

### Aufgabe 6.1

Sei  $A$  das Alphabet der Zeichen  $\{\_, a, b, \dots, z, .\}$ . Eine vollständige Auflistung der Zeichen aus  $A$  finden Sie in der unten aufgeführten Tabelle in Zeilen eins und drei. Sei außerdem eine Abbildung  $val : A \rightarrow \mathbb{Z}_{28}$  definiert, deren Wert in Zeile zwei, bzw. vier der unteren Tabelle für jedes  $x \in A$  explizit aufgelistet ist. Ferner sei die Umkehrfunktion von  $val$  als  $val^{-1} : \mathbb{Z}_{28} \rightarrow A$  definiert.  $val^{-1}$  bildet jede Zahl  $n \in \mathbb{Z}_{28}$  auf das entsprechende  $x \in A$ , mit  $val(x) = n$  ab.

$x \in A$	$\_$	a	b	c	d	e	f	g	h	i	j	k	l	m
$val(x)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$x \in A$	n	o	p	q	r	s	t	u	v	w	x	y	z	.
$val(x)$	14	15	16	17	18	19	20	21	22	23	24	25	26	27

Damit die Daten der B.I.R.Ds auf dem Weg zu seiner geheimen Zentrale vertraulich bleiben, hat sich Dr. Meta eine Verschlüsselungsfunktion  $Enc : A^* \times A^+ \rightarrow A^*$  überlegt. Seit seiner Promotion ist er allerdings des Definierens von Funktionen überdrüssig. Da Sie ihre Fähigkeiten auf diesem Gebiet bereits zum wiederholten Male unter Beweis gestellt haben, dürfen Sie diese Aufgabe für ihn übernehmen. Die Verschlüsselung soll eine Nachricht  $w \in A^*$ , sowie einen Schlüssel  $k \in A^+$  wie folgt verarbeiten:

Zum Verschlüsseln eines Zeichens der Nachricht wird es mit einem Zeichen des Schlüsselwortes „aufaddiert“. Hierzu wird zunächst mittels  $val$  der Zahlenwert der jeweiligen Zeichen berechnet. Diese Werte werden addiert und das Ergebnis wird mittels  $val^{-1}$  wieder auf ein Zeichen aus  $A$  abgebildet. Die verschlüsselte Nachricht ergibt sich als Konkatination aller jeweils auf diese Weise verschlüsselten Zeichen. Hierbei wird für alle  $i \in \mathbb{Z}_{|w|}$   $w(i)$  unter Verwendung von  $k(i)$  verschlüsselt.

Die Folgende Nachricht wurde von den B.I.R.D-Drohnen gesendet:

„wnlgbnovtezjznquqtaoneejfmifxfb\_nez.j\_iem.“

Sie ist mit Dr. Metas Universalpasswort „genial\_boese“ verschlüsselt. Entschlüsseln Sie sie und geben sie die originale Nachricht an. Rechenweg **nicht** gefordert.