1 Aufgabe 1

1.1 A

$C : \alpha \to Perm(S)$ // C injektiv $\to |K| \leq |Perm(S)|$
$|S| = 2^n$
$|Perm(S)| = (2^n)!$

1.2 B

$f : A \to B$
$f : x \to f(x)$

$$\left.\begin{array}{l} geg. : y \in f(A) \subset B \\ ges. : x \in A : f(x) = y \end{array}\right\} \text{schwierig}$$

1.3 G

Der Koinzidenzindex ist Wahrscheinlichkeit wenn ich zwei mal ein Buchstaben aus einem Text herausgreiffe das ich den selben Buchstaben erwische

2 Aufgabe 2: RSA

$p = 23$, $q = 29$
$n = 23 * 29 = 667$
$\varphi(n) = 23 * 28 = 616 = 2^3 * 7 * 11$

2.1 A

$e \in \{3, 5, 13\}$ // $ggT(e, \varphi(n)) = 1$

2.2 B

$d * e \equiv 1 mod \varphi(n)$

i	q	r	s	t
0	-	616	1	0
1	205	3	0	1
		1	1	-206

$-205 * 3 + 1 * 616 = 1$
$d = -205 \equiv 411 mod \varphi(n)$

3 Aufgabe 3

3.1 A

a	4
b	3
c	5
d	6

$IC_T = \frac{4*3+3*2+5*4+6*5}{18*17} = \frac{68}{306} = \frac{2}{8}$

3.2 B

Schlüssellänge Text in p Teile teilen von diesen den Koinsidenzindex vergleichen ob er in dem Bereich einer Sprache ist.

Schlüssel Wir nehmen die Abschnitte und machen pro Abschnitt eine Statistik und verschiebe dan die Buchstaben bis es einen Sinn ergiebt.

4 Aufgabe 4: RSA

(n,e) = (91,7), (n,d)=(91,31)
Alice: (n, e_A)=(91,5)
a) Gesucht: $d_A mit d_A \equiv d_A mod \varphi(n)$

$e*d-1 = k*\varphi(n) = 216$ // $ggT(d_A, \varphi(n)) = 1$
$h := e*d-1$, // $g = ggT(e*d-1, e_A) = 1$

Es könnte sein:
$e*d-1 = k*\varphi(n) = 2*5^2*13*\varphi(n) = h$
$h := \frac{h}{g}$, $g := ggT(h, e_A) = 5$

Zu lösen: $d_A * e + f * h = 1$
$d_A = -43 \equiv 173$ mod h (-43 + 216= 173)

b) Gesucht: c=3 entschlüsseln
$c^{d_A} \equiv m$ mod n
3^173 mod 91 (173=128+32+8+4+1)
$3^2 \equiv 9$ mod 91
$2^4 \equiv (3^2)^2 \equiv 81$ mod 91
$3^8 = (3^4)^2 \equiv 81^2 = (-10)^2 = 10^2 \equiv 9$ mod 91
$3^16 \equiv 81$ mod 91
$3^32 \equiv 9$ mod 91
$3^64 \equiv 81$ mod 91
$3^128 \equiv 9$ mod 91

5 Aufgabe 5

m= $\underbrace{0111\ \ 0100}_{m_1}\ \underbrace{0011\ \ 0000}_{m_2}$

$IV \oplus m_1$	0000	1001
		0011
		0101
		0000
$runde_1$	1001	0110
		1001
		1100
		1001
c_1=	0110	1100
$c_1 \oplus m_2$	0101	1100
		1001
		0101
		0101
$runde_1$	1100	1001
		0110
		1100
		1100
c_2 =	1001	0110

6 Aufgabe 6

Fixes kleines e $\Rightarrow$ d gross
$n = p * Q = 19 * 31 = 589$
$\varphi(n) = 540$
$e = 7$
$d = 463$

6.1 A

$[log_2(e)]$ (abgerundet) + EB-1 mit EB=#Einsen in binärer Darstellung von e.
$e = 7 \Rightarrow$ #Mult. = 2+2
$7 = (111)_2$

6.2 B

$d = 463 > 2^8 = 256 \Rightarrow [log_2(463)] = 8$
$463 = 256 + 128 + 64 + 8 + 4 + 2 + 1 = \underbrace{(111001111)_2}_{EB=7}$
#Mult= 8+EB-1=8+8=14

6.3 D

$d_p \equiv 13$ mod p
$d_p \equiv 13$ mod q

$m_q \equiv c^{d_q}$ mod q
$m_p \equiv c^{d_p}$ mod $p \equiv 3$ mod 19