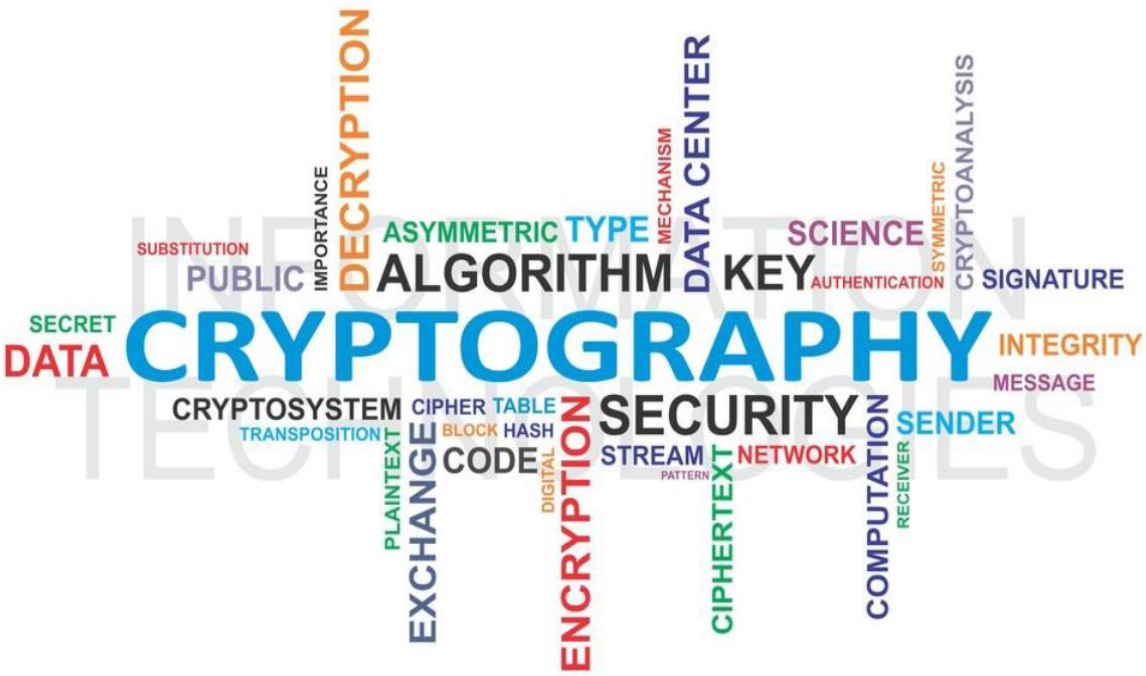
J ∫ Skripte

Mo. 13. Feb.

Kryptologie ICS.KRYPTO

Folien zur Präsenz 1
«Grundlagen der Kryptographie», FS 24, V4.2

Kap. 1 – 3 = Präsenz 0 = war Vorbereitung (flipped classroom)



©Josef Schuler, dipl. math., dipl. Ing. NDS ETHZ, MSc Applied IT-Security, Feldhof 25, 6300 Zug, j.schuler@bluewin.ch resp. josef.schuler@hslu.ch

Inhaltsübersicht

- Eine Einführung in die Kryptographie
  - Typische Angriffe
  - Definition der Schutzmechanismen
  - 4 Einschübe
    - Schlüssel und Passwort
    - Unterschied zw. Verfahren und Schlüssel
    - Einführung in die Hashfunktionen
    - Der Informationsgehalt (= informationstheoretische Entropie) in Bit
  - Die verschiedenen Grundprinzipien

Der Slogan zu dieser Präsenz

Die (sym. & asym.) Verschlüsselung verhindert nur einen von acht standardisierten Angriffen!

Lernziele

- Ich kann den Nutzen von kryptographischen Massnahmen beurteilen.
- Ich kann die verschiedenen Schutzmechanismen unterscheiden.
- Ich kann die 8 typischen Angriffe, die mit Hilfe der Kryptographie verhindert werden können, aufzählen.
- Ich kann die Zuordnung, mit welchen Schutzmechanismen welche Angriffe verhindert werden können, anwenden.
- Ich kann bei einem kryptographischen System erkennen, welches der Schlüssel und welches das Verfahren (Algorithmus) ist.
- Ich kenne den Unterschied zwischen symmetrischer und asymmetrischer Kryptographie.
- Ich kenne den Unterschied zwischen Verschlüsseln und Integritätsschutz.
- Ich kenne den Unterschied zwischen einer digitalen Signatur und einem MAC.
- Ich kann die Anzahl Schlüssel berechnen.
- Ich kann die Stärke eines Passwortes in die Länge eines kryptographischen Schlüssels umrechnen.
- Ich kann die Entropie resp. Redundanz einer Sequenz berechnen.
- Ich habe einen ersten Eindruck in Hashfunktionen erhalten.

Verweise zur Literatur

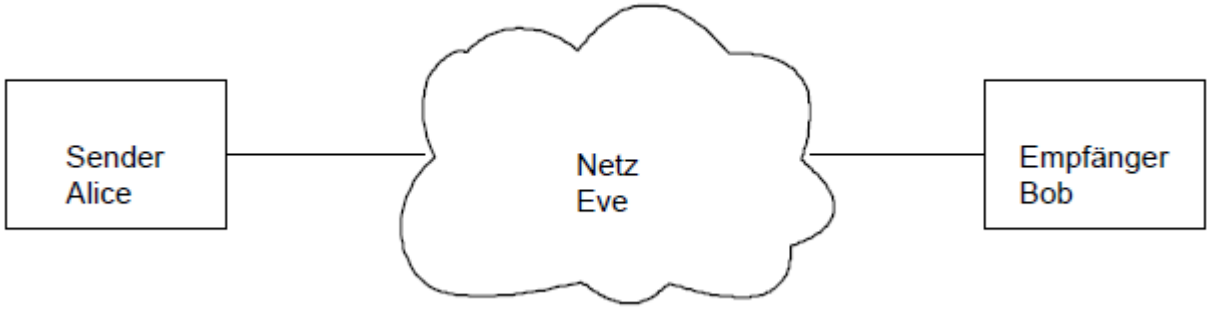
- ***Theorie und (weitere Aufgaben):***
  - JS Skripte „Einführung in die Kryptologie“, Kap. 4 – 6.
  - Die Kapitelnummerierung (Kap. 4 – 6 usw.) in den folgenden Folien entspricht derjenigen im oben erwähnten JS Skript „Einführung in die Kryptologie“. D.h. die Details zu den Folien können im Skript nachgelesen werden. Zudem hat es im Skript weitere Übungen und Beispiele. ***Die Aufgabennummerierung im JS Skript «Einführung in die Kryptologie» und in den vorliegenden Folien stimmen nicht überein!***
  - ***Wichtig:*** Es ist unbedingt zu beachten, dass nur das Bearbeiten und Lernen der Folien nicht genügt. Das Durcharbeiten der oben erwähnten Kapitel in JS Skripte „Einführung in die Kryptologie“ sind absolut zentral zum Bestehen der Modulendprüfung.
  - ***Wichtig:*** Die Standortbestimmung am Schluss des Skripts soll dazu dienen, zu checken, ob das Grundwissen verstanden worden ist.

- ***Die Quellenangaben sind im JS Skript, nicht aber in den Folien enthalten!***

Kap. 4

ANGRIFFE, SCHUTZMECHANISMEN UND ANZAHL SCHLÜSSEL

Angriffe im klassischen Kryptomodell



- Eve, aber auch Alice & Bob können nun angreifen:
  - Eve
    -
    -
    -
    -
    -
  - Alice
    -
    -
    -
  - Bob
    -

Angriffe im klassischen Kryptomodell, Lösung

- Eve
  - Abhören der Meldung (Confidentiality)
  - Verändern der Meldung (Integrity) (*)
  - Eine erfundene Meldung einspielen (Insertion) (*)
  - Eine Meldung abfangen und später wieder einspielen (Replay) (*)
  - Löschen von Meldungen (Delete) (*)
  - Sich für jemanden anders (z.B. für Alice) ausgeben (Masquerade) (**)
- Alice
  - Abstreiten die Meldung geschickt zu haben (Non repudiation of origin) (*)
  - Eine schon einmal geschickte Meldung nochmals schicken (Replay) (*)
  - Sich für jemanden anders ausgeben (Masquerade) [In diesem Fall wäre Alice in der Rolle von Eve] (**)
- Bob
  - Abstreiten die Meldung erhalten zu haben (Non repudiation of receipt) (*)

(*) gehören zum Begriff der (Daten-)Authentizität.
(**) gehören zum Begriff der (Benutzer-)Authentizität, oder anders gesagt, wenn eine Masquerade verhindert werden soll, so braucht es eine sichere Authentisierung. Diese wird oft im Rahmen von IAM (Identity und Access Management) oder von AAA (Architectures Authentication, Authorization, and Access Control) behandelt.

Sicherheitsanforderungen versus Angriffe

- Vertraulichkeit:
  - Abhören einer Meldung (Confidentiality)
- Daten-Integrität/Daten-Authentizität
  - Verändern der Meldung (Integrity)
  - Eine erfundene Meldung einspielen (Insertion)
  - Abstreiten die Meldung geschickt zu haben (Non repudiation of origin)
  - Eine Meldung abfangen und später wieder einspielen (Replay).
  - Löschen von Meldungen (Delete).
  - Abstreiten die Meldung erhalten zu haben (Non repudiation of receipt, z.B. in SIC = Swiss Interbank Clearing).
- Benutzer (oder Instanz)-Authentizität (Authentisierung)
  - Sich für jemanden anders ausgeben (Masquerade).

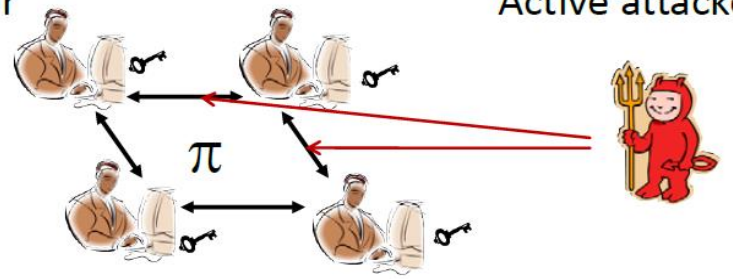
Angreifer, siehe auch intelligent/unintelligent

Insbesondere macht es bei den intelligenten Gegnern (= Angreifer = attacker) Sinn noch weitere Unterscheidungen vorzunehmen:

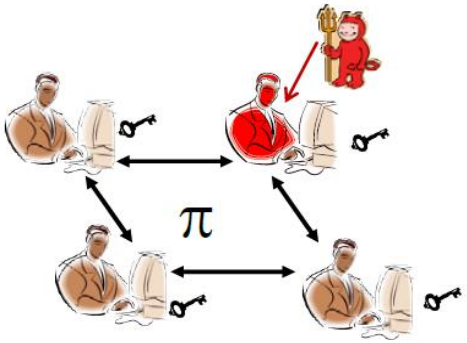
- Outsider und Insider, deren Bedeutung selbstredend ist.
- Aktiv und Passive.
  - Passiv bedeutet, dass der Angreifer sich passiv verhält, dass er zwar alles unternimmt, um abzuhören, verfälscht aber nichts und greift auch nicht aktiv ein.
  - Aktiv bedeutet, dass der Gegner Meldungen, Meldungsabläufe (Protokolle) auch bewusst verfälschen will.

- **Outsider attacker**
  - Passive attacker

Active attacker



- **Insider attacker**



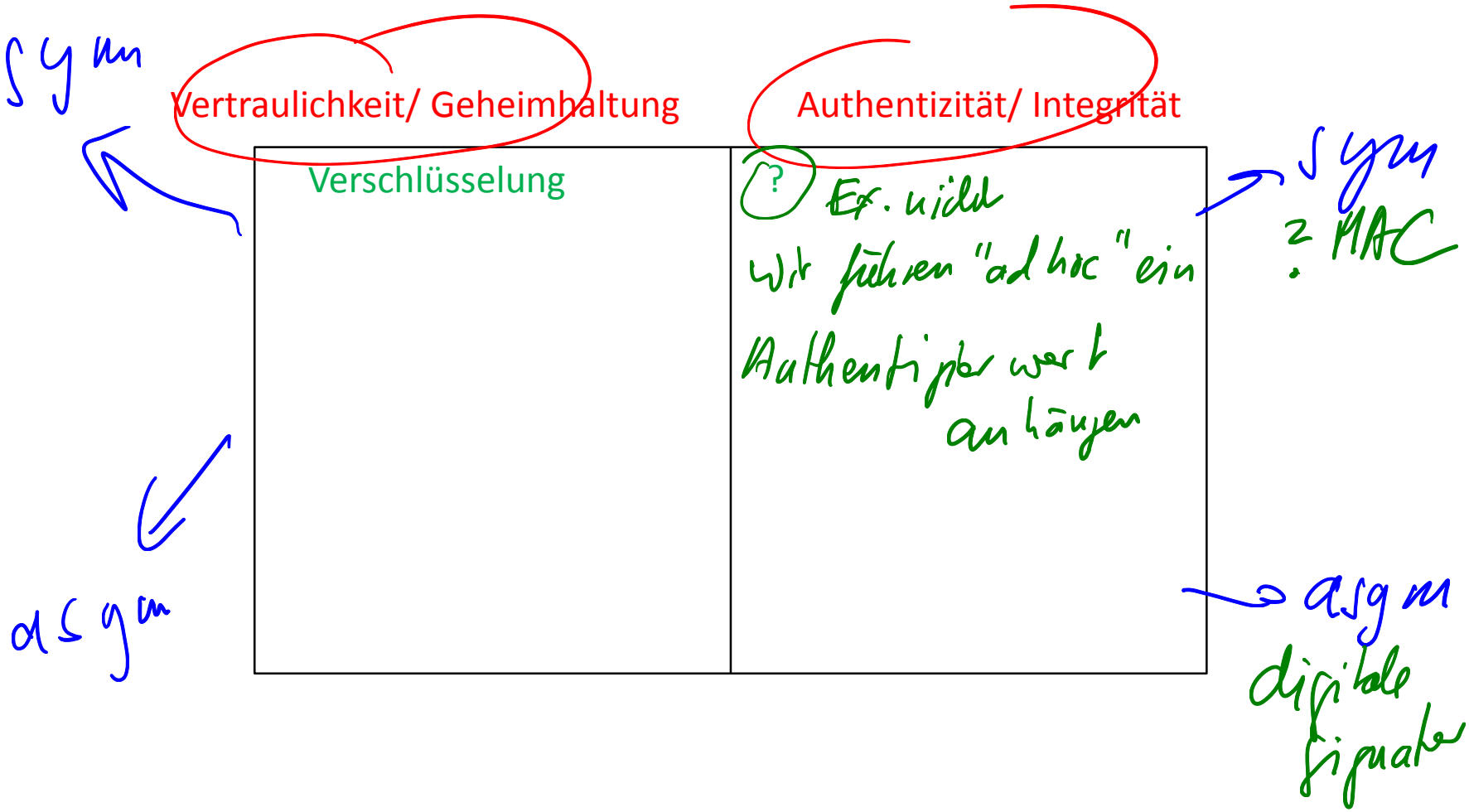
Aufgabe 4.1

a) Ordnen Sie an Alice, Bob und Eve die Begriffe Insider/Outsider Angreifer zu.

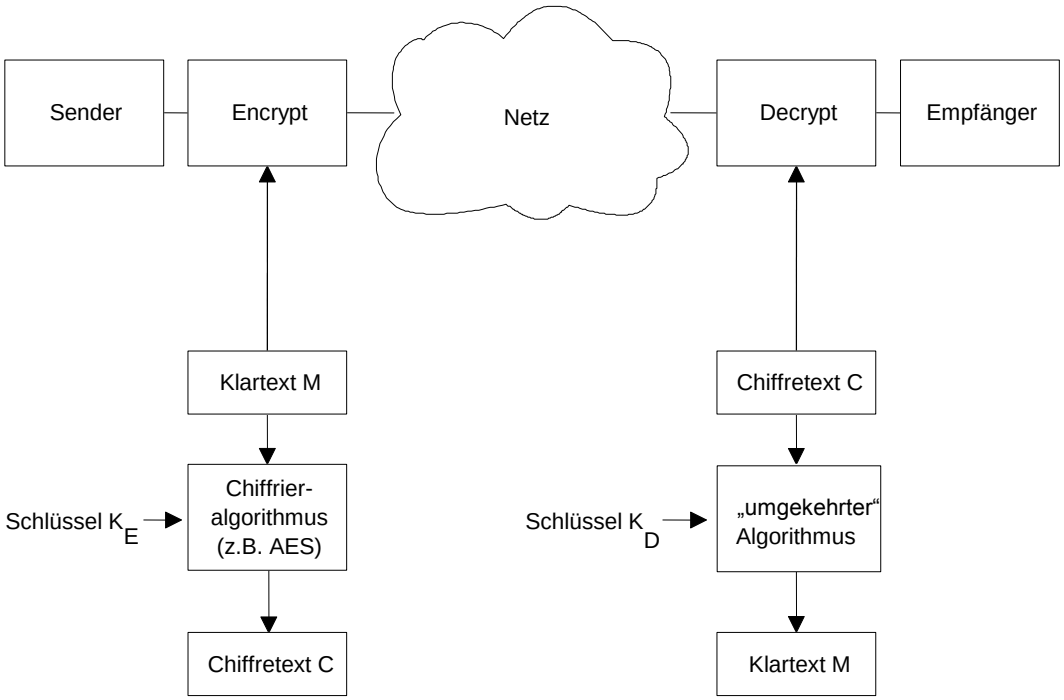
b) Welche der vorhin 8 erwähnten Angriffe sind passive, welche sind aktive?

Siehe auch Bemerkung zur «Traffic Analyse» im JS Skript, Kap. 4.1.2 «Angreifer».

2 Sicherheitsanford. → 2 Schutzmechanismen



Verschlüsselung



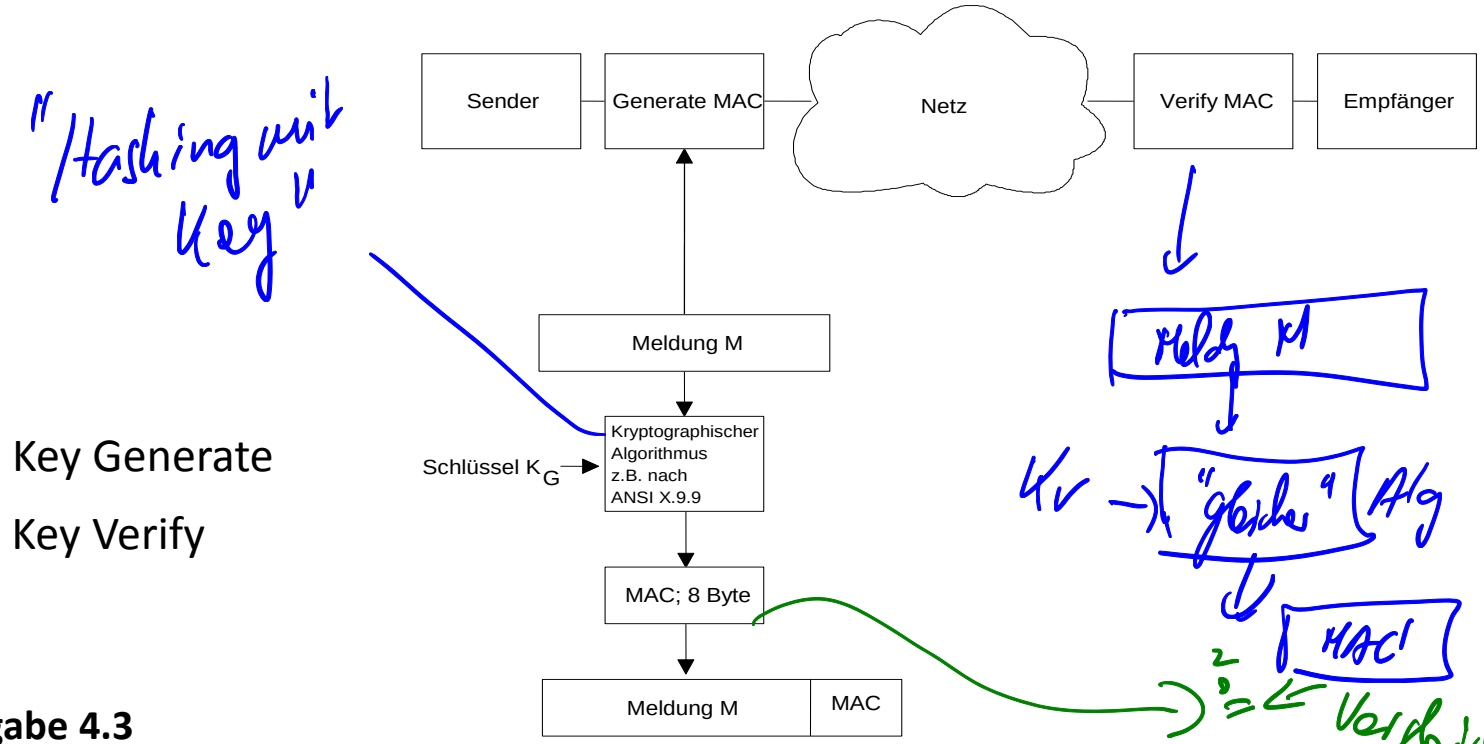
K_E = Key Encrypt

K_D = Key Decrypt

Aufgabe 4.2

- Gilt $K_E = K_D$, dann spricht man von einem symmetrischen Verfahren;
  z.B. AES; 3-DES; u.a.
- Gilt $K_E \neq K_D$, dann spricht man von einem asymmetrischen Verfahren;
  z.B. RSA; ECC
- K_E ist im asymmetrischen Fall der Public Key des Empfängers
  und K_D ist der Secret / Private Key des Empf.

«Authentizierwert anhängen»



K_G = Key Generate

K_V = Key Verify

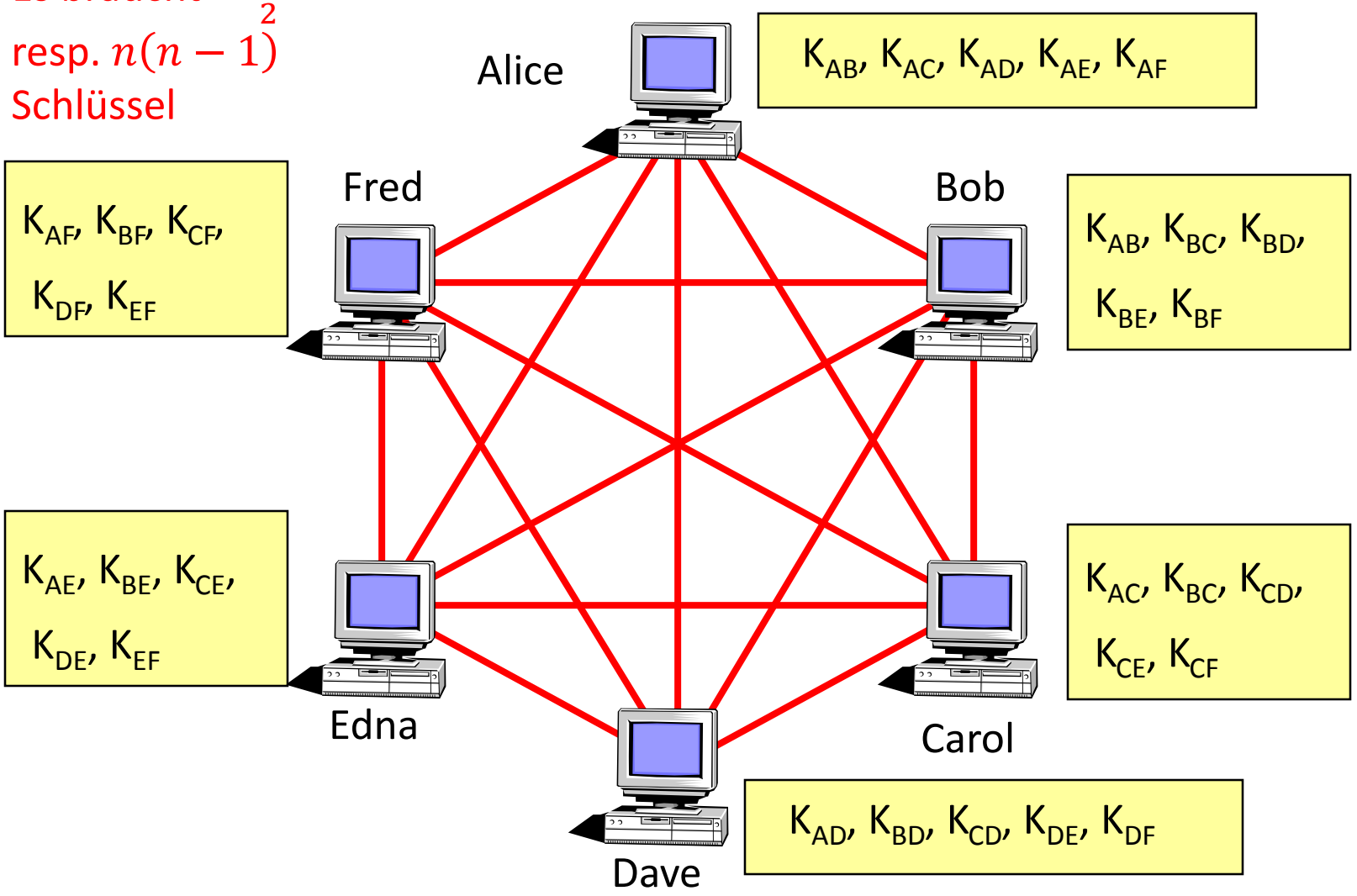
Aufgabe 4.3

- Gilt $K_G = K_V$, dann heisst der Authentizierwert MAC ;
- Gilt $K_G \neq K_V$, dann heisst der Authentizierwert digitaler Signatur,
  z.B. mit RSA, ECC; Schnorr, DSA usw., die beim Signieren
- Für den asymmetrischen Fall ist K_G ist der private Key des Senders,
  und K_V ist der Public Key des Senders

n Computer: symmetrisch Jeder mit Jedem

$O(n^2)$

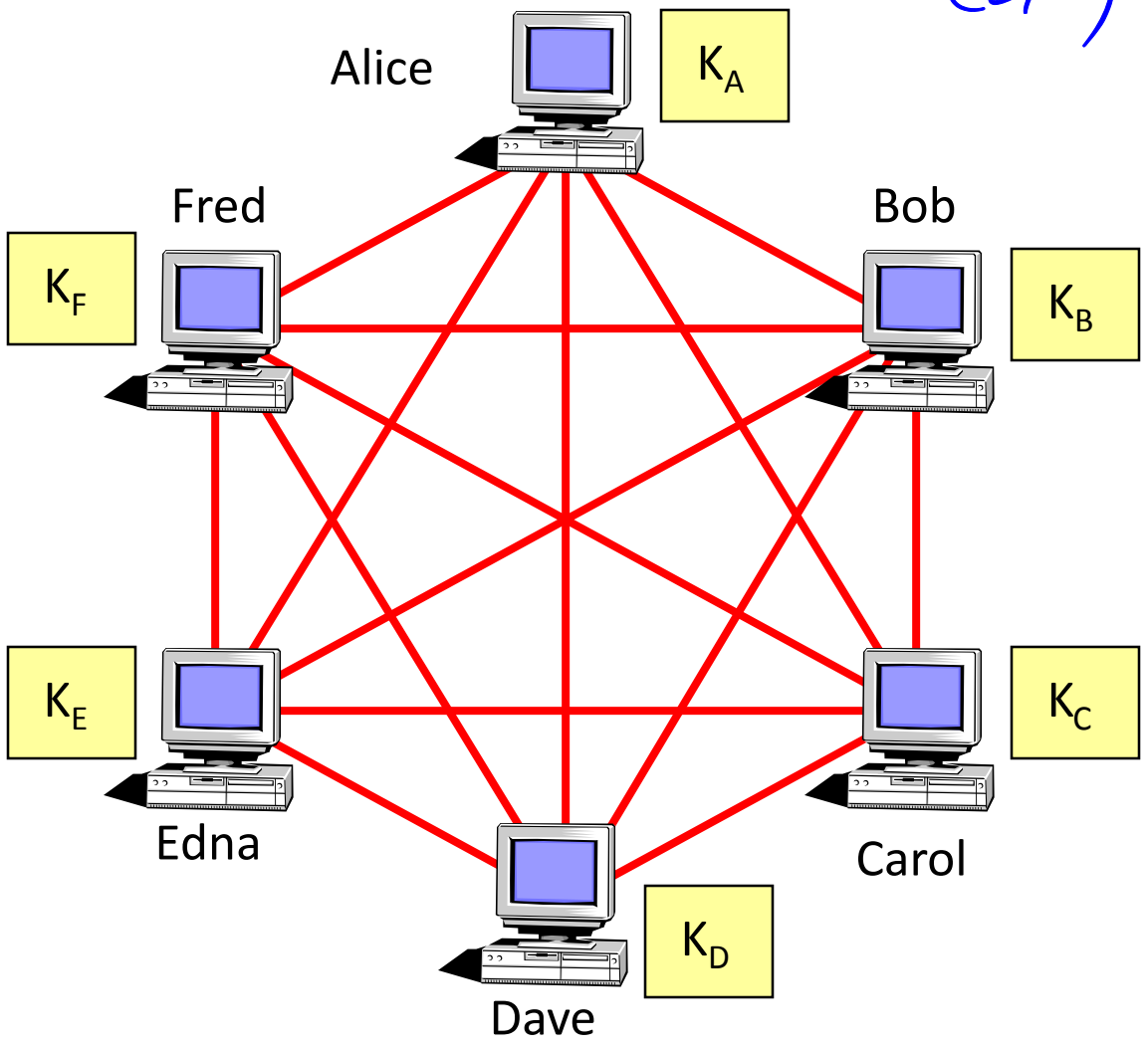
Es braucht $\frac{n(n-1)}{2}$
resp. $n(n-1)$
Schlüssel



n Computer: asymmetrisch Jeder mit Jedem

$O(n)$

Es braucht nur n Schlüsselpaare



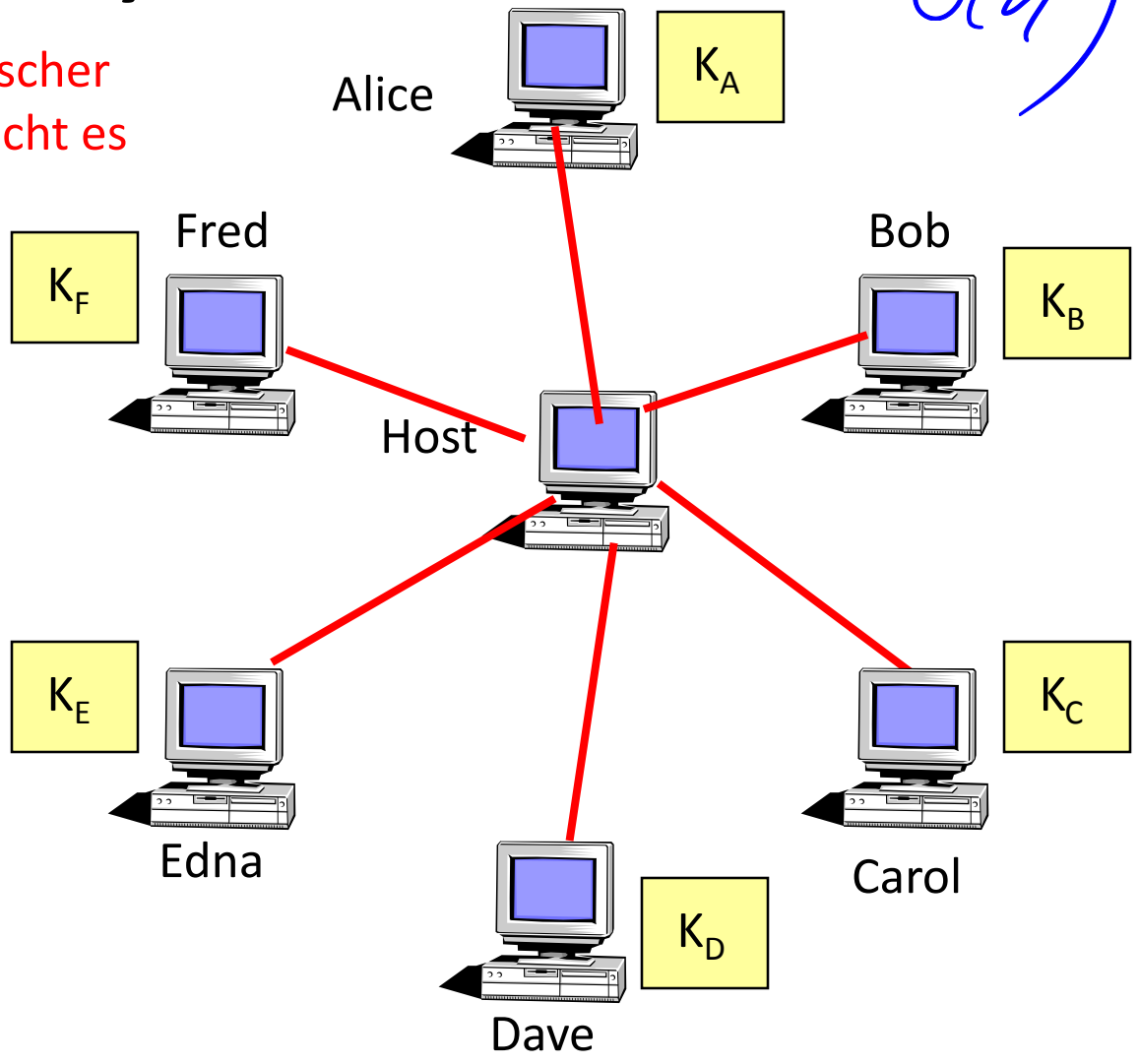
Öffentliches Verzeichnis

Alice	K_A
Bob	K_B
Carol	K_C
Dave	K_D
Edna	K_E
Fred	K_F

Situation in einer Sterntopologie, wie z.B. das Bancomatsystem.

O(n)

Auch mit symmetrischer Kryptographie braucht es nur n Schlüssel



Wichtig zu wissen:

- Bei symmetrischen Verfahren ist es grundsätzlich möglich, dass die Kommunikationsrichtungen A → B und von B → A mit den gleichen Schlüsseln getätigt werden. I.d.R. werden diese Wege aber mit unterschiedlichen Schlüsseln geschützt.
- Bei asymmetrischen Verfahren sind unterschiedliche Schlüssel von A → B und B → A grundsätzlich schon gegeben.
- Pro Dienst (z.B. Verschlüsselung der Meldung, Integritätsschutz, PIN-Verschlüsselung usw.) werden unterschiedliche Schlüssel verwendet. Also z.B. im asymmetrischen Fall ist es nicht erlaubt mit dem gleichen Schlüsselpaar zu Verschlüsseln wie zu Signieren.

Aufgabe 4.4 ***Anzahl Schlüssel beim asymmetrischen und symmetrischen Verschlüsseln.***

1000 Computer sollen so vernetzt werden, dass jeder mit jedem einen separaten Schlüssel hat.

a) Wie viele Schlüssel braucht es mit symmetrischer Kryptographie?
   i. Wenn nur ein Dienst (z.B. Verschlüsselung) gemacht wird und die Wege A → B und B → A die gleichen Schlüssel verwenden?
   ii. Wenn nur ein Dienst (z.B. Verschlüsselung) gemacht wird und die Wege A → B und B → A unterschiedliche Schlüssel verwenden?
   iii. Wenn nur zwei Dienste (z.B. Verschlüsselung & MAC) gemacht werden und die Wege A → B & B → A unterschiedliche Schlüssel verwenden?

b) Wie viele Schlüsselpaare braucht es mit asymmetrischer Kryptographie?
   i. Wenn nur ein Dienst (z.B. Verschlüsselung) gemacht wird und die Wege A → B und B → A die gleichen Schlüssel verwenden?
   ii. Wenn nur ein Dienst (z.B. Verschlüsselung) gemacht wird und die Wege A → B und B → A unterschiedliche Schlüssel verwenden?
   iii. Wenn nur zwei Dienste (z.B. Verschlüsselung & Signatur) gemacht werden und die Wege A → B und B → A unterschiedliche Schlüssel verwenden?

bis 17h00 dann Pause bis 17h10

Kap. 5

VIER EINSCHÜBE

Kap. 5.1 Die Entropie
Kap. 5.2 Passwort, resp. Schlüssel der Grösse 128 Bit
Kap. 5.3 Unterschied zwischen Verfahren und Schlüssel
Kap. 5.4 Einführung in die Hashfunktionen

Kap. 5.1 Entropie = mittlerer Informationsgehalt

Einführungsfrage 1:

Wie viele Bits resp. HEX-Zeichen – also Halbbytes sind da geschrieben?
0110 0011 1100 0001 1111 1000 0000 resp. 63 C1 F8 0
1001 1100 0011 1110 0000 0111 1111 resp. 9C 3D 07 F

Antwort 1: 2·28 = 56 bit resp. 2·7 = 14 Hex

Einführungsfrage 2:

Die obigen zwei Zeilen stellen je einen Schlüssel (oder Passwort) für eine Kryptographische Anwendung dar.

- Welche Schlüsselgrösse wird in dieser Anwendung gebraucht?
- Wie gross ist der Schlüsselraum? D.h. wie viele mögliche Schlüssel gibt es?

Antwort 2: Theoretisch beträgt der Schlüsselraum 28 bit $\Rightarrow 2^{28}$ $\approx$ 268,5 Mio Schlüssel

Die entscheidende Frage 3:

Wir sind unbewusst davon ausgegangen, dass jedes Bit dieses – vermeintlich 28 Bit grossen – Schlüssels zufällig erzeugt wird. Zugegeben, das macht auch Sinn.
Der Zufallszahlengenerator ist defekt. Das erste Bit wird zwar absolut zufällig erzeugt, doch danach werden die restlichen 27 Bit nach einem bestimmten Schema erzeugt.
So kommen wir zur entscheidenden Frage 3:
Wie viele verschiedene Schlüssel werden erzeugt und wie gross ist der Schlüsselraum?

Antwort 3: Nur 2 verschiedene Schlüssel

Die Entropie, ein Zufälligkeitsmass

a) Der Informationsgehalt eines Zeichens x_i wird definiert mit:

$$H(x_i) = -\log_2\big(P(x_i)\big) \overset{Log.Gesetz}{=} \log_2\left(\frac{1}{P(x_i)}\right)$$

b) Die Entropie oder mittlere Informationsgehalt der Nachrichtenquelle wird definiert:

$$H(X) = -\sum_{i=1}^{n} P(x_i)\cdot\log_2\big(P(x_i)\big) = \sum_{i=1}^{n} P(x_i)\cdot\log_2\left(\frac{1}{P(x_i)}\right) = \sum_{i=1}^{n} P(x_i)\cdot H(x_i)$$

c) Falls alle Zeichen gleichwahrscheinlich sind, so nennt man $H(X) = H_0 =$ Entscheidungsgehalt und es gilt:

$$H_0(X) = \log_2(n)$$

d) Die Differenz von Entscheidungsgehalt und Entropie heisst Redundanz R.

$$R(X) = H_0(X) - H(X)$$

e) Die relative Redundanz r

$$r(X) = \frac{R(X)}{H_0(X)} = 1 - \frac{H(X)}{H_0(X)}$$

f) Es gilt die Ungleichung: $0 \le H(X) \le \log_2(n) = H_0(X)$

Die Entropie, ein Beispiel

Wir nehmen an eine gedächtnislose Quelle erzeugt die Buchstaben A, …, H mit den folg. Wahrscheinlichkeiten.

x_i	A	B	C	D	E	F	G	H
$P(x_i)$	$\frac{1}{2}$	$\frac{1}{8}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$
$H(x_i) = -\log_2(P(x_i))$	1	3	4	4	4	4	4	4

b) $$H(X) = -\sum_{i=1}^{8} P(x_i) \cdot \log_2(P(x_i)) = -\left(\frac{1}{2} \cdot \log_2\left(\frac{1}{2}\right) + \frac{1}{8} \cdot \log_2\left(\frac{1}{8}\right) + 6 \cdot \frac{1}{16} \cdot \log_2\left(\frac{1}{16}\right)\right)$$

$$= -\left(\frac{1}{2} \cdot (-1) + \frac{1}{8} \cdot (-3) + 6 \cdot \frac{1}{16} \cdot (-4)\right) = -\left(-\frac{1}{2} - \frac{3}{8} - \frac{3}{2}\right) = \frac{19}{8} = 2{,}375$$

Resp.

$$H(X) = \sum_{i=1}^{8} P(x_i) \cdot H(x_i) = \left(\frac{1}{2} \cdot 1\right) + \left(\frac{1}{8} \cdot 3\right) + 6 \cdot \left(\frac{1}{16} \cdot 4\right) = \frac{1}{2} + \frac{3}{8} + \frac{3}{2} = \frac{19}{8}$$

$$= 2{,}375$$

→ Alle Zeichen kommen mit Wsk. 1/8 vor

c) $H_0(X) = \log_2(8) = 3$

d) $R(X) = H_0(X) - H(X) = 3 - \frac{19}{8} = \frac{5}{8} = 0{,}625$ Redundanz

e) $r(X) = \frac{R(X)}{H_0(X)} = \frac{0{,}625}{3} = \frac{5}{24}$ resp. $r(X) = 1 - \frac{H(X)}{H_0(X)} = 1 - \frac{2{,}375}{3} = 1 - \frac{19}{24} = \frac{5}{24}$

f) Check der Ungleichung $0 \leq H(X) \leq \log_2(n) = H_0(X)$ ist erfüllt, da $0 \leq 2{,}375 \leq \log_2(n) = 3$

Die Entropie, eine Aufgabe

Aufgabe 5.1 Füllen Sie die letzte Zeile und lösen Sie b) – f)

x_i	A	B	C
$P(x_i)$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$
$H(x_i) = -\log_2(P(x_i))$	1	2	2

b) $H(X) =$

c) $H_0(X) =$

d) $R(X) =$

e) $r(X) =$

f) Check der Ungleichung:

Kap. 5.2 Passwort resp. Schlüssel mit 128 Bit

Die Frage: Was ist der Unterschied zwischen einem Passwort und einem Schlüssel?
Antwort: Sind im Wesentlichen synonym. Ein kryptographischer Schlüssel wird aber in aller Regel in HEX-Zeichen dargestellt, ein Passwort oft in anderen Codierungen.

<u>Codierungen, die Anzahl Bit pro Zeichen und je ein Beispiel</u>

1. 10 verschiedene Digits (0, ..., 9): 39 digits * 3.32 bits/digits (*)
   39475 10485 98021 43380 05872 49759 70291 2634

2. 16 verschiedene Hexadecimal (0, ..., F): 32 nibbles * 4 bits/nibble (**)
   3F8A 84D1 EA7B 5092 C64F 8EA6 73BD F01B

3. 26 verschiedene Buchstaben im Alphabet (A, ..., Z): 28 characters * 4.7 bits/character (*)
   AWORH GHJBP IUCMX MLZFQ TZDOP ZJV

4. 36 verschiedene Werte (A, ..., Z, 0, ..., 9): 25 symbols * 5.17 bits/symbol (*)
   E5RGL UPQ7A 8F3ZP NWTIC 22JBM

5. 64 verschiedene Werte Base64 (A...Z, a...z, 0...9, /, +): 22 symbols * 6 bits/symbol (*) & (***)
   y5GNa Riq92 VCm4Q 1BOKl x0

(*) Der Wert ist leicht über 128 Bit.
(**) Nibble = Halbbyte (in der HEX Codierung)
(***) Die Base64 Codierung ist in der nächsten Folie aufgeführt.

<u>Beispiel:</u>

Für die Berechnung, dass die 10 Digits 3,32 Bit Information brauchen, muss die Gleichung $2^x = 10$ gelöst werden. Die Lösung lautet: $x = \log_2 10 = \frac{lg10}{lg2} = 3{,}32$. Für 128 Bit braucht es $\frac{128}{3{,}32} = 38{,}55$, also 39 Zeichen.

Aufgabe 5.2 Wie gross ist kryptographische Stärke einer 6-stelligen PIN?

Base 64 Codierung

Base64-Zeichensatz

Wert			Zeichen	Wert			Zeichen	Wert			Zeichen	Wert			Zeichen
dez.	binär	hex.		dez.	binär	hex.		dez.	binär	hex.		dez.	binär	hex.	
0	000000	00	A	16	010000	10	Q	32	100000	20	g	48	110000	30	w
1	000001	01	B	17	010001	11	R	33	100001	21	h	49	110001	31	x
2	000010	02	C	18	010010	12	S	34	100010	22	i	50	110010	32	y
3	000011	03	D	19	010011	13	T	35	100011	23	j	51	110011	33	z
4	000100	04	E	20	010100	14	U	36	100100	24	k	52	110100	34	0
5	000101	05	F	21	010101	15	V	37	100101	25	l	53	110101	35	1
6	000110	06	G	22	010110	16	W	38	100110	26	m	54	110110	36	2
7	000111	07	H	23	010111	17	X	39	100111	27	n	55	110111	37	3
8	001000	08	I	24	011000	18	Y	40	101000	28	o	56	111000	38	4
9	001001	09	J	25	011001	19	Z	41	101001	29	p	57	111001	39	5
10	001010	0A	K	26	011010	1A	a	42	101010	2A	q	58	111010	3A	6
11	001011	0B	L	27	011011	1B	b	43	101011	2B	r	59	111011	3B	7
12	001100	0C	M	28	011100	1C	c	44	101100	2C	s	60	111100	3C	8
13	001101	0D	N	29	011101	1D	d	45	101101	2D	t	61	111101	3D	9
14	001110	0E	O	30	011110	1E	e	46	101110	2E	u	62	111110	3E	+
15	001111	0F	P	31	011111	1F	f	47	101111	2F	v	63	111111	3F	/

Kap. 5.3 Unterschied zw. Verfahren & Schlüssel

HA

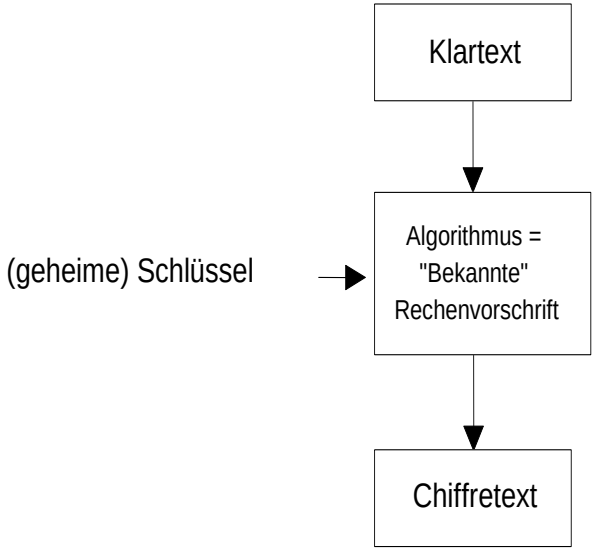
Beispiel:

Der Algorithmus sei die folgende aus 4 Schritten bestehende Rechenvorschrift:

1) Multipliziere die Klartextzahl mit der ersten Ziffer des Schlüssels.
2) Addiere zum Resultat die zweite Ziffer des Schlüssels.
3) Dividiere das Resultat mit der dritten Ziffer des Schlüssels.
4) Subtrahiere vom Resultat die vierte Ziffer des Schlüssels.
5) Das erhaltene Resultat ist die verschlüsselte Zahl

Sei nun 12 die Klartextzahl und 3624 der Schlüssel:

1) 12 x 3 = 36
2) 36 + 6 = 42
3) 42 ÷ 2 = 21
4) 21 – 4 = 17
5) 17 ist die verschlüsselte (chiffrierte) Zahl.



Aufgabe 5.3

Schreiben Sie je für den Papierstreifen der Spartaner und die Verschlüsselung von Cäsar auf, welches der Schlüssel und welches der Algorithmus ist.

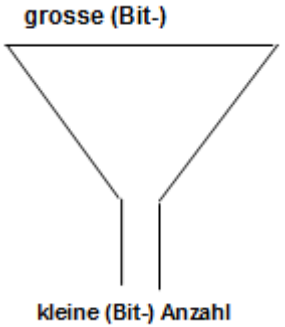
Kap. 5.4 Einführung in die Hashfunktionen

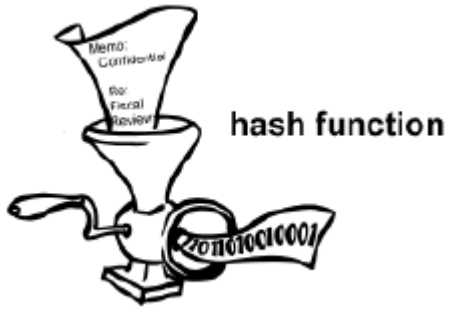
Präsenz 1 wird das im Skript → HA einmal durchlesen

Definition 1:

Unter einer ***Hashfunktion*** verstehen wir eine Funktion, die die Elemente von einer „grossen“ Menge in eine „kleine“ abbildet.

Wir können uns diese Funktion als Trichter Mit beliebiger grossen Inputgrösse vorstellen.

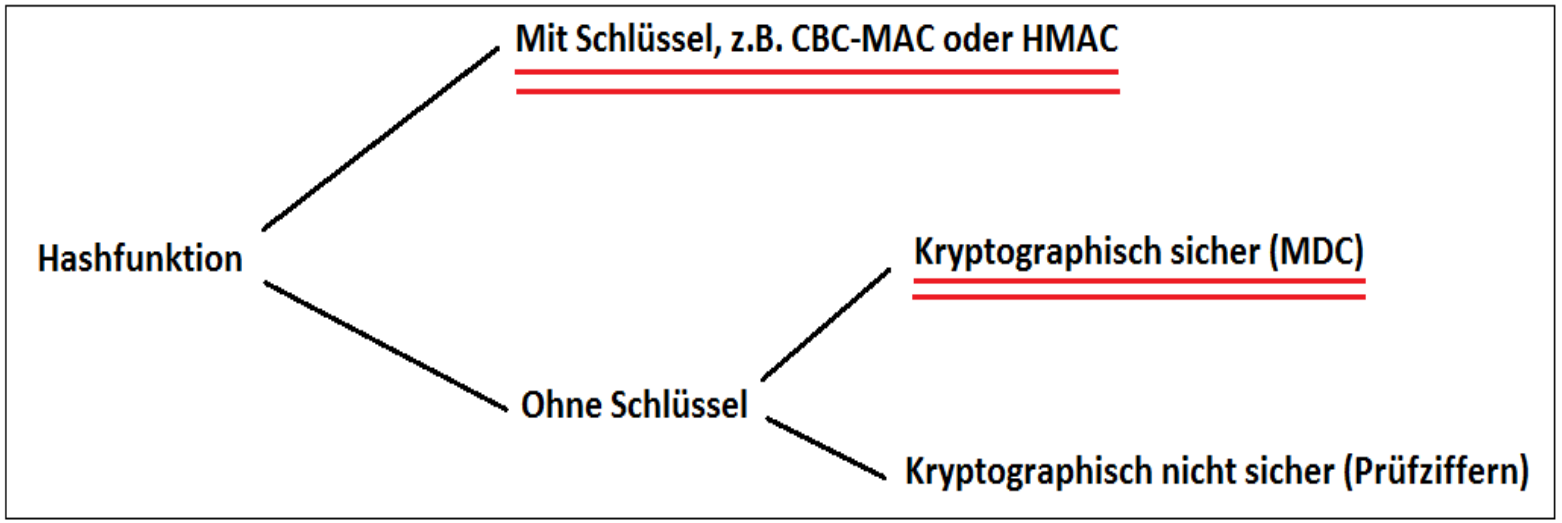




Beispiele:

- Parity-Bit: Outputgrösse ist 1 Bit.
- Meldung Byteweise zusammenzählen (mod 256): Outputgrösse ist 8 Bit.
- CRC: Outputgrösse ist je nach Polynom 16, 32 oder 64 Bit.
- Hashfunktion = keyless hash function z.B. MD-5, SHA-1, RIPEMD, SHA-2 & SHA-3 Familie: Outputgrösse ist je nach Hashfunktion 128, 160, 256, 512 Bit.
- HMAC = Keyed Hash function = Konstruktion mit Hashfunktion und zugefügtem Schlüssel: Outputgrösse ist je nach Hashfunktion 128, 160, 256, 512 Bit.
- MAC z.B. nach ANSI X9.9 (= CBC-MAC) und ähnliche: je nach Blockalgorithmus, 64 oder 128 Bit.
- Konventionelle Prüfsummen (z.B. Bei Barcodelesern)

Einführung in die Hashfunktionen, Übersicht



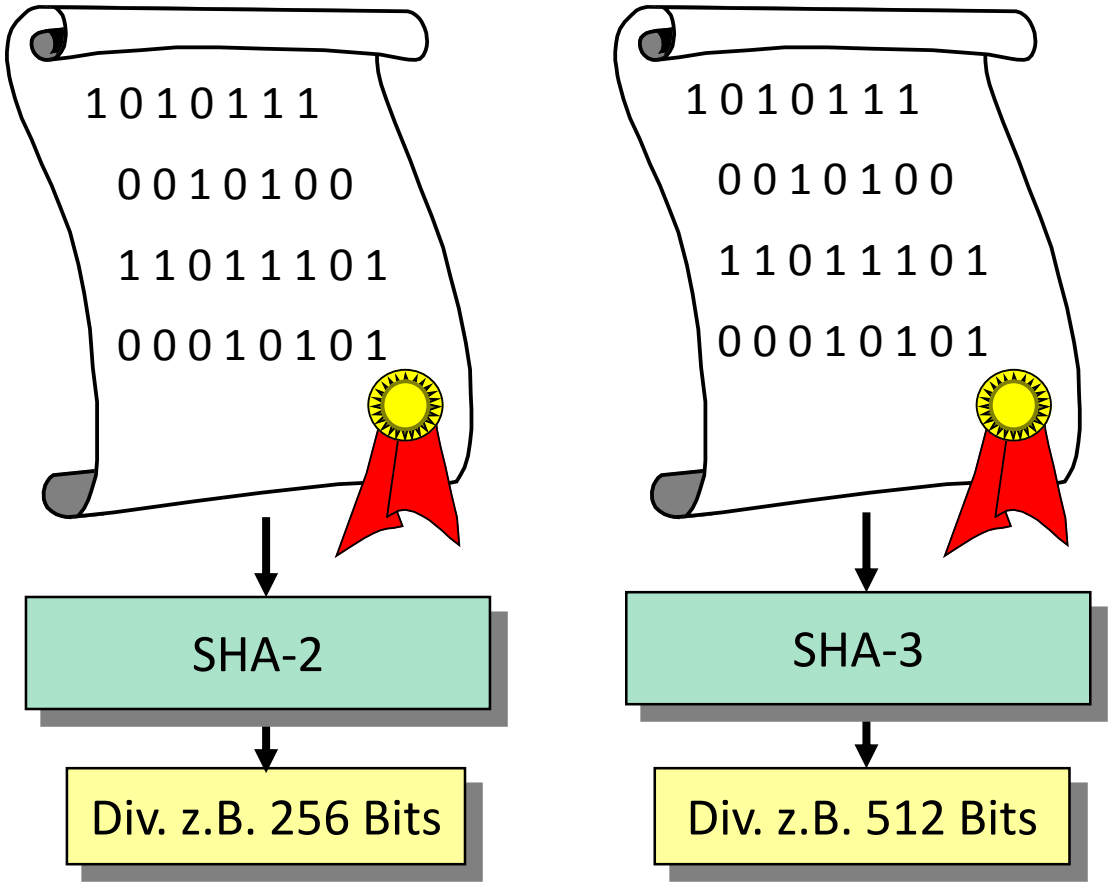
MDC = Manipulation Detection Code

Definition 2:

Unter einer ***kryptographisch sicheren Hashfunktion*** verstehen wir eine Hashfunktion, für die es „schwierig“ ist, zwei Elemente aus der „grossen“ Menge zu finden, die die gleichen Werte in der „kleinen“ haben.

Schlüssellose kryptographisch sichere Hashfunktionen sind notwendige Hilfsmittel

Dokument
oder
Meldung

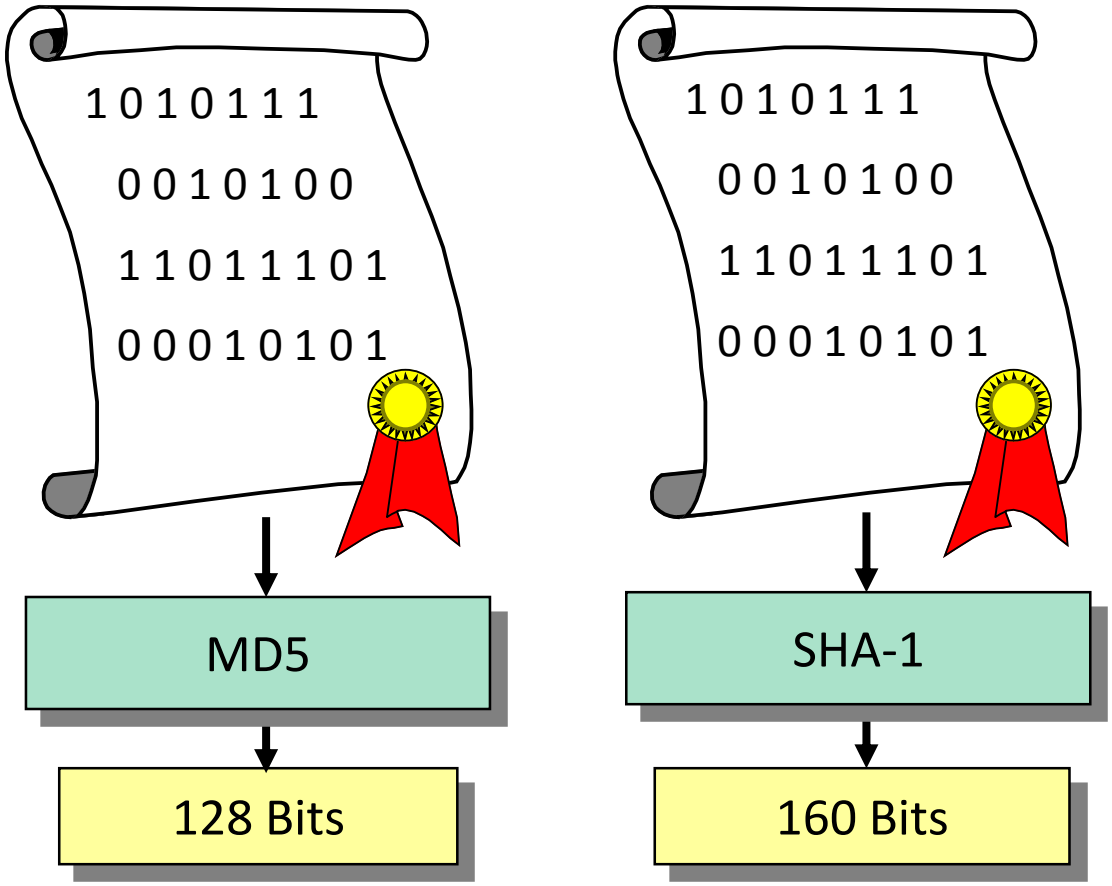


Hash Funktion

Message Digest MD
oder Hash
oder Fingerprint

Diese schlüssellosen Hashfunktionen dürfen für Signaturen nicht mehr verwendet werden

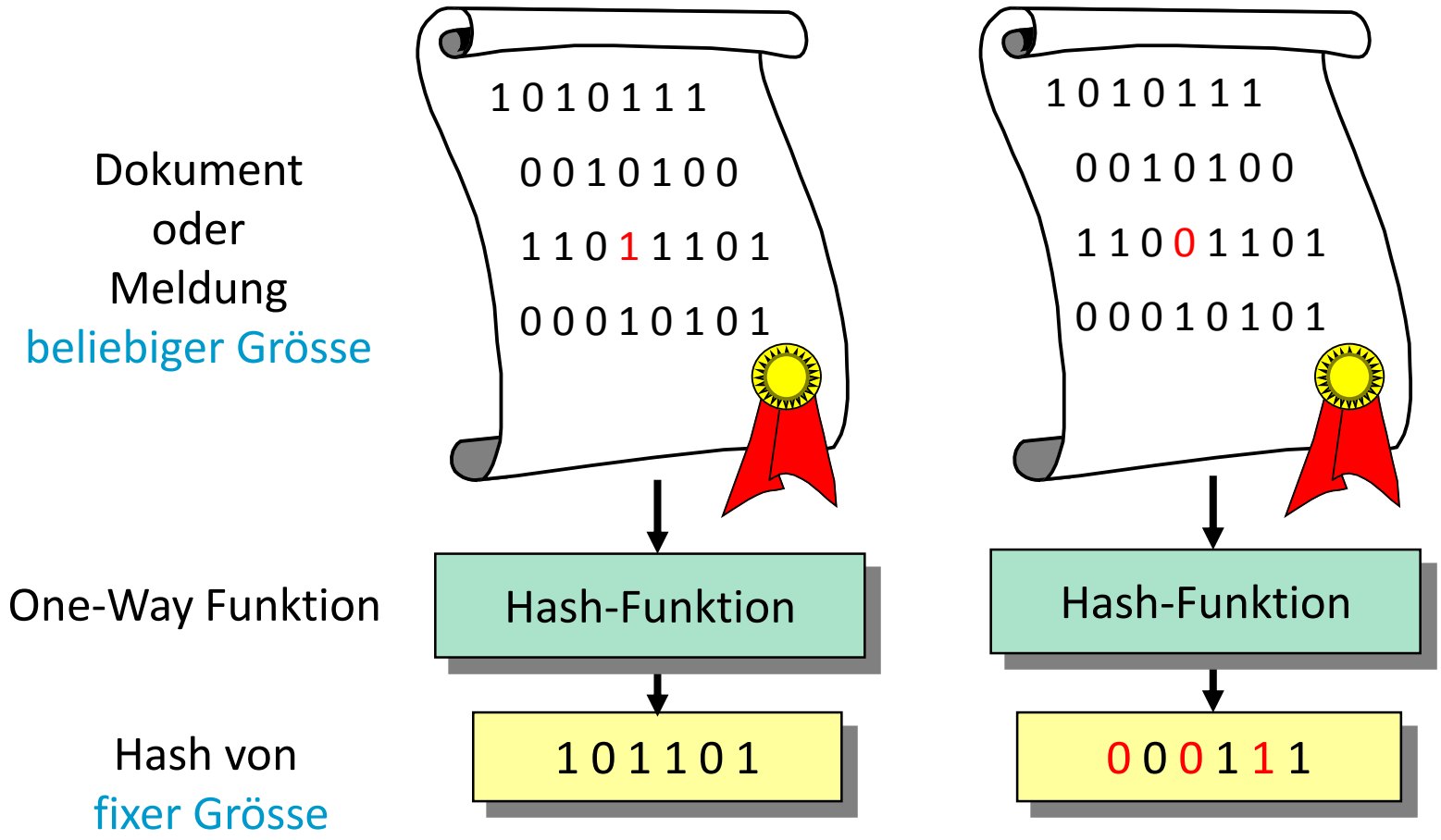
Dokument
oder
Meldung



Hash Funktion

Message Digest MD
oder Hash
oder Fingerprint

Wichtige Eigenschaft einer solchen Hashfunktion

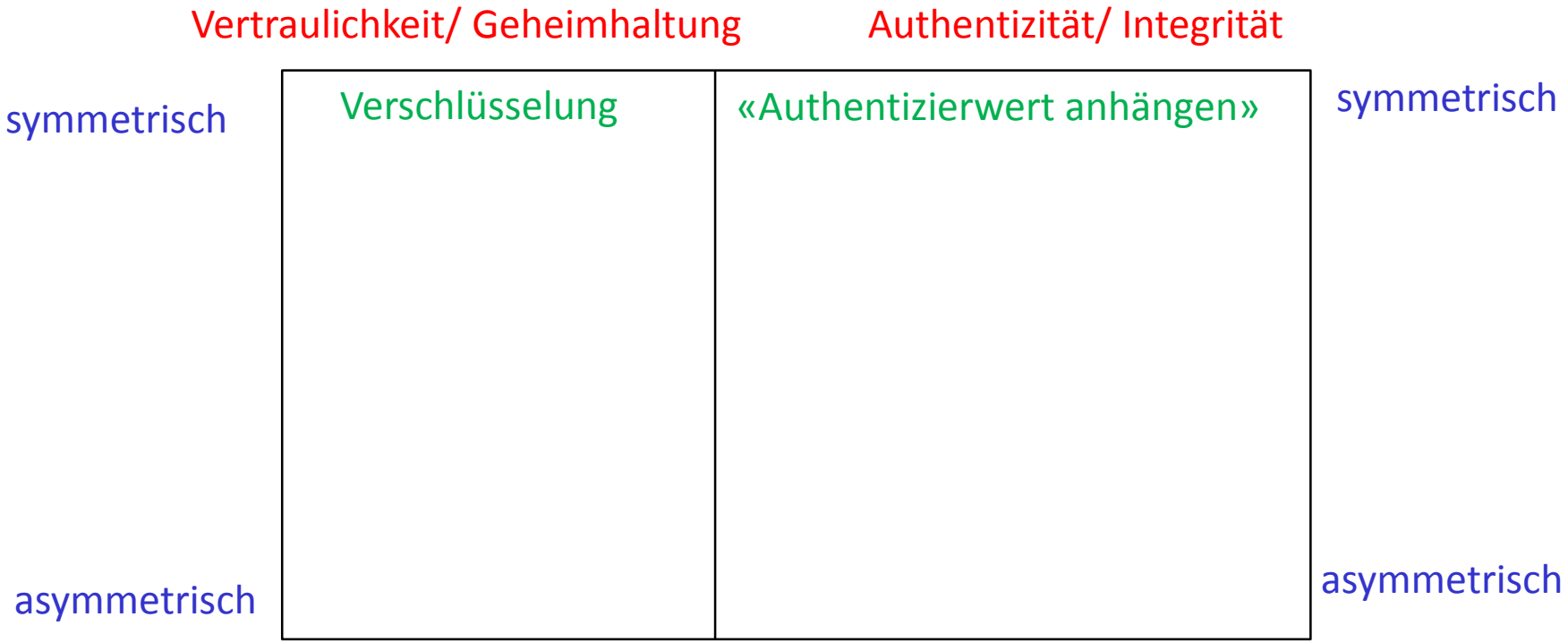


- Das Ändern eines einzigen Bits im Dokument hat zur Folge, dass im statistischen Mittel ca. 50% der Bits im Hash geändert werden.

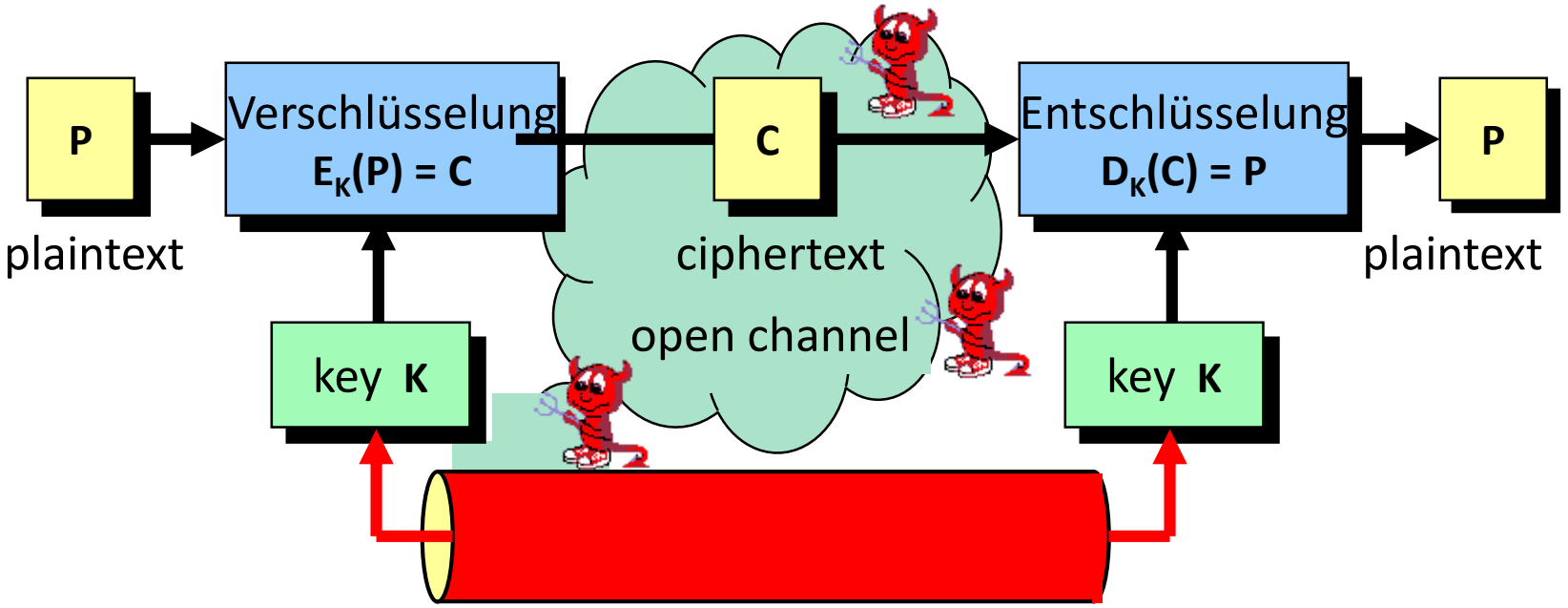
Kap. 6

DIE VERSCHIEDENEN PRINZIPIEN

*2 Sicherheitsanford. → 2 Schutzmechanismen → 2*2 = 4 Prinzipien*



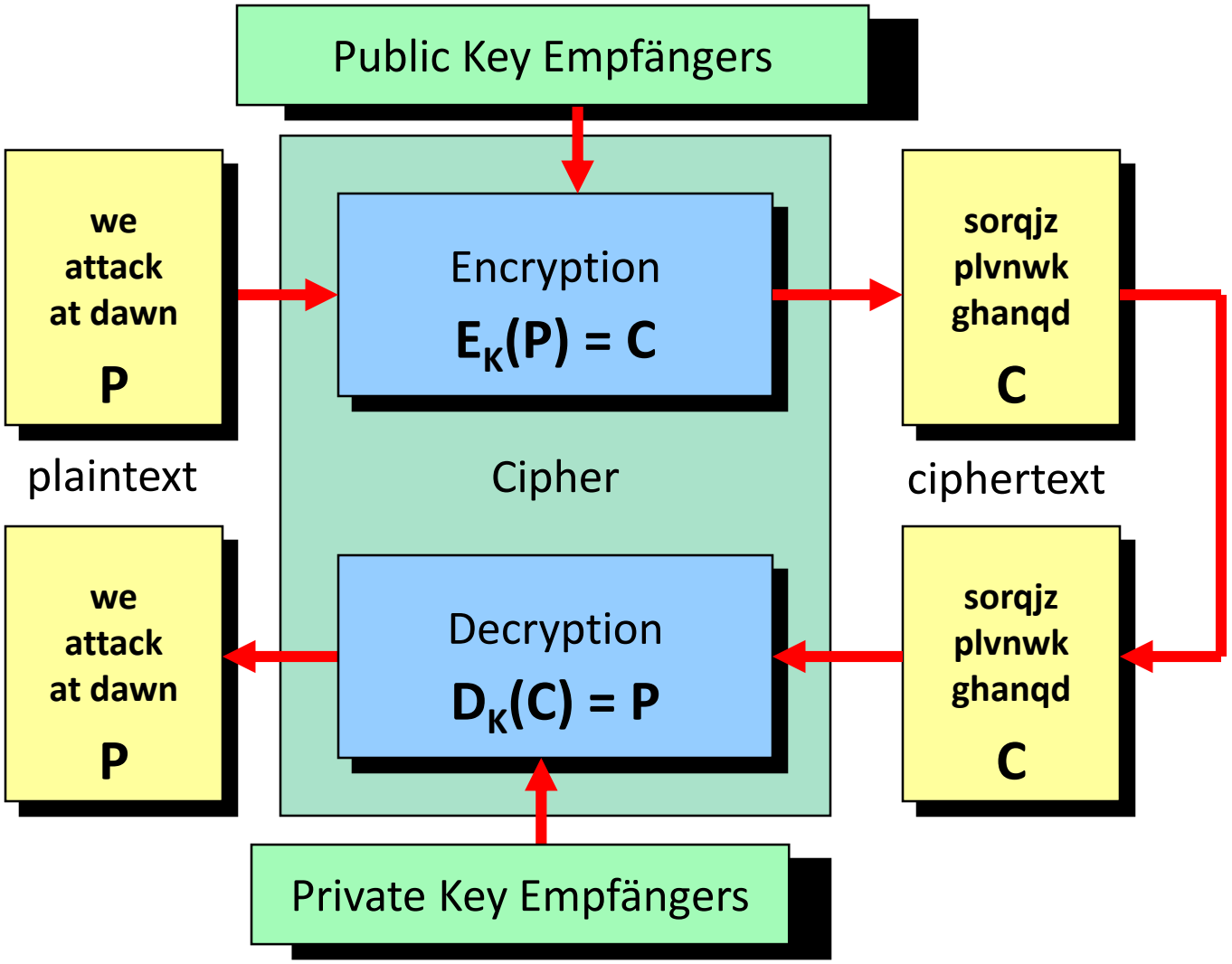
Secret Key Krypto 1: Symmetrische Verschlüsselung



Der geheime Schlüssel muss über einen sicheren Kanal verteilt werden!

- Gleicher Schlüssel für Verschlüsselung und Entschlüsselung
- Schlüssel muss unbedingt geheim gehalten sein
- Grösstes Problem: Sichere Schlüsselverteilung!
- Grösster Vorteil: Schnell!
- Mit der symmetrischen Verschlüsselung kann nur das Abhören verhindert werden. Resp. es kann nur Geheimhaltung ***nicht*** aber Integrität erreicht werden!!!

Public Key Kryptografie 1: Asym. Verschlüsselung



Public Key Verschlüsselung: Key Words

- Asymmetrische Verschlüsselung
- Öffentlicher Schlüssel des Empfängers: zum Verschlüsseln von Daten
- Privater Schlüssel des Empfängers: zum Entschlüsseln von Daten
- Grösstes Problem: ca. 1000-mal langsamer als sym. Alg.
- Grösster Vorteil: «Einfaches Key Management»
- $\frac{n^2}{2}$ (genauer $\frac{n(n-1)}{2}$) Schlüssel bei symmetrischen Verfahren versus n Schlüsselpaare bei asymmetrischen Verfahren
- Mit der asymmetrischen Verschlüsselung kann ebenfalls nur das Abhören verhindert werden. Resp. es kann nur Geheimhaltung ***nicht*** aber Integrität erreicht werden!!!

Aufgabe 6.1: ***Weder asymmetrisch noch symmetrisch Verschlüsseln sondern …***
Wie werden grosse Dateien asymmetrisch verschlüsselt ausgetauscht?

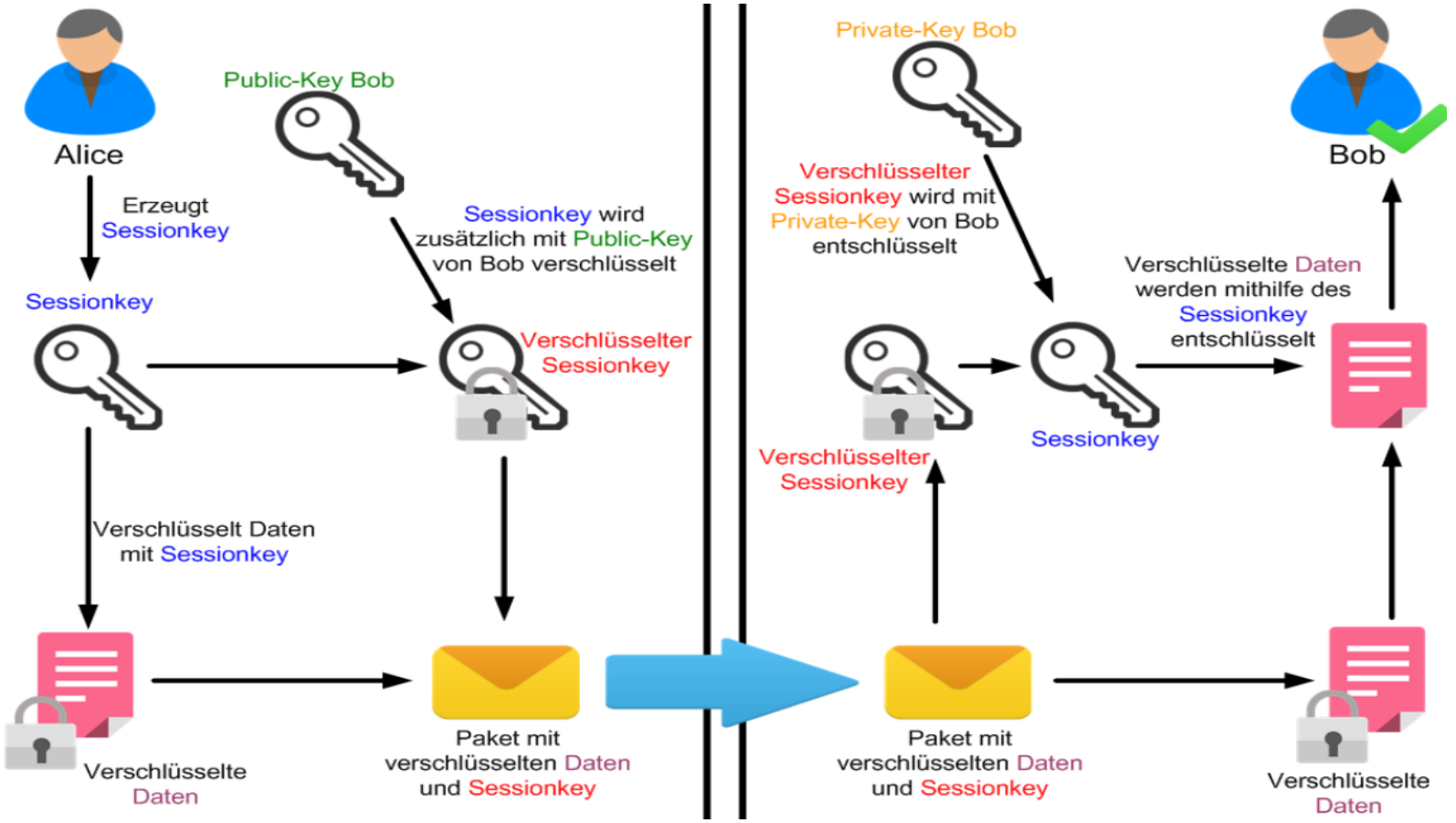
Public Key Krypto. 2: Hybridverschlüsselung

Problem: Grosse Daten können nicht asymmetrisch verschlüsselt werden.

Lösung: Die Hybridverschlüsselung

- Erzeugung eines zufällig gewählten symmetrischen Session Key‘s (cf. z.B. mit Randomfunktion in Kap. 8.4 im JS Skript „Einführung in die Kryptologie“)
- Die Dokumenten- oder Meldungsverschlüsselung wird mit symmetrischen Verfahren durchgeführt.
- Der verwendete symmetrische Schlüssel wird mit einem asymmetrischen Verfahren verschlüsselt und mitgeschickt.
- Vorteile:
  - „Einfaches“ Key Management (cf. asymmetrisches Verfahren).
  - Die bessere Performance der symmetrischen Verfahren wird mit der besseren Schlüsselverteilung der asymmetrischen Verfahren kombiniert.

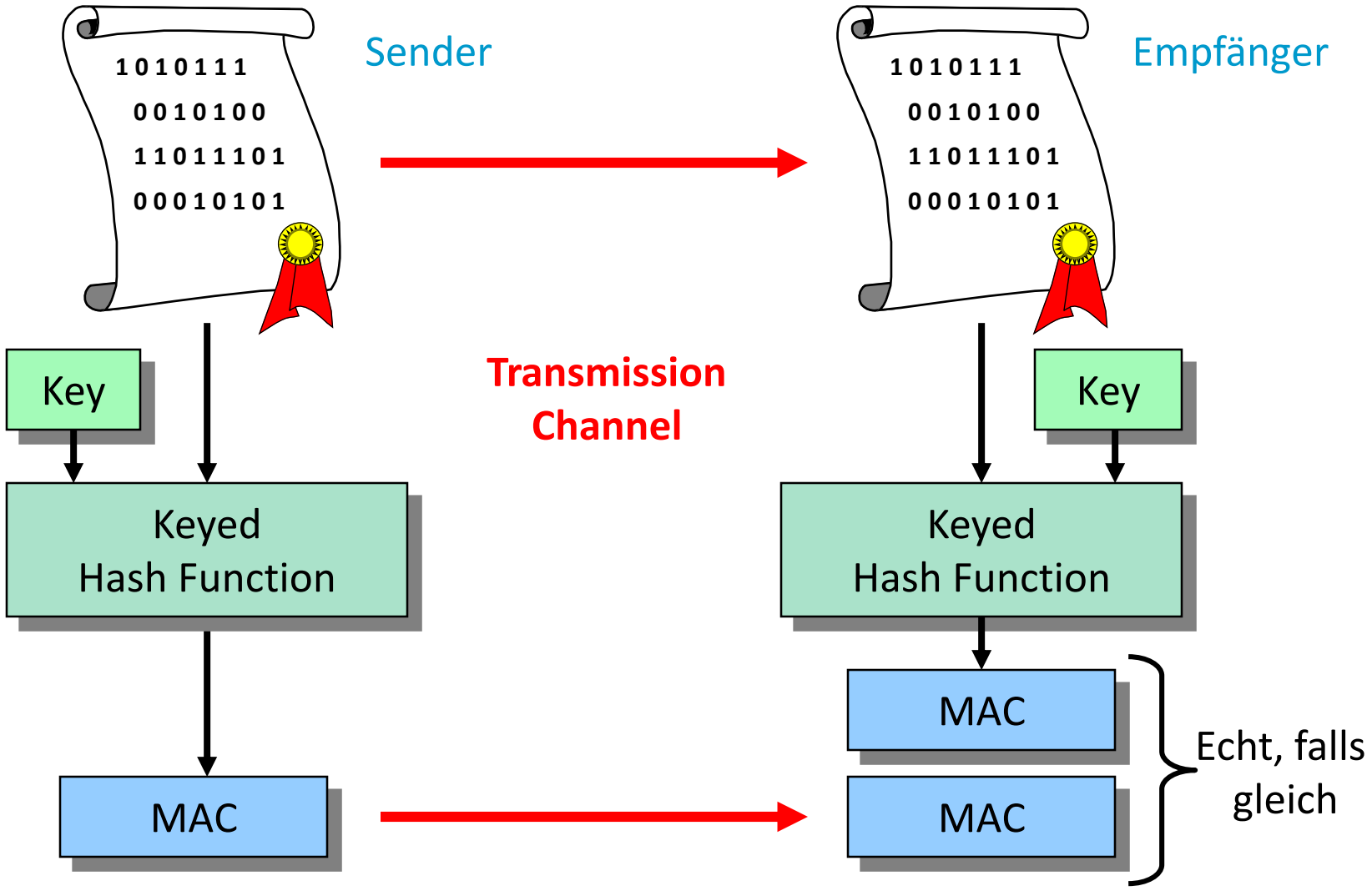
Public Key Krypto. 2: Hybridverschlüsselung



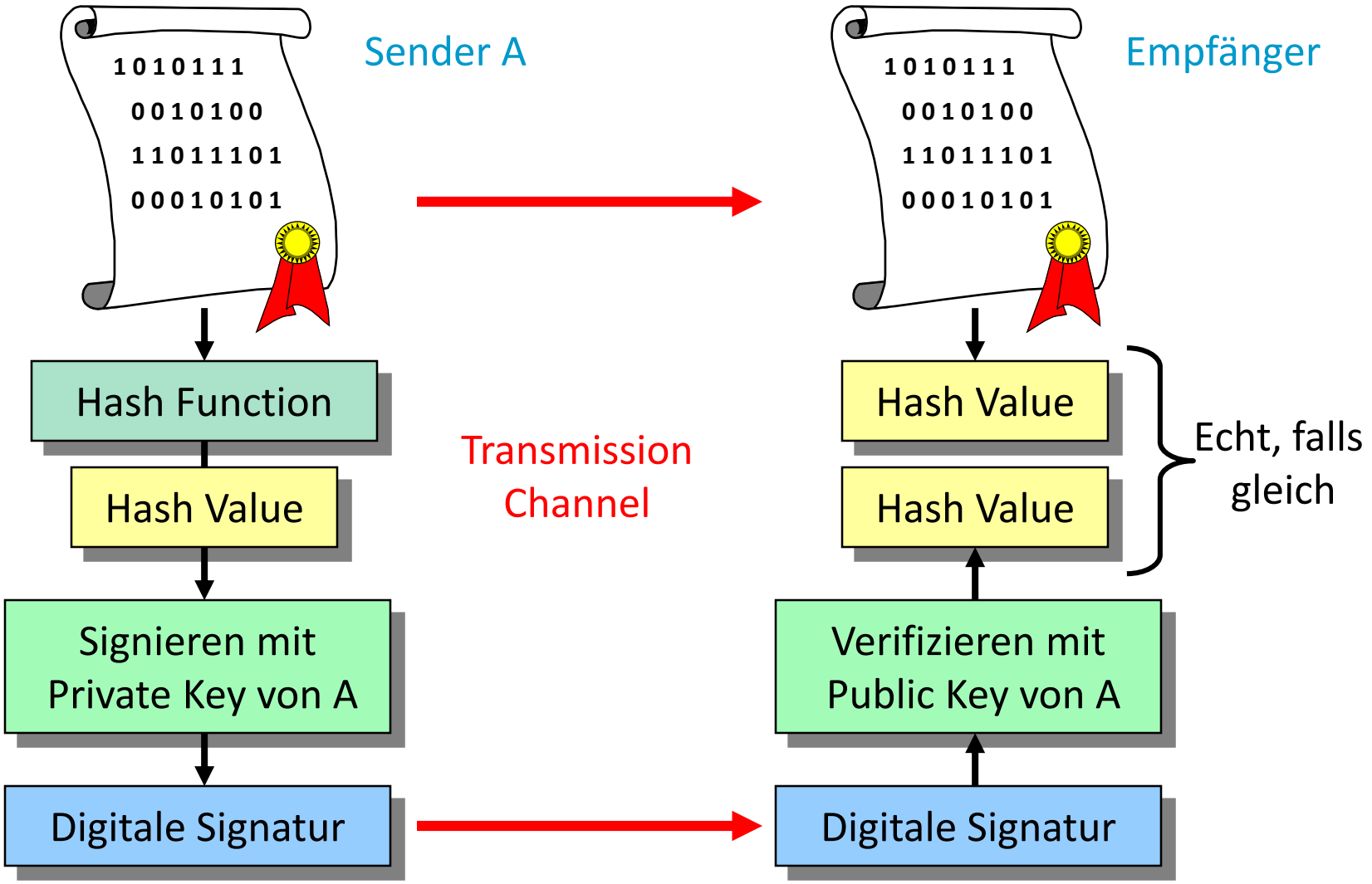
Aufgabe 6.2

Was müssen Sie (resp. das Programm) zwangläufig machen, wenn Sie das Dokument gleichzeitig an zwei unterschiedliche Personen verschicken wollen? Sie wollen aber unbedingt vermeiden, dass das **Dokument** zweimal unterschiedlich verschlüsselt wird.

Secret Key Kryptografie 2: MAC-Berechnung



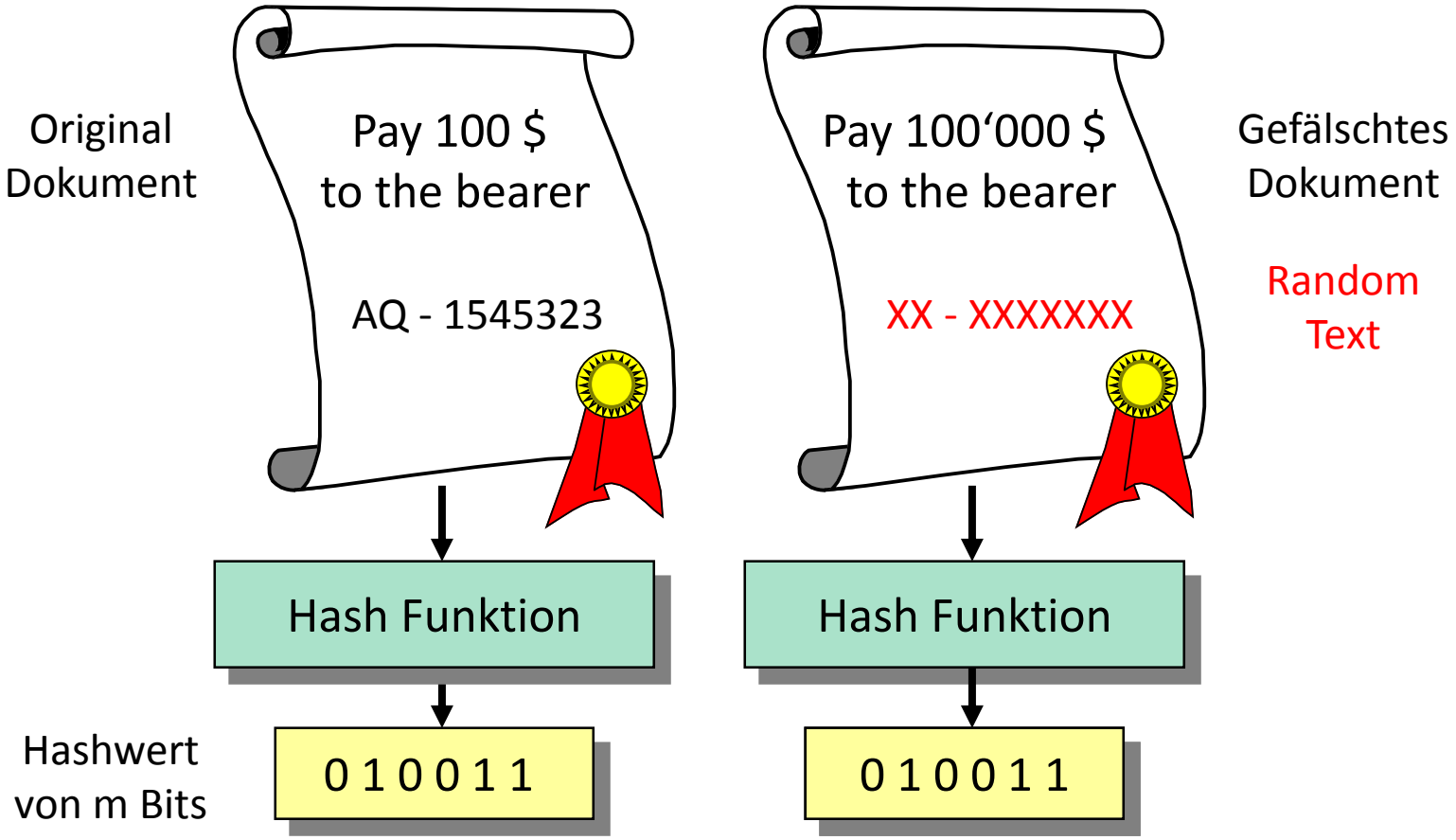
Public Key Krypto. 3: Digitale Signatur (z.B. RSA)



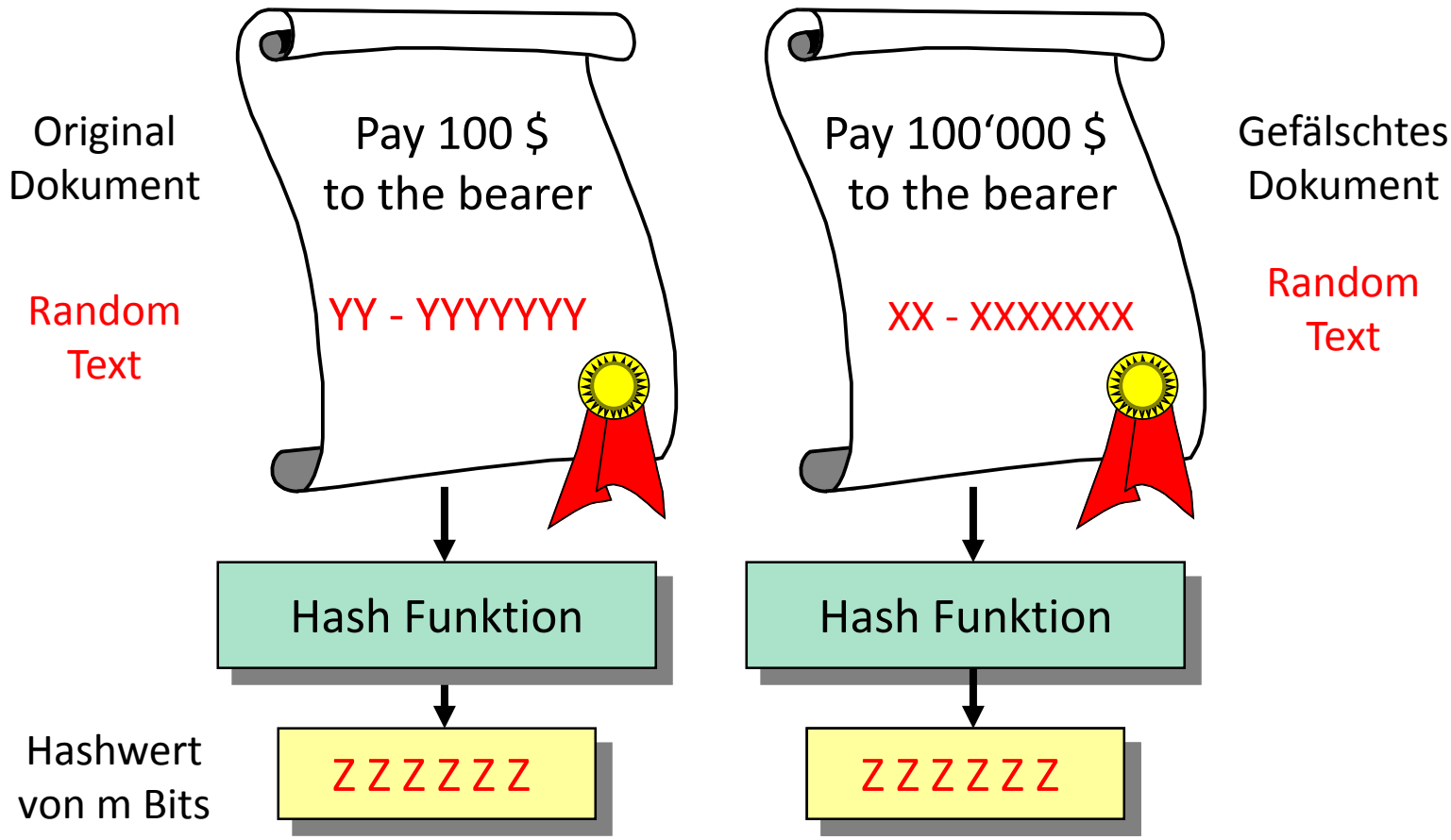
MAC-Berechnung & Digitale Sig.: Key Words

- MAC-Berechnung
  - Gewährt resp. vor
    - Integrität
    - Insertion
- Digitale Signatur
  - Privater Schlüssel des Senders: zum Signieren (= Berechnen der digitalen Unterschrift) der Daten/Dokumente.
  - Öffentlicher Schlüssel des Senders: zum Verifizieren der Unterschrift.
  - Gewährt resp. vor
    - Integrität
    - Insertion
    - Non repudiation of origin!!

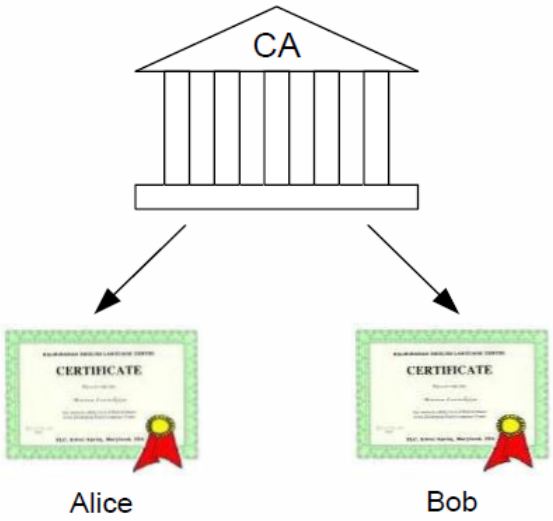
Die Gefahr 1: Pre-Image Angriff: Fälschen von Dokumenten



Die Gefahr 2: Kollisionsangriff: Fälschen von Dokumenten



Woher kommen nun diese Schlüssel?



Vertrauenswürdige Institution
=
Zertifizierungsstelle
=
Certificate Authority (CA)

Siehe Präsenz zu PKI in der Präsenz 11

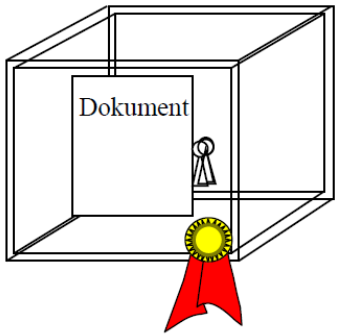
Aufgabe 6.3 *Bedrohung/Massnahmen Kataster, Teil 1*

Bedrohungen / Massnahmen	Meldung Abhören	Meldung Verändern	Neue Meld. Erfinden	Abstreiten Meldung geschickt zu haben
Symmetrische Verschlüsselung				
Asymmetrische Verschlüsselung				
MAC-Berechnung (sym.)				
Digitale Signatur (asym.)				

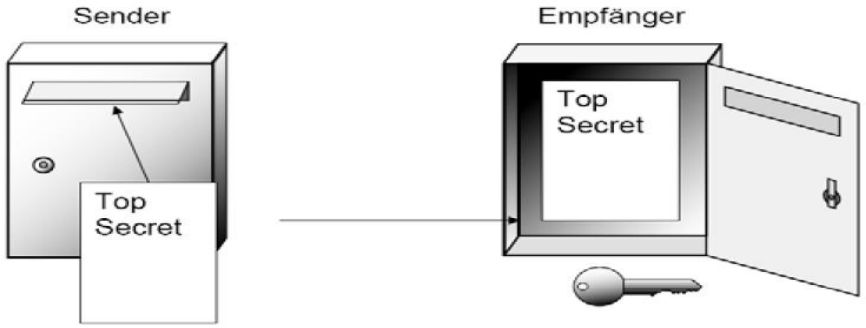
Aufgabe 6.4 *Mechanische Analoga*

Unten sind 4 mechanische Analogon angegeben, erklären Sie das passende Kryptosystem! Welches Prinzip wird nicht dargestellt?

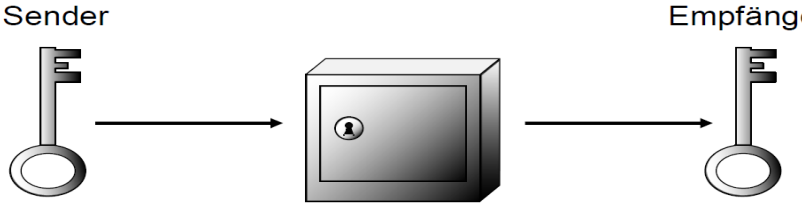
1)



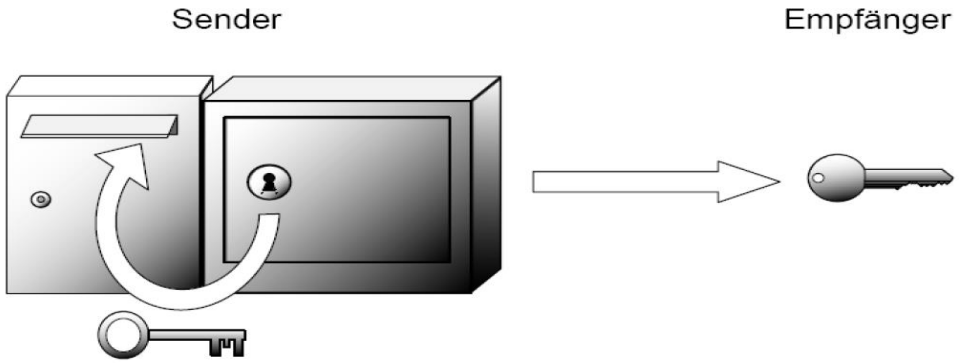
2)



3)



4)



Aufgabe 6.5 *Asymmetrisch Verschlüsseln und Signieren*

Teilnehmer A (Sender) schickt Teilnehmer B (Empfänger) eine asymmetrisch verschlüsselte Meldung, die mit einer digitalen Signatur versehen ist. Kreuzen Sie – in der chronologisch richtigen Reihenfolge – an. Die Parteien haben alle benötigten Schlüssel.

Reihenfolge	Wer	Aktion	Schlüsseltyp
1)	☑ Teiln. A ☐ Teiln. B	☐ signiert mit ☐ verschlüsselt mit ☐ verifiziert mit ☐ entschlüsselt mit	☐ Public Key von A ☐ Public Key von B ☐ Secret Key von A ☐ Secret Key von B
2)	☑ Teiln. A ☐ Teiln. B	☐ signiert mit ☐ verschlüsselt mit ☐ verifiziert mit ☐ entschlüsselt mit	☐ Public Key von A ☐ Public Key von B ☐ Secret Key von A ☐ Secret Key von B
3)	☐ Teiln. A ☑ Teiln. B	☐ signiert mit ☐ verschlüsselt mit ☐ verifiziert mit ☐ entschlüsselt mit	☐ Public Key von A ☐ Public Key von B ☐ Secret Key von A ☐ Secret Key von B
4)	☐ Teiln. A ☑ Teiln. B	☐ signiert mit ☐ verschlüsselt mit ☐ verifiziert mit ☐ entschlüsselt mit	☐ Public Key von A ☐ Public Key von B ☐ Secret Key von A ☐ Secret Key von B

8 Angriffe und 4 Prinzipien: Zwischenbilanz

- Die folgenden 4 können direkt mit einem kryptographischen Mechanismus bekämpft werden:
  - Abhören einer Meldung (Confidentiality)
  - Verändern der Meldung (Integrity)
  - Eine erfundene Meldung einspielen (Insertion)
  - Abstreiten die Meldung geschickt zu haben (Non repudiation of origin)
- Die folgenden 4 müssen mit einer applikatorischen Massnahme und/oder mit einem Challenge-Response Protokoll erweitert werden:
  - Eine Meldung abfangen und später wieder einspielen (Replay).
  - Löschen von Meldungen (Delete).
  - Sich für jemanden anders ausgeben (Masquerade).
  - Abstreiten die Meldung erhalten zu haben (Non repudiation of receipt, z.B. in SIC).

Die 4 Prinzipien erweitert

- Die folgenden 4 müssen mit einer applikatorischen Massnahme und/oder mit einem Challenge-Response Protokoll erweitert werden:
  - Eine Meldung abfangen und später wieder einspielen (Replay).
  - Löschen von Meldungen (Delete).
    - Sequenznummer (z.B. im Header) führen und über die ganze Meldung eine MAC-Berechnung durchführen oder digitale Signatur rechnen.
  - Sich für jemanden anders ausgeben (Masquerade).
    - C-R Protokoll versehen mit einer MAC-Berechnung oder einer digitalen Signatur. Solche Protokolle heissen „mutual authentication“ Protokolle.
  - Abstreiten die Meldung erhalten zu haben (Non repudiation of receipt, z.B. in SIC = Swiss Interbank Clearing).
    - Protokoll mit digitaler Signatur analog einem eingeschriebenen Brief.
    - Das Verhindern von non rep. of receipt wird selten verlangt und wird dementsprechend selten implementiert.

Eine häufig gestellte Frage

- Eine häufig gestellte Frage ist: «Warum schützen in den C-R Protokollen die Verschlüsselungen nicht gegen die Angriffe Masquerade und Non repudiation of receipt»?
- Antworten:
  - Bei der Masquerade werden wir das in Präsenz 12 (Einführung in die Protokolle) sehen. Bei Verwenden von Verschlüsselungen in den Authentizierprotokollen gibt es die sog. Oracle Session, resp. Parallel Session Attacke. Erst bei Verwenden von MAC's oder digitalen Signaturen kann man diese Angriffe abwenden. Das werden wir noch sehen.
  - Bei Non rep. of receipt ist die Sache anders. Eine Person (hier der Empfänger) muss etwas bestätigen, was keine andere Person bestätigen können darf. Das geht (streng genommen) nur mit einer digitalen Signatur. Es gibt Protokolle, die das mit (halben) MAC's in den Antworten macht. In diesem Fall könnte aber der Sender sich die Antwort selber erzeugen.

Aufgabe 6.6 *Bedrohung/Massnahmen Kataster, Teil 2*

Bedrohungen / Massnahmen	Meldung Löschen	Meldung Wiedereinspielen	Masquerade	Abstreiten Meldung erhalten zu haben
Sym. Verschlüsselung und Sequenznummer				
MAC- Berechnung und Sequenznummer				
Asym. Verschlüsselung und Sequenznummer				
Digitale Signatur und Sequenznummer				
C-R Protokoll mit Verschlüsselung				
C-R Protokoll mit MAC				
C-R Protokoll mit digitaler Signatur				

Aufgabe 6.7 *Ein Begriffs-Puzzle*

Füllen Sie die offenen Stellen aus (Nummer eintragen), es stehen die folgenden Wörter zur Verfügung:

(1) Digitale Signatur
(2) C-R Protokoll
(3) (gegenseitige) Authentisierung
(4) Masquerade
(5) MAC
(6) Benutzerauthentizität

Das Sicherheitsziel _____ wird durch den Angriff _____ gefährdet. Mittels einer _____ mit Hilfe von einem _____ welches auf dem kryptographischen Mechanismus _____ oder _____ beruht, wird der Angriff Masquerade verhindert.

Basis-Test Präsenz 1

Aussage	Richtig oder falsch?	Begründung
Denial of Service Attacke ist eine der 8 besprochenen Angriffe, die mit Krypt. Methoden verhindert werden können.	☐ richtig ☐ falsch	
Im Alice, Bob und Eve Modell können alle 3 Parteien mind. einen Angriff durchführen.	☐ richtig ☐ falsch	
Bob kann im Wesentlichen einen Angriff durchführen.	☐ richtig ☐ falsch	
Mit Verschlüsseln einer Meldung können die meisten der 8 Angriffe verhindert werden.	☐ richtig ☐ falsch	
Von den 8 aufgezeigten Angriffen gehören 7 zum Obergriff Authentizität.	☐ richtig ☐ falsch	
Wir haben Benutzer- und Datenauthentizität gleichgesetzt.	☐ richtig ☐ falsch	
Nur 4 der 8 Angriffe können direkt mit einem krypt. Mechanismus verhindert werden.	☐ richtig ☐ falsch	
3 der 8 Angriffe müssen in Kombination von krypt. und applikatorischen Massnahmen verhindert werden.	☐ richtig ☐ falsch	
2 der 8 Angriffe müssen in Kombination von C-R Protokoll und krypt. Methoden verhindert werden.	☐ richtig ☐ falsch	
Passive Attacker hören nur ab, sie verfälschen nichts.	☐ richtig ☐ falsch	
Alle Attacker sind aktive Attacker, da sie versuchen zu betrügen.	☐ richtig ☐ falsch	
Passwort und krypt. Schlüssel sind grundsätzlich etwas anderes.	☐ richtig ☐ falsch	

Basis-Test Präsenz 1, Fortsetzung

Aussage	Richtig oder falsch?	Begründung
Ein krypt. Schlüssel wird i.d.R. mit HEX Zeichen dargestellt.	☐ richtig ☐ falsch	
Ein krypt. Verfahren muss unbedingt geheim gehalten werden.	☐ richtig ☐ falsch	
Zur Sicherheitsanforderung der Geheimhaltung passt der Oberbegriff Verschlüsselung.	☐ richtig ☐ falsch	
Zur Sicherheitsanforderung der Authentizität/Integrität gibt es keinen analogen Oberbegriff wie bei der Verschlüsselung.	☐ richtig ☐ falsch	
Ein symmetrisches krypt. Verfahren zeichnet sich dadurch aus, dass Sender und Empfänger unterschiedliche Schlüssel haben.	☐ richtig ☐ falsch	
Um ein Dokument zu signieren, muss es zuerst gehasht werden.	☐ richtig ☐ falsch	
Signieren ist wie Verschlüsseln, einfach mit dem Private Key des Signieres.	☐ richtig ☐ falsch	
MAC und HMAC sind symmetrisch erzeugte Authentizierwerte.	☐ richtig ☐ falsch	
Grosse Dokumente können problemlos direkt mit einem asymmetrischen Verfahren verschlüsselt werden.	☐ richtig ☐ falsch	
In einer Sterntopologie braucht es ungefähr n^2 Schlüssel bei n Teilnehmern.	☐ richtig ☐ falsch	
Asymmetrische Verfahren sind viel langsamer als symmetrische.	☐ richtig ☐ falsch	

LÖSUNGEN DER AUFGABEN

Aufgabe 4.1

a) Alice & Bob sind Insider; Eve ist ein Outsider Angreifer.
b) Abhören ist der einzige passive Angriff, die anderen sind alles aktive Angriffe.

Aufgabe 4.2

- Gilt $K_E = K_D$, dann spricht man von einem symmetrischen Verfahren; z.B. AES, DES resp. 3-DES, SAFER, IDEA u.a.
- Gilt $K_E \neq K_D$, dann spricht man von einem asymmetrischen Verfahren; z.B. RSA.
- K_E ist im asymmetrischen Fall der Public Key des Empfängers und K_D ist der Private Key des Empfängers.

Aufgabe 4.3

- Gilt $K_G = K_V$, dann heisst der Authentizierwert MAC (Message Authentication Code);
- Gilt $K_G \neq K_V$, dann heisst der Authentizierwert digitale Signatur; digitale Signatur z.B. mit RSA u.a.
- Für den asymmetrischen Fall ist K_G ist der Private Key des Senders, und K_V ist der Public Key des Senders.

Aufgabe 4.4 ***Anzahl Schlüssel beim asymmetrischen und symmetrischen Verschlüsseln.***

a) Wie viele Schlüssel braucht es mit symmetrischer Kryptographie?
   i. $\frac{n(n-1)}{2}$ also 1000*999/2 = 499'500; also ungefähr $\frac{n^2}{2}$
   ii. $n(n-1)$ also 1000*999 = 999'000; also ungefähr n^2
   iii. $2n(n-1)$ also 2*1000*999 = 1'998'000; also ungefähr $2n^2$

b) Wie viele Schlüsselpaare braucht es mit asymmetrischer Kryptographie?
   i. 1000 Schlüsselpaare, also n, ***Achtung:*** Es können nicht A → B und B → A gleiche Schlüssel verwendet werden!!
   ii. 1000 Schlüsselpaare, also n, denn es ist automatisch erfüllt, dass von A → B und B → A unterschiedliche Schlüssel verwendet werden.
   iii. 2'000, also 2n.

Aufgabe 5.1

x_i	A	B	C
$P(x_i)$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$
$H(x_i) = -\log_2\big(P(x_i)\big)$	1	2	2

b) $H(X) = -\sum_{i=1}^{3} P(x_i) \cdot \log_2\big(P(x_i)\big) = -\left(\frac{1}{2} \cdot \log_2\left(\frac{1}{2}\right) + 2 \cdot \frac{1}{4} \cdot \log_2\left(\frac{1}{4}\right)\right) = -\left(\frac{1}{2} \cdot (-1) + 2 \cdot \frac{1}{4} \cdot (-2)\right) = 1{,}5$

c) $H_0(X) = \log_2(3) \approx 1{,}585$

d) $R(X) = H_0(X) - H(X) = 1{,}585 - 1{,}5 = 0{,}085$

e) $r(X) = \frac{R(X)}{H_0(X)} = \frac{0{,}085}{1{,}585} = 0{,}0536$ resp. $r(X) = 1 - \frac{H(X)}{H_0(X)} = 1 - \frac{1{,}5}{1{,}585} = 0{,}0536$

f) Check der Ungleichung: $0 \leq H(X) \leq \log_2(n) = H_0(X)$ ist erfüllt, da $0 \leq 1{,}5 \leq \log_2(3) = 1{,}585$

Aufgabe 5.2 6*3,3 Bit; also ungefähr 20 Bit.

Aufgabe 5.3 ***Schlüssel:*** Bei Spartanern = Dicke des Stabes, bei Cäsar = die Anzahl Stellen.
Algorithmus: Bei Spartanern = Wickeln, bei Cäsar = Verschieben.

Aufgabe 6.1 Hybride Verschlüsselung, siehe die nachfolgenden Folien

Aufgabe 6.2 Der (identische) symmetrische Schlüssel mit den zwei verschiedenen Public Keys verschlüsselt werden.

Aufgabe 6.3 ***Bedrohung/Massnahmen Kataster, Teil 1***

Bedrohungen / Massnahmen	Meldung Abhören	Meldung Verändern	Neue Meld. Erfinden	Abstreiten Meldung geschickt zu haben
Symmetrische Verschlüsselung	X			
Asymmetrische Verschlüsselung	X			
MAC-Berechnung (sym.)		X	X	
Digitale Signatur (asym.)		X	X	X

Aufgabe 6.4 *Mechanische Analoga*

1) Digitale Signatur
2) Asymmetrische Verschlüsselung
3) Symmetrische Verschlüsselung
4) Hybride Verschlüsselung

Bemerkung: Es fehlt ein Analogon zum MAC.

Aufgabe 6.5

Reihenfolge	Wer	Aktion	Schlüsseltyp
1)	☑ Teiln. A ☐ Teiln. B	☑ signiert mit ☐ verschlüsselt mit ☐ verifiziert mit ☐ entschlüsselt mit	☐ Public Key von A ☐ Public Key von B ☑ Secret Key von A ☐ Secret Key von B
2)	☑ Teiln. A ☐ Teiln. B	☐ signiert mit ☑ verschlüsselt mit ☐ verifiziert mit ☐ entschlüsselt mit	☐ Public Key von A ☑ Public Key von B ☐ Secret Key von A ☐ Secret Key von B
3)	☐ Teiln. A ☑ Teiln. B	☐ signiert mit ☐ verschlüsselt mit ☐ verifiziert mit ☑ entschlüsselt mit	☐ Public Key von A ☐ Public Key von B ☐ Secret Key von A ☑ Secret Key von B
4)	☐ Teiln. A ☑ Teiln. B	☐ signiert mit ☐ verschlüsselt mit ☑ verifiziert mit ☐ entschlüsselt mit	☑ Public Key von A ☐ Public Key von B ☐ Secret Key von A ☐ Secret Key von B

Aufgabe 6.6 ***Bedrohung/ Massnahmen Kataster, Teil 2***

Bedrohungen / Massnahmen	Meldung Löschen	Meldung Wiedereinspielen	Masquerade	Abstreiten Meldung erhalten zu haben
Sym. Verschlüsselung und Sequenznummer				
MAC- Berechnung und Sequenznummer	X	X		
Asym. Verschlüsselung und Sequenznummer				
Digitale Signatur und Sequenznummer	X	X		
C-R Protokoll mit Verschlüsselung				
C-R Protokoll mit MAC			X	
C-R Protokoll mit digitaler Signatur			X	X

Aufgabe 6.7

Das Sicherheitsziel Benutzerauthentizität (6) wird durch den Angriff Masquerade (4) gefährdet. Mittels einer (gegenseitigen) Authentisierung (3) mit Hilfe von einem C-R Protokoll (2) welches auf dem kryptographischen Mechanismus MAC (5) oder digitaler Signatur (1) beruht, wird der Angriff Masquerade verhindert.

Basis-Test Präsenz 1

Aussage	Richtig oder falsch?	Begründung
Denial of Service Attacke ist eine der 8 besprochenen Angriffe, die mit Krypt. Methoden verhindert werden können.	☐ richtig ☑ falsch	
Im Alice, Bob und Eve Modell können alle 3 Parteien mind. einen Angriff durchführen.	☑ richtig ☐ falsch	
Bob kann im Wesentlichen einen Angriff durchführen.	☑ richtig ☐ falsch	Er kann Abstreiten eine Meldung erhalten zu haben.
Mit Verschlüsseln einer Meldung können die meisten der 8 Angriffe verhindert werden.	☐ richtig ☑ falsch	Mit Verschlüsseln kann man nur das Abhören verhindern; genauer, dass die abgehörte Meldung verstanden wird.
Von den 8 aufgezeigten Angriffen gehören 7 zum Obergriff Authentizität.	☑ richtig ☐ falsch	Siehe vorherige Frage.
Wir haben Benutzer- und Datenauthentizität gleichgesetzt.	☐ richtig ☑ falsch	
Nur 4 der 8 Angriffe können direkt mit einem krypt. Mechanismus verhindert werden.	☑ richtig ☐ falsch	Geheimhaltung, Integrität, Insertion & Non rep. of Origin
3 der 8 Angriffe müssen in Kombination von krypt. und applikatorischen Massnahmen verhindert werden.	☐ richtig ☑ falsch	Nur 2, nämlich Replay und Delete.
2 der 8 Angriffe müssen in Kombination von C-R Protokoll und krypt. Methoden verhindert werden.	☑ richtig ☐ falsch	Non rep. of receipt und Mutual Authentication.
Passive Attacker hören nur ab, sie verfälschen nichts.	☑ richtig ☐ falsch	
Alle Attacker sind aktive Attacker, da sie versuchen zu betrügen.	☐ richtig ☑ falsch	Siehe vorherige Frage.
Passwort und krypt. Schlüssel sind grundsätzlich etwas anderes.	☐ richtig ☑ falsch	

Basis-Test Präsenz 1, Fortsetzung

Aussage	Richtig oder falsch?	Begründung
Ein krypt. Schlüssel wird i.d.R. mit HEX Zeichen dargestellt.	☑ richtig ☐ falsch	
Ein krypt. Verfahren muss unbedingt geheim gehalten werden.	☐ richtig ☑ falsch	Nur die geheimen Schlüssel müssen geheim gehalten werden.
Zur Sicherheitsanforderung der Geheimhaltung passt der Oberbegriff Verschlüsselung.	☑ richtig ☐ falsch	
Zur Sicherheitsanforderung der Authentizität/Integrität gibt es keinen analogen Oberbegriff wie bei der Verschlüsselung.	☑ richtig ☐ falsch	Wir haben ad hoc den Begriff „Authentizierwert anhängen“ eingeführt. Er beschreibt aber nicht alle Facetten der Authentizität.
Ein symmetrisches krypt. Verfahren zeichnet sich dadurch aus, dass Sender und Empfänger unterschiedliche Schlüssel haben.	☐ richtig ☑ falsch	Das ist das wesentliche Merkmal von asymmetrischen krypt. Verfahren.
Um ein Dokument zu signieren muss es zuerst gehasht werden.	☑ richtig ☐ falsch	
Signieren ist wie Verschlüsseln, einfach mit dem Private Key des Signieres.	☐ richtig ☑ falsch	Signieren ist keine Verschlüsselung, obwohl das z.T. in (schlechten) Lehrbüchern steht.
MAC und HMAC sind symmetrisch erzeugte Authentizierwerte.	☑ richtig ☐ falsch	
Grosse Dokumente können problemlos direkt mit einem asymmetrischen Verfahren verschlüsselt werden.	☐ richtig ☑ falsch	Grosse Dokumente müssen hybrid verschlüsselt werden.
In einer Sterntopologie braucht es ungefähr n^2 Schlüssel bei n Teilnehmern.	☐ richtig ☑ falsch	Es braucht nur n Schlüssel bei n Teilnehmern.
Asymmetrische Verfahren sind viel langsamer als symmetrische.	☑ richtig ☐ falsch	

Quellenangaben & Danksagung

- Angaben zur Literatur und Bilder sind in diesen Folien keine gemacht worden. Im JS Skript „Einführung in die Kryptologie“, sind diese jedoch vollständig enthalten.
- Ein herzliches Dankeschön geht an zwei Kollegen:
  - Einige Folien entstammen aus der Vorlesung „Sichere Netzwerkkommunikation“ von Prof. Dr. Andreas Steffen, Hochschule Rapperswil.
  - Die Folie „Woher stammen diese Schlüssel?“ stellte mir Armand Portmann HSLU aus seiner Vorlesung „Zertifikatsbasierende Anwendungen und PKI I“ des CAS-IS-T Informationssicherheit zur Verfügung.