LÖSUNGEN KRYPTOLOGIE

Aufgabe 1

„Wie Sie sehen ist eine solche Methode nicht sehr sicher und kann relativ einfach gebrochen werden“

Aufgabe 2

1.

n_1	n_2	a_1	a_2	b_1	b_2	q	r
132	128	1	0	0	1	1	4
128	4	0	1	1	-1	32	0

$ggT(132,128) = n_2 = 4 = a_2 \cdot 132 + b_2 \cdot 128 = 1 \cdot 132 + (-1) \cdot 128$

2. Da $a \cdot \Phi(n)$ ohne Rest durch $\Phi(n)$ teilbar ist und 1 dividiert durch $\Phi(n)$ sicher den Rest 1 ergibt, folgt:

$$1 \bmod \Phi(n) = \left[a \cdot \Phi(n) + b \cdot e\right] \bmod \Phi(n)$$
$$1 = b \cdot e \bmod \Phi(n)$$

Der Faktor b erfüllt demnach die Bedingung des geheimen Schlüssels. Da uns nur der Rest bei Division durch $\Phi(n)$ interessiert, gilt:

$$d = b \bmod \Phi(n).$$

3. d = 77.

Aufgabe 3

1. Um $a^{2^{16}} = a^{2 \cdot 2 \cdot \ldots \cdot 2} = \left(\left(\left(\left(a^2\right)^2\right)^2\right)^2 \cdots\right)^2$ zu berechnen muss 16 mal quadriert werden, was 16 Multiplikationen erfordert. Um $a^{2^{16}+1} = a^{2^{16}} \cdot a$ zu erhalten muss abschliessend noch mit a multipliziert werden. Man benötigt gesamthaft 17 Multiplikationen.

2. Anzahl Multiplikationen $\leq \frac{(L-1)\cdot L}{2} + (L-1)$.

Aufgabe 4

a) $R_d(n_1 + n_2) = R_d(R_d(n_1) + Rd(n_2))$
„Der Rest der Summe ist gleich dem Rest aus der Summe der Resten“

b) $R_d(n_1 \cdot n_2) = R_d(R_d(n_1) \cdot Rd(n_2))$
„Der Rest des Produkts ist gleich dem Rest aus den Produkten der Resten“

$\Rightarrow$ Nach jeder einzelnen Operation muss nur der Rest betrachtet werden.

Aufgabe 5

	Vertraulichkeit	Authentikation	Integrität
Rose im Knopfloch		✓	
Brief in Umschlag stecken, zukleben	✓		(✓)
Fingerabdruck		✓	
Briefsiegel		✓	✓
Unterschrift		✓	

Aufgabe 6

Einen Nachricht wird „verschlüsselt“, indem sie in den Briefkasten des Empfängers gesteckt wird. Dies kann jedermann machen. Den Briefkasten öffnen und somit die Nachricht „entschlüsseln“ kann nur der Inhaber des Briefkastens.

Aufgabe 7

1. Alice sendet eine Nachricht an Bob, indem sie diese in den Koffer steckt, diesen mit ihrem Vorhängeschloss zuschliesst und an Bob schickt. Bob kann den Koffer nicht öffnen, verschliesst ihn aber ebenfalls mit seinem Vorhängeschloss und schickt ihn zurück an Alice. Diese entfernt nun ihr Vorhängeschloss und schickt den Koffer ein weiteres Mal an Bob zurück, welcher nun wiederum sein Vorhängeschloss entfernt und die Nachricht lesen kann. Der Koffer war immer mit mindestens einem Schloss gesichert und konnte so von keinem Unbefugten geöffnet werden. Hingegen muss sichergestellt sein, dass nicht ein Angreifer die Rolle von Bob übernehmen und so Alice überlisten kann (Authentizität des Transportwegs).
2.

Alice an Bob	$m^{e_A} \bmod p$
Bob an Alice	$\left(m^{e_A}\right)^{e_B} \bmod p = m^{e_A \cdot e_B} \bmod p$
Alice an Bob	$\left(m^{e_A \cdot e_B}\right)^{d_A} \bmod p = m^{e_A \cdot d_A \cdot e_B} \bmod p = m^{e_B} \bmod p$
Bob entschlüsselt	$\left(m^{e_B}\right)^{d_B} \bmod p = m^{e_B \cdot d_B} \bmod p = m$

Aufgabe 8

1. Ist ziemlich aufwendig
2. Liefert Gleichungsystem:

$$14803 = p \cdot q$$
$$14560 = (p-1)(q-1)$$

$\Rightarrow$ Quadratische Gleichung mit den Lösungen 113 und 131.

Aufgabe 9

a) $c = m^e \bmod n = \underline{\underline{205}}$

b) $c = m^e \bmod n = 100^7 \bmod n$

$= (10^7)^2 \bmod n = (10^7 \bmod n)^2 \bmod n$

$= 205^2 \bmod 247 = \underline{\underline{35}}$

c) $n = 247 = 13 \cdot 19 = p \cdot q$

Gesucht: d, so dass $e \cdot d \bmod (p-1)(q-1) = 1$

$\Rightarrow 7 \cdot d \bmod 216 = 1$

d muss sicher grösser sein als $216/7 = 30{,}86$

Versuch: $d = 31 \Rightarrow 7 \cdot 31 \bmod 216$

$= 217 \bmod 216$

$= 1$

$\Rightarrow \underline{\underline{d = 31}}$ *)

d) $m^* = c^d \bmod n = \underline{\underline{193}}$

*) Kann auch mit euklidischem Algorithmus (S. Aufgabe 2) bestimmt werden.

Aufgabe 10

a) $c = m^e \bmod n = 3^3 \bmod 10 = \underline{\underline{7}}$

b) Durch Probieren: $3 \cdot 7 \bmod 10 = 21 \bmod 10$

$= 1$

$\Rightarrow d = \underline{\underline{7}}$

c) $m^* = c^d \bmod n = 7^7 \bmod 10 = \underline{\underline{3}}$

d) $c_1 = m_1^e \bmod n = 4^2 \bmod 10 = 6$

$c_2 = m_2^e \bmod n = 6^2 \bmod 10 = 6$

Unterschiedliche Klartexte ergeben gleichen Geheimtext $\Rightarrow$ Verschlüsselung ist nicht mehr eindeutig umkehrbar!

Grund: $n = p \cdot q = 2 \cdot 5$

$e = 2$ ist nicht teilerfremd zu $q - 1 = 4$

Aufgabe 11

a) $n = p_1^2 \Rightarrow \varphi(n) = p_1^2 - 1 - (p_1 - 1)$

$= \underline{\underline{p_1^2 - p_1}}$

b) $n = p_1^n \Rightarrow \varphi(n) = p_1^n - 1 - (p_1^{n-1} - 1)$

$= \underline{\underline{p_1^n - p_1^{n-1}}}$

c) $n = p_1^2 \cdot p_2$

$\Rightarrow \varphi(n) = n - 1 - \left(\frac{n}{p_1} - 1\right) - \left(\frac{n}{p_2} - 1\right) + \left(\frac{n}{p_1 p_2} - 1\right)$

$= p_1^2 p_2 - 1 - (p_1 p_2 - 1) - (p_1^2 - 1) + (p_1 - 1)$

$= \underline{\underline{p_1^2 p_2 - p_1 p_2 - p_1^2 + p_1}}$

d) $n = p_1 \cdot p_2 \cdot p_3$

$\Rightarrow \varphi(n) = n - 1 - \left(\frac{n}{p_1} - 1\right) - \left(\frac{n}{p_2} - 1\right) - \left(\frac{n}{p_3} - 1\right) + \left(\frac{n}{p_1 p_2} - 1\right) + \left(\frac{n}{p_1 p_3} - 1\right) + \left(\frac{n}{p_2 p_3} - 1\right)$

$= p_1 p_2 p_3 - 1 - (p_2 p_3 - 1) - (p_1 p_3 - 1) - (p_1 p_2 - 1) + (p_3 - 1) +$
$+ (p_2 - 1) + (p_1 - 1)$

$= \underline{\underline{p_1 p_2 p_3 - p_2 p_3 - p_1 p_3 - p_1 p_2 + p_1 + p_2 + p_3 - 1}}$

$= p_1 p_2 p_3 \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \left(1 - \frac{1}{p_3}\right)$

Aufgabe 12

a) Der Exponent e ist teilerfremd zu $p-1 = 10$ und $q-1 = 12$.

b) $c = m^e \bmod n = \underline{\underline{5}}$

c) Gesucht d, so dass $e \cdot d \bmod (p-1)(q-1) = 1$

$$11 \cdot d \bmod 120 = 1$$

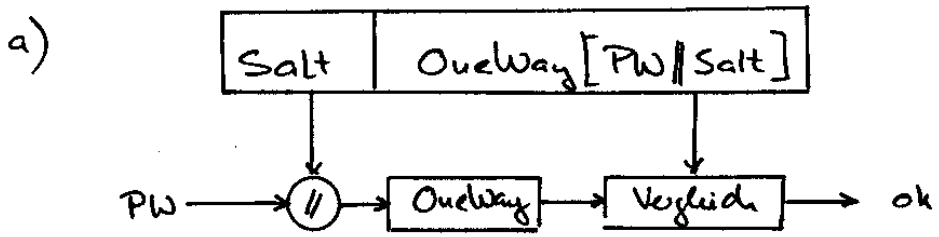
$$\Rightarrow \quad \underline{\underline{d = 11}}$$

Aufgabe 13

	IDEA	DES	AES	Triple DES
Beinhaltet ein Feistel-Netzwerk	☐ ja ☑ nein	☑ ja ☐ nein	☐ ja ☑ nein	
Gilt als sicher	☑ ja ☐ nein	☐ ja ☑ nein	☑ ja ☐ nein	☑ ja ☐ nein
Schlüssellänge in Bit	128	56	128 – 256	112
Blocklänge in Bit	64	64	128 – 256	64
Anzahl Runden	8 + 1	16	10 - 14	

Aufgabe 14

a)



b)

- Der Angreifer kann nicht eine im Voraus berechnete Passwort-tabelle verwenden.
- Gleiche Passwörter sind nicht aus den Einträgen der Passwort-datei ersichtbar.

Aufgabe 15

1. Einfache Implementation auf 16-Bit Mikroprozessoren
2. Kompatibilität mit DES (64:4 = 16)
3. $2^{16} + 1$ ist Primzahl, was wichtig ist für die Umkehrbarkeit der Multiplikation.

Aufgabe 16

a) Einweg-Hashfunktion

Aufgabe 17

a) $n = 2^{512} \approx 1.3 \cdot 10^{154} \Rightarrow \pi(n) \approx \underline{3.8 \cdot 10^{151}}$

b) Anzahl Byte $\approx 512 \cdot 3.8 \cdot 10^{151} / 8 \approx 2.4 \cdot 10^{153}$ Byte $\approx 2.4 \cdot 10^{144}$ GByte
Masse der Festplatte $\approx \underline{2.4 \cdot 10^{141}\ \text{kg}}$

c) Die Festplatte würde zu einem schwarzen Loch kollabieren!

Aufgabe 18

a)

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**
n = 23	1	1	1	1	22	1	22	1	1	22	22	1	1	22	22	1	22	1	22	22	22	22
n = 15	1	8	12	4	5	6	13	2	9	10	11	3	7	14								

b) Falls n prim ist $\Rightarrow$ Entscheidung immer richtig.
Falls n nicht prim ist $\Rightarrow$ Irrtumswahrscheinlichkeit $\leq 2^{-k}$.

Aufgabe 19

		x =																																				
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	**31**	r	ggT(a^(r/2)+1,N)	ggT(a^(r/2)-1,N)
a =	1																																				
	2	**2**	4	8	16	32	64	51	25	50	23	46	15	30	60	43	9	18	36	72	67	57	37	74	71	65	53	29	58	39	1	**2**	30	11	7
	3	**3**	9	27	4	12	36	31	16	48	67	47	64	38	37	34	25	75	71	59	23	69	53	5	15	45	58	20	60	26	1	**3**	30	7	11
	4	**4**	16	64	25	23	15	60	9	36	67	37	71	53	58	1	**4**	16	64	25	23	15	60	9	36	67	37	71	53	58	1	**4**	15	**r ungerade**	
	5	**5**	25	48	9	45	71	47	4	20	23	38	36	26	53	34	16	3	15	75	67	27	58	59	64	12	60	69	37	31	1	**5**	30	7	11
	6	**6**	36	62	64	76	71	41	15	13	1	**6**	36	62	64	76	71	41	15	13	1	**6**	36	62	64	76	71	41	15	13	1	**6**	10	**$a^{r/2} \equiv -1$**	
	7	**ggT(a,N) = 7 ist Teiler**																																				
	8	**8**	64	50	15	43	36	57	71	29	1	**8**	64	50	15	43	36	57	71	29	1	**8**	64	50	15	43	36	57	71	29	1	**8**	10	11	7
	9	**9**	4	36	16	67	64	37	25	71	23	53	15	58	60	1	**9**	4	36	16	67	64	37	25	71	23	53	15	58	60	1	**9**	15	**r ungerade**	
	10	**10**	23	76	67	54	1	**10**	23	76	67	54	1	**10**	23	76	67	54	1	**10**	23	76	67	54	1	**10**	23	76	67	54	1	**10**	6	**$a^{r/2} \equiv -1$**	
	11	**ggT(a,N) = 11 ist Teiler**																																				
	12	**12**	67	34	23	45	1	**12**	67	34	23	45	1	**12**	67	34	23	45	1	**12**	67	34	23	45	1	**12**	67	34	23	45	1	**12**	6	7	11
	13	**13**	15	41	71	76	64	62	36	6	1	**13**	15	41	71	76	64	62	36	6	1	**13**	15	41	71	76	64	62	36	6	1	**13**	10	**$a^{r/2} \equiv -1$**	
	14	**ggT(a,N) = 7 ist Teiler**																																				
	15	**15**	71	64	36	1	**15**	71	64	36	1	**15**	71	64	36	1	**15**	71	64	36	1	**15**	71	64	36	1	**15**	71	64	36	1	**15**	5	**r ungerade**	

Aufgabe 20

$a_1 = 1$, $a_2 = 3$, $a_3 = 4$

$m_1 = 2$, $m_2 = 5$, $m_3 = 7$

$m = 2 \cdot 5 \cdot 7 = 70$

$M_1 = m/m_1 = 35$, $M_2 = m/m_2 = 14$, $M_3 = m/m_3 = 10$

$N_1 = 1$, weil $1 \cdot 35 \bmod 2 = 1$

$N_2 = 4$, weil $4 \cdot 14 \bmod 5 = 1$

$N_3 = 5$, weil $5 \cdot 10 \bmod 7 = 1$

$\Rightarrow x = \underline{53}$

Aufgabe 21

(aus der Vorlesung „Informationssicherheit und Kryptographie“ von Prof. U. Maurer der ETH Zürich)

a) Zuerst faktorisieren wir 899. Man erhält $29 \cdot 31 = 900 - 1 = 899$. Daher gilt $\varphi(899) = (29-1) \cdot (31-1) = 840$ und $d \equiv e^{-1} \pmod{840}$. Das Inverse von $e = 11$ findet man mit Extended Euklid oder mit dem Tipp aus der Aufgabenstellung:

$$d \cdot 11 + b \cdot 840 = 1$$

Letztere Gleichung ist erfüllt für $b = -8$ und $d = 611$. Nun muss man nur noch $7^{611} \equiv 7^{401} \cdot 7^{210} \equiv 20 \pmod{899}$ berechnen.

Da e relativ prim zu $\varphi(n)$ sein muss, kommt kein kleinerer Wert als 11 dafür in Frage.

b) RSA funktioniert auch mit einem Modulus, der mehr als zwei Primfaktoren besitzt.

Für die Verwendung von mehr als zwei Faktoren spricht, dass ein schneller, noch nicht bekannter Algorithmus existieren könnte, der die Faktorzerlegung von n nur dann schnell findet, wenn n das Produkt von zwei Primfaktoren ist.

Die Laufzeit einiger Faktorisierungsalgorithmen hängt vor allem von der Grösse des kleinsten Faktors ab. Deshalb kann die Verwendung von mehr als zwei Faktoren auch dazu führen, dass in grösseren Restklassen gerechnet werden muss.

c) Folgende Kryptogramme können beobachtet werden:

$$\begin{aligned} y_1 &\equiv x^3 \pmod{n_1} \\ y_2 &\equiv x^3 \pmod{n_2} \\ y_3 &\equiv x^3 \pmod{n_3} \end{aligned}$$

Mit dem Chinesischen Restsatz lässt sich daraus

$$y = x^3 \pmod{n_1 n_2 n_3}$$

berechnen. Da $x < n_i$ für $i = 1, 2, 3$ gilt, folgt $x^3 < n_1 n_2 n_3$, das heisst $y = x^3$ wird nicht reduziert. Man kann x durch Berechnen der dritten Wurzel aus y in den ganzen Zahlen erhalten.

Die beschriebene Attacke heisst *Attacke von Håstad*. Sie klappt analog auch für $e > 3$, falls die gleiche Nachricht mit mindestens e verschiedenen Public Keys verschlüsselt wird.