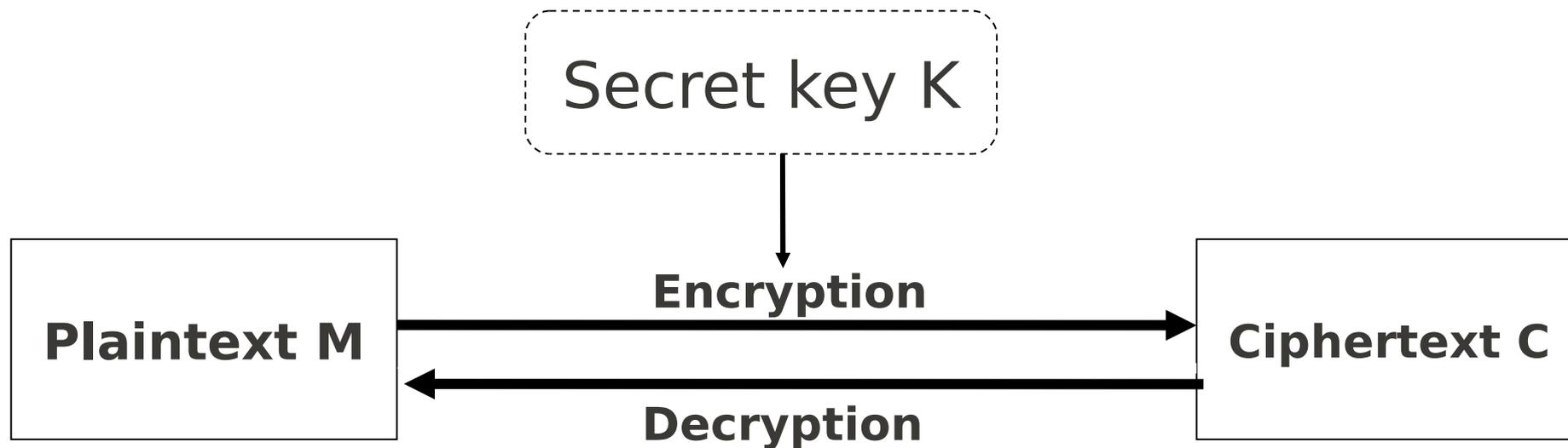


Internet III: „Man-in-the-Middle“



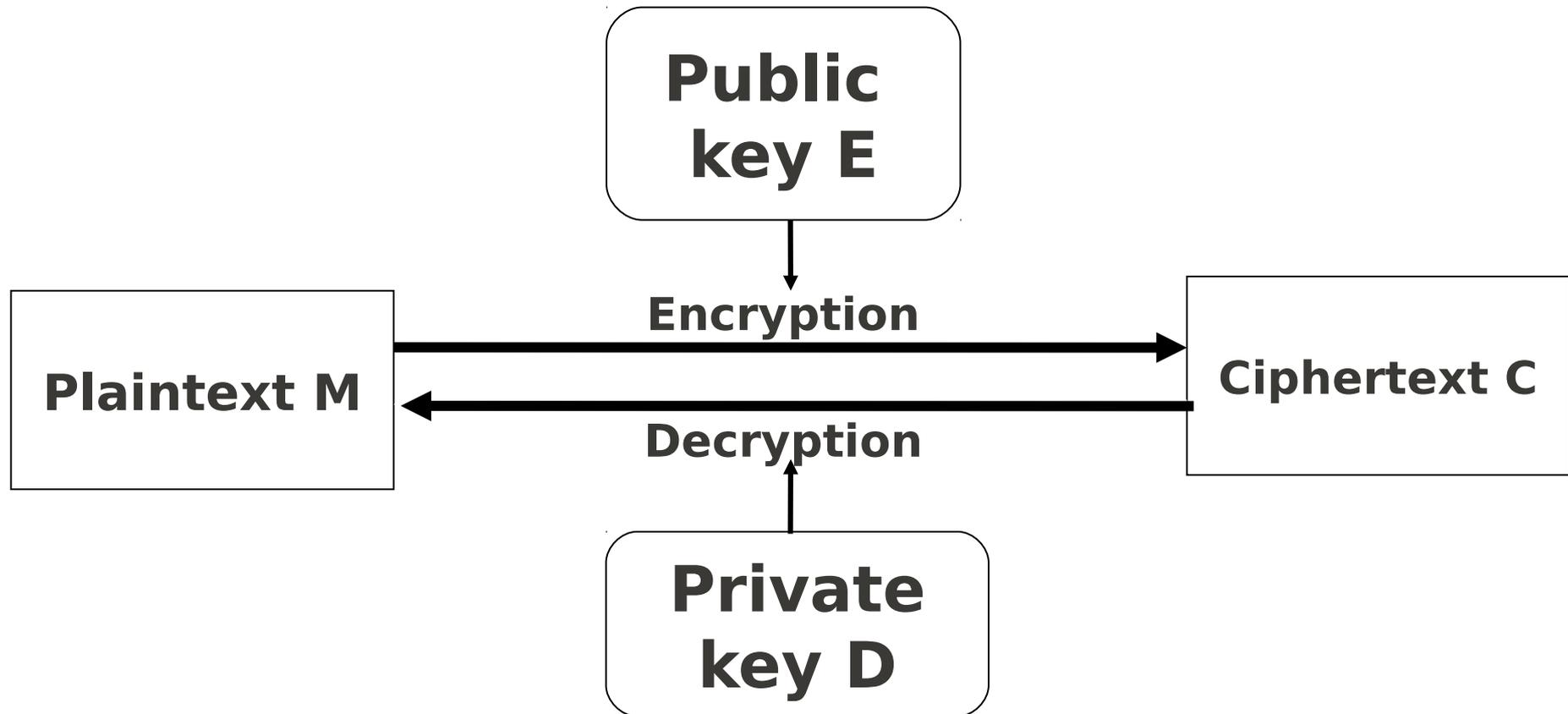
Abwehr: Kryptographie





Relations:

$$C = K(M) \text{ and } M = K(C)$$



Relations:

$$C = E(M) \text{ and } M = D(C)$$

Diskussion: Asymm. Verschlüsselung

- a) Wenn man bedenkt, dass die Menge der möglichen zu verschlüsselnden Texte sehr klein sein kann (z.B. nur die Nachrichten “ja” oder “nein”), welches Problem ergibt sich bei einem deterministischen Public-Key-Verfahren ?
- b) Wie kann man das Problem lösen ? (Hinweis: deterministische Abhängigkeit vom jeweils gegebenen Plaintext verhindern.)

- a) Wieder angenommen, man hat ein deterministisches Verschlüsselungsverfahren, der Verschlüsselungsschlüssel bleibt diesmal geheim. Wenn man annimmt, dass der Schlüssel selten gewechselt wird, und dass sich Plaintexte öfters wiederholen, können teilweise Informationen über einen verschlüsselten Text bekannt werden ?
- b) Wie kann man das Problem lösen ?

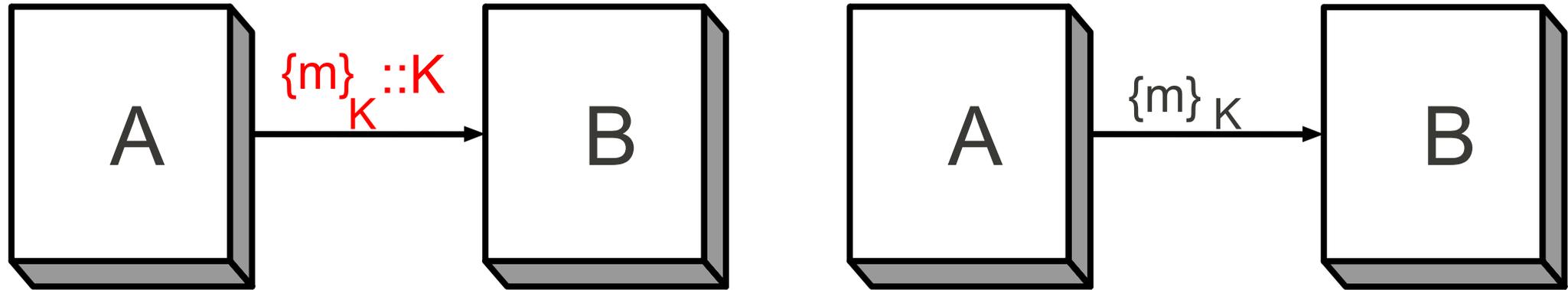
Symmetrisch:

- Digital Encryption Standard (DES), 3DES
- Advanced Encryption Standard (AES): Ryndael 2001

Asymmetrisch:

- RSA (Rivest/Shamir/Adleman): Integer Faktorisierung
- ElGamal: diskreter Logarithmus
- Diffie-Hellman: Sitzungsschlüssel generieren

Symm. Verschlüsselung vs. Vertraulichkeit



Gegen passiven Angreifer: Vertraulichkeit von m ...

- bei Versenden von $\{m\}_K :: K$ **nicht** bewahrt,
- bei Versenden von $\{m\}_K$ **bewahrt**

(wobei $::$ Konkatenation, $\{m\}_K$ Verschlüsselung von m mit symmetrischem Schlüssel K).

Aufgabe 3.1

Aufgabe 3.1

– Bei Verwendung von symmetrischer Verschlüsselung und gegen einen passiven Angreifer: wird die Vertraulichkeit von m ...

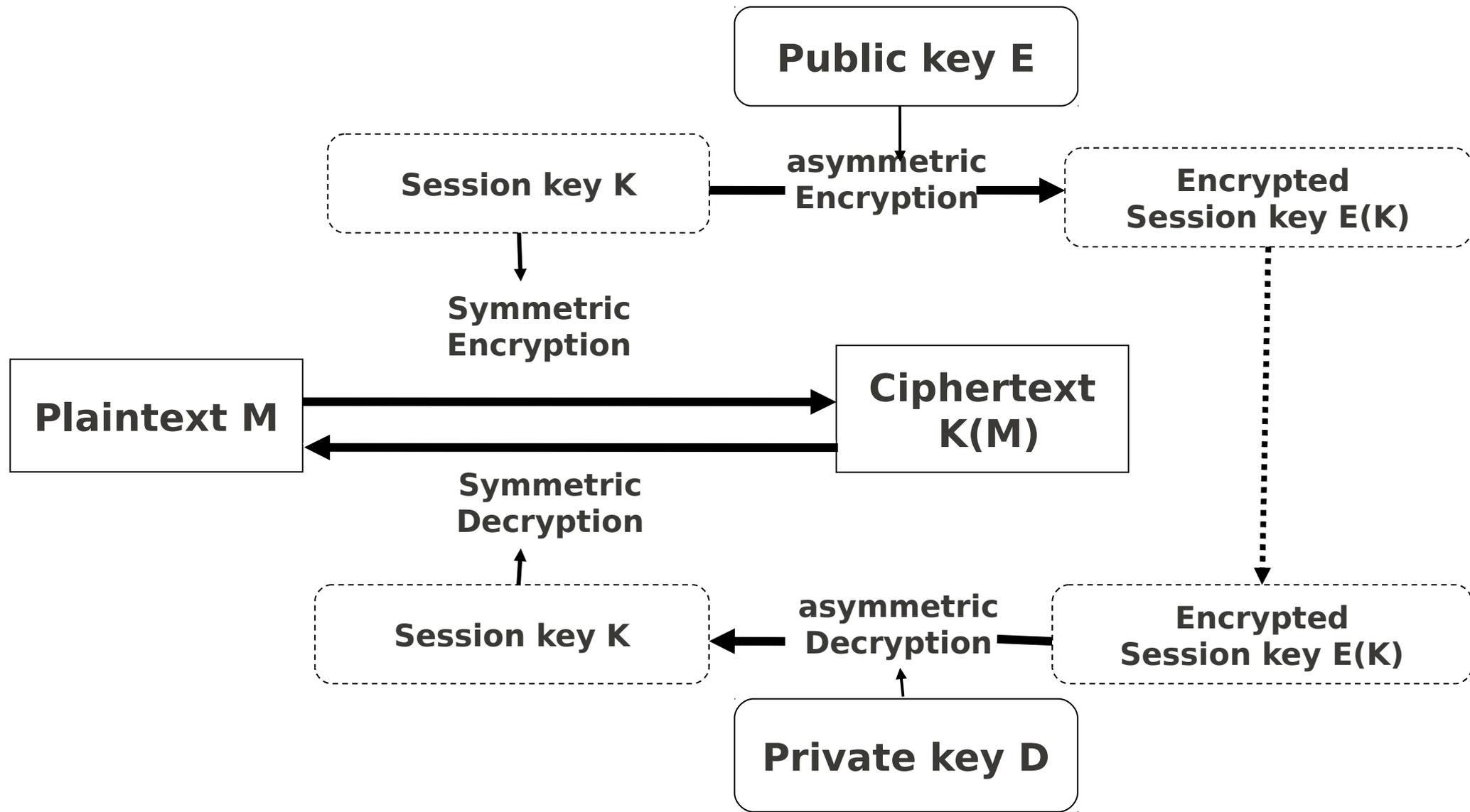
a) bei Versenden von $\{\{m\}_{K1}\}_{K2}::K1$ bewahrt ? [1 P.]

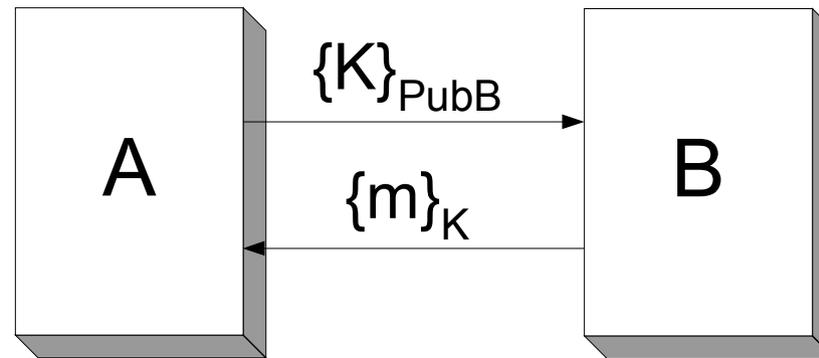
b) bei Versenden von $\{m\}_{K1}::\{m\}_{K2}::K1$ bewahrt ? [1 P.]

c) bei Versenden von $\{\{m\}_{K1}\}_{K2}::\{K1\}_{K2}$ bewahrt ? [1 P.]

(wenn man annimmt, dass $K1$ und $K2$ verschiedene Schlüsseln sind).

Hybride Verschlüsselung



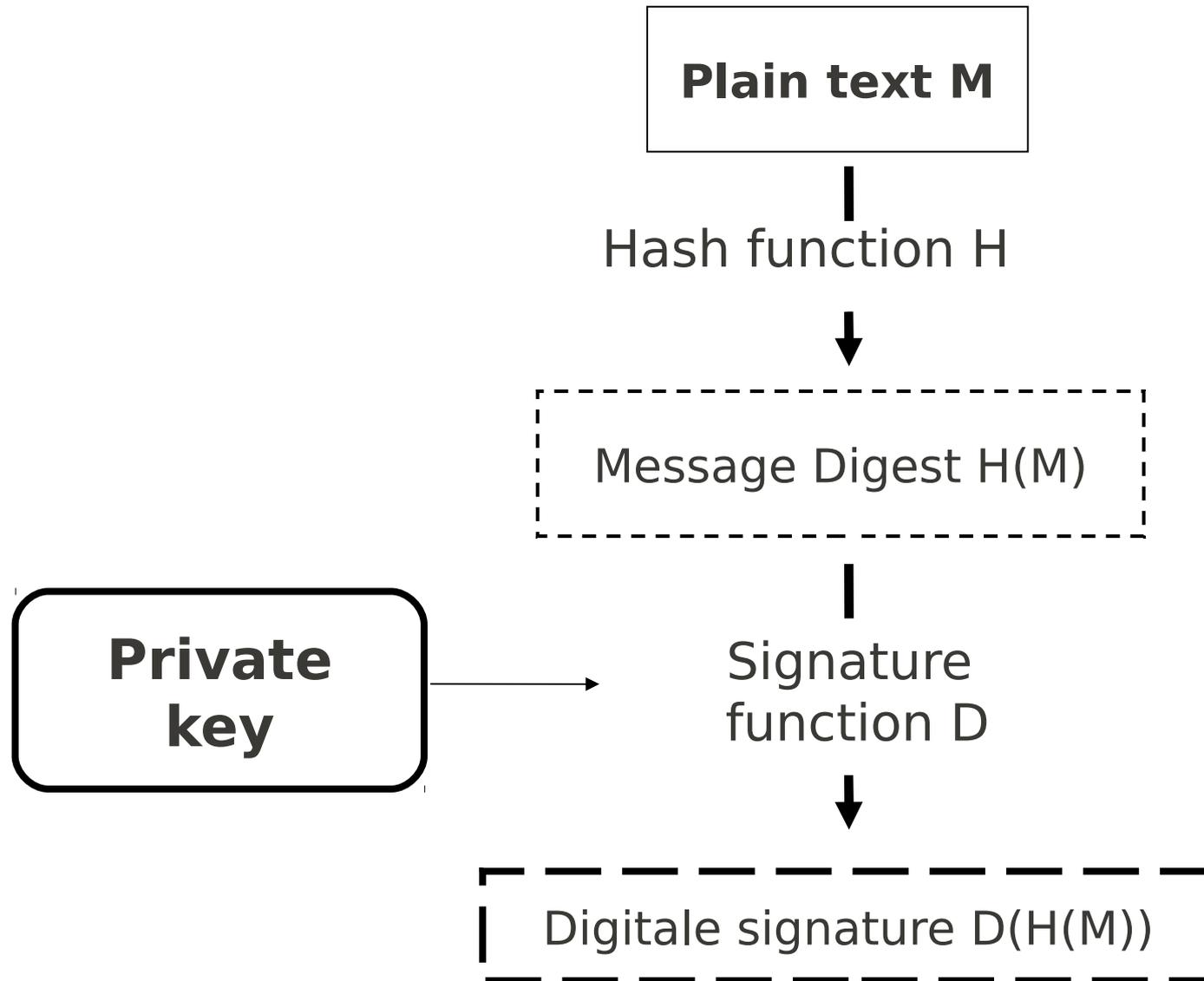


Für symmetrischen Schlüssel K und öffentlichen (asymm.)
Schlüssel $PubB$:

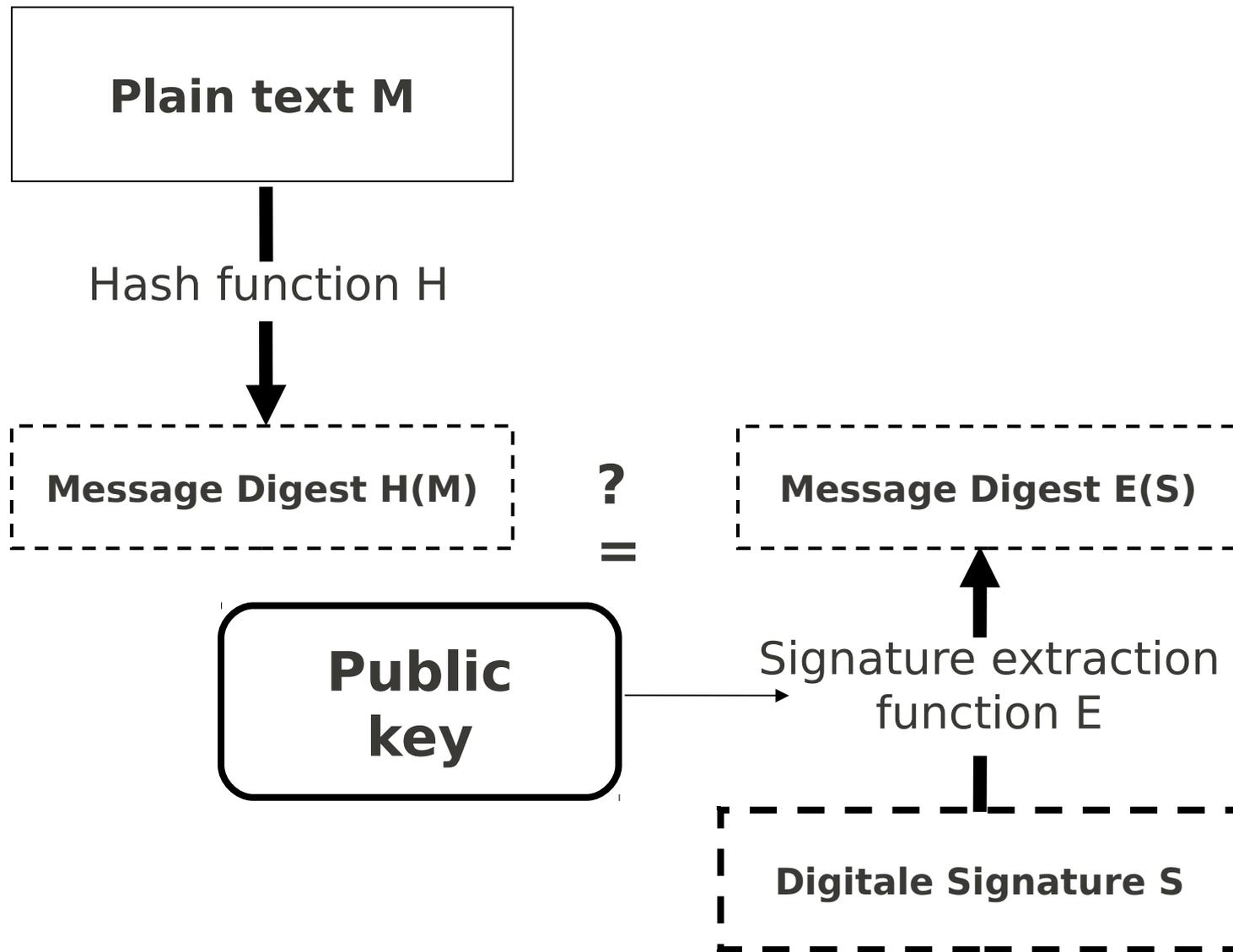
Vertraulichkeit von m **nicht** bewahrt gegen Angreifer der
Nachrichten löschen und einfügen kann.

Vertraulichkeit von m **bewahrt** gegen passiven Angreifer.

Erzeugung digitaler Signaturen



Verifikation digitaler Signaturen



Aufgabe 5

Der RSA-Signaturalgorithmus D hat die Homomorphie-Eigenschaft, dass:

$$D(M1::M2)=D(M1)::D(M2)$$

für alle Nachrichten $M1$, $M2$. Wenn man kein Hash verwenden würde – wie könnte dann ein Angreifer den Geldbetrag in der Signatur D (“Ich schulde Dir 10 EUR.”) auf 100 EUR erhöhen, ohne den Algorithmus brechen zu müssen (wenn Zeichenketten Konkatenationen von Zeichen sind) ? [3 P.]

Brute Force Angriffe



Schlüssellänge in Bit

Kosten (\$)	40	56	64	80	112	128
100.000	2 s	35 h	1 J	70.000 J	10^{14} J	10^{19} J
1.000.000	0,2 s	3,5 h	37 T	7.000 J	10^{13} J	10^{18} J
10 Mio	20 ms	21 min	4 T	700 J	10^{12} J	10^{17} J
100 Mio	2 ms	2 min	9 h	70 J	10^{11} J	10^{16} J
1 Mrd	0,2 ms	13 s	1 h	7 J	10^{10} J	10^{15} J
10 Mrd	20 μ s	1 s	5,4 min	245 T	10^9 J	10^{14} J
100 Mrd	2 μ s	0,1 s	32 s	24 T	10^8 J	10^{13} J
10^{12}	0,2 μ s	10 ms	3 s	2,4 T	10^7 J	10^{12} J
10^{13}	20 ns	1 ms	0,3 s	6 h	10^6 J	10^{11} J

NSA ???

Vergleichbare Sicherheit von symmetrische und asymmetrischen Schlüssellängen

Schlüssellänge (in Bits)

Symmetrisch

asymmetrisch

56

384

64

512

80

768

112

1792

128

2304

[Schneier: Angewandte Kryptographie]

21

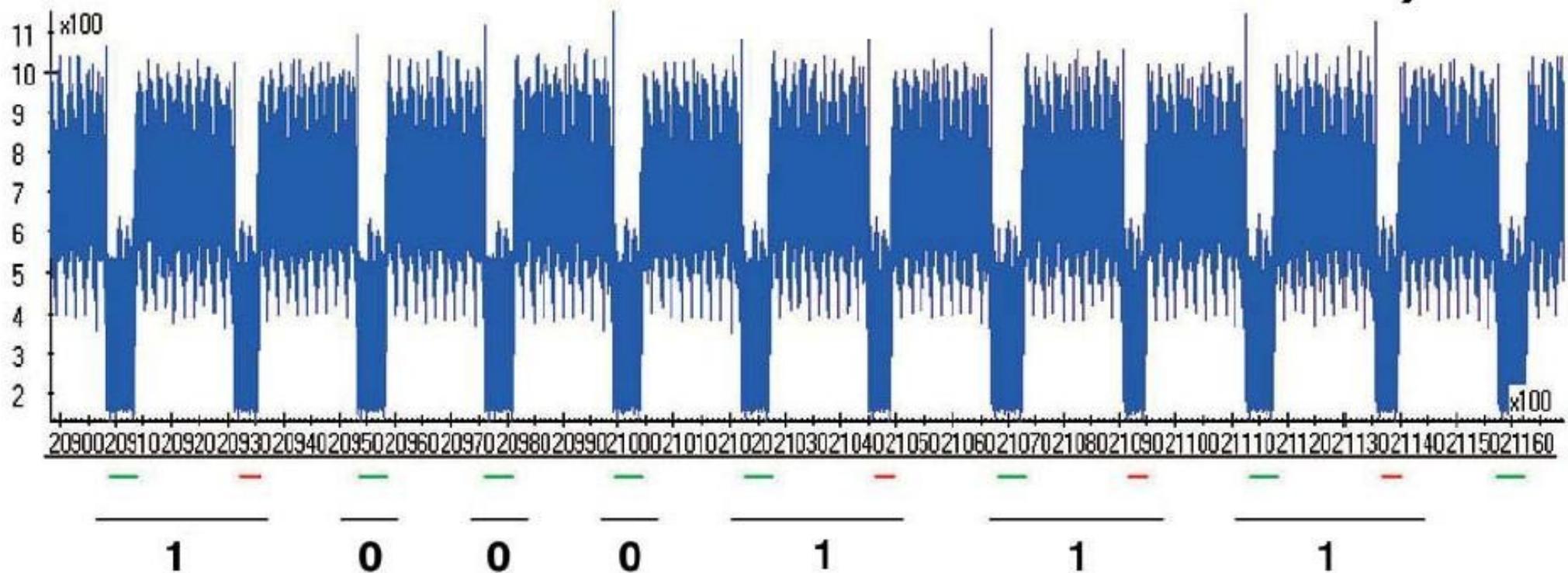
Schlüssellängen



Informationsart	Lebensdauer	Bits (min.)
militärtaktische Informationen	Min. / Stunden	56 – 64
Produktankündigungen, Firmen- zusammenschlüsse, Zinssätze	Tage / Wochen	64
langfristige Geschäftsplanungen	mehrere Jahre	64
Wirtschaftsgeheimnisse (Coca Cola)	Jahrzehnte	112
geheime Daten zur Wasserstoffbombe	über 40 Jahre	128
Identität von Spionen	über 50 Jahre	128
personenbezogene Daten	über 50 Jahre	128
Geheimdiplomatie	über 65 Jahre	> 128
Daten der US-Volkszählung	100 Jahre	> 128

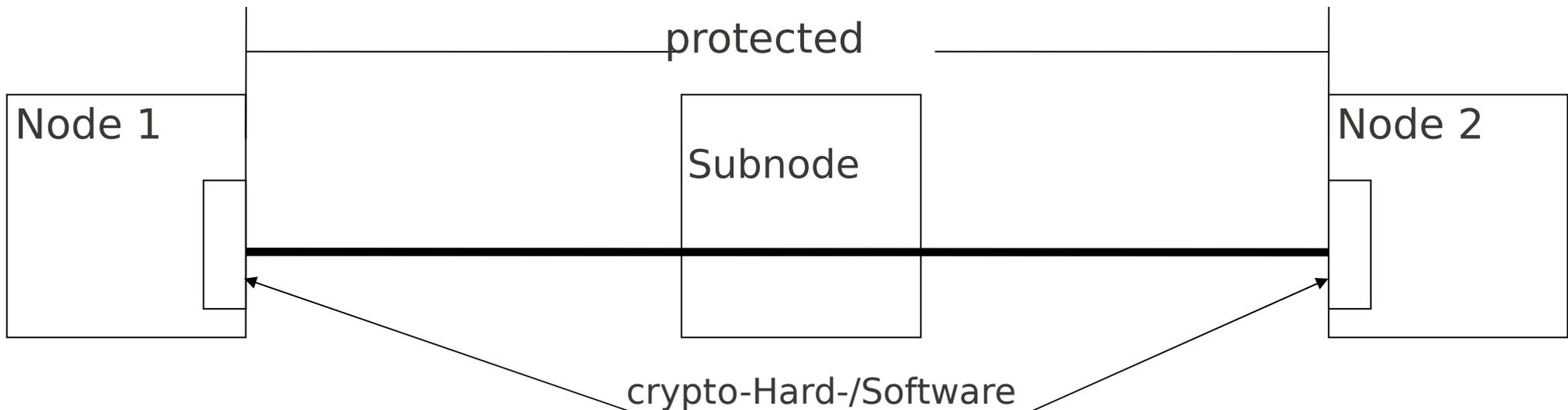
„Side Channel“ Angriffe

Vertrauliche kryptographische Daten rekonstruieren (z.B. externen Stromverbrauch von Smartcard beobachten)



„End-to-End-Encryption“

- Daten durchgehend verschlüsselt
- komplexer zu implementieren
- intransparent für Software, separate Behandlung von Adressen und Daten



Freies Programmpaket zum „Erfahren“ von Kryptographie (www.cryptool.de; B. Esslinger (Deutsche Bank), C. Eckert (TUD) et al.).

Kryptoverfahren anwenden und analysieren.

Fast alle State-of-the-Art Kryptofunktionen.

- klassische Verfahren (Cäsar,...) und Analysen (Entropie, gleitende Häufigkeit,...)
- moderne (a-)symmetrische Verfahren (3DES, AES, RSA, ...), Analysen
- Signaturen, Zufallszahlen, Hash, MACs,...

Aufgabe 2

– Im Cryptool unter

- Hilfe
- Szenarien (Tutorials)
- Angriff auf den Hashwert der digitalen Signatur
- Angriff auf die digitale Signatur

für die dort mitgelieferten Dateien Original.txt und Faelschung.txt mit den voreingestellten Optionen Erweiterungen konstruieren lassen (und als Lösung abgeben), die eine Hash-Kollision darstellen. [3 P.]