

# Kryptografie

Von Vertretungsstunde bis  
Projekttag

Katrin Büttner

Thomas Knapp

MS „J.W.v. Goethe“  
Heidenau

MS Kötzschenbroda  
Radebeul

buettner@ibisath.info

knapp@ibisath.info

# Inhalte

1. Was bei den Sachsen läuft ☺
2. Überblick
3. Klassische Verfahren
4. „Kryptographie kompakt“
5. Bonus: Steganographie

# Inhalte

1. Was bei den Sachsen läuft ☺
2. Überblick
3. Klassische Verfahren
4. „Kryptographie kompakt“
5. Bonus: Steganographie

# Kryptologie

## Kryptographie

Sicherheit der eigenen  
geheimen  
Kommunikation gegen  
unbefugte Entzifferung  
oder Veränderung

## Kryptoanalyse

Das Brechen der  
Sicherheit der  
Kommunikation

## Kryptologie



```
graph TD; A[Kryptographie] --> D[Kryptologie]; B[Kryptoanalyse] --> D;
```

(nach: <http://de.wikipedia.org/wiki/Kryptologie>; 17.03.11; 21:00)

# Kryptologie

Ziele:

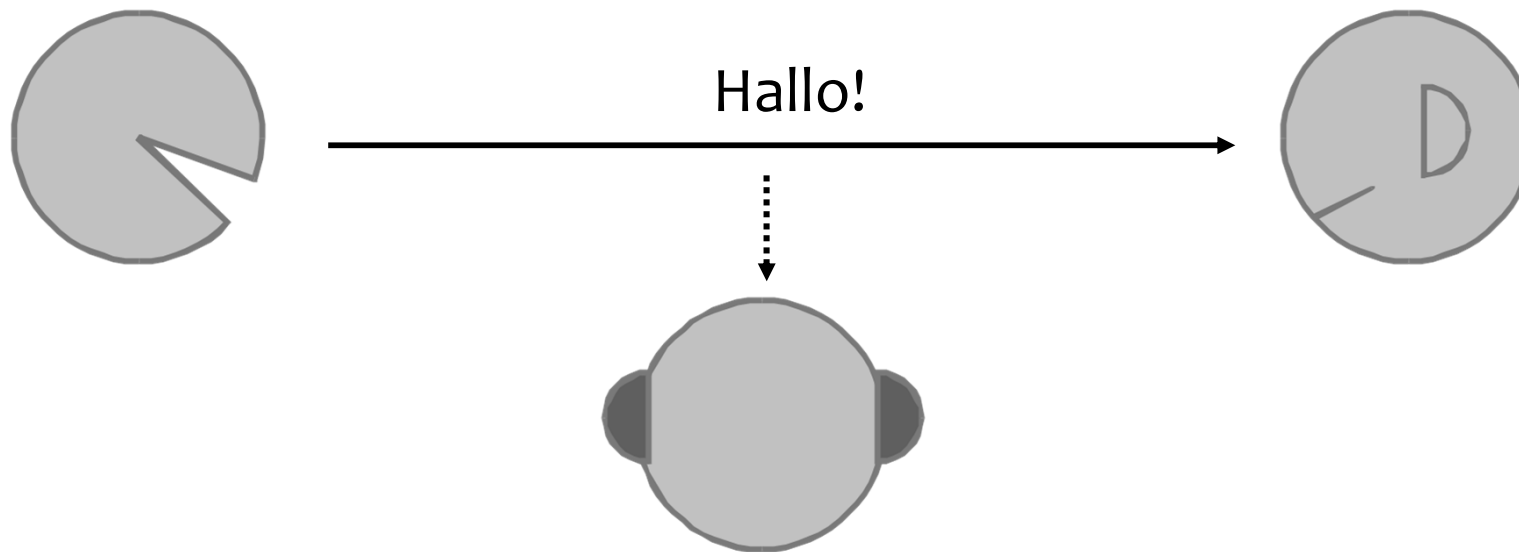
- Vertraulichkeit
- Integrität
- Zurechenbarkeit

Moderne Alltagsbeispiele:

- Login-Prozeduren am PC
- Sichere Web-Seiten (https)
- Signierte und verschlüsselte Emails
- Verschlüsselung von Datenträgern (Sichern von Daten, keine Übertragung)

# Nachrichtenübertragung

- Nachricht
- Sender, Empfänger
- Zu-, Mit- Hörer



# Codieren

## *Übersetzen*

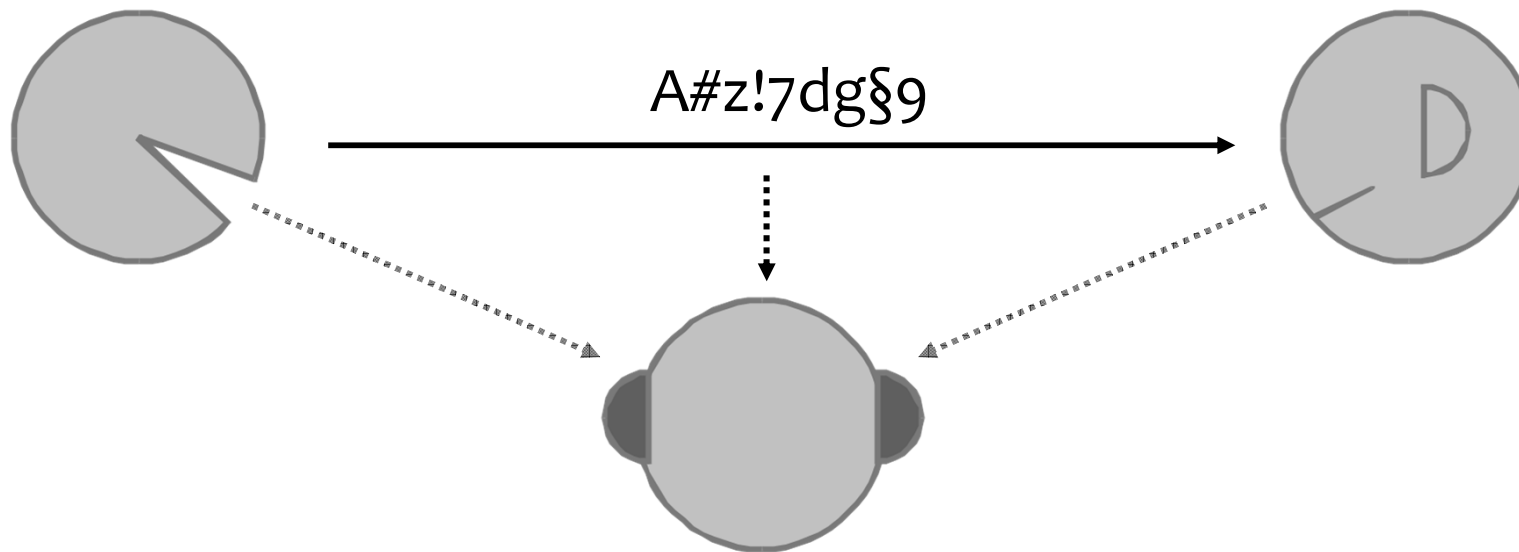
Bringe die Nachricht in eine übertragbare Form.

- Brieftaube
- Morsealphabet
- Blindenschrift
- ASCII
- Englisch
- ...



# Geheime Nachrichtenübertragung

- Geheime Nachricht
- Sender, Empfänger
- Zu-, Mit- Hörer (Angreifer)



# Chiffrieren

## *Verschlüsseln*

Bringe die Nachricht in eine geheime Form.

- Cäsar
- Vigenère
- One-Time-Pad
- Skytale
- Preußischer optischer Zeigertelegraf
- ...

# Codieren

- Verfahren (Algorithmus, öffentlich)
- Zuordnung (öffentlich, bekannt, ...)
- Original → Code

Original	A	B	C	D	E	F	...	X	Y	Z
Code	..	....	----	...	.	----	...	----	----	----

Original	Klaus Schmeh, Versteckte Botschaften, Heise
Code	978-3-936931-54-9

# Chiffrieren/Verschlüsseln

- Verfahren (Algorithmus, öffentlich)
- Schlüssel (geheim)
- Klartext (KT) → Geheimtext (GT)
- Klartextalphabet (KTA) → Geheimtextalphabet (GTA)

KTA	A	B	C	D	E	F	...	X	Y	Z
GTA	Z	Y	X	W	V	U	...	C	B	A

# Inhalte

1. Was bei den Sachsen läuft ☺
2. Überblick
3. Klassische Verfahren
4. „Kryptographie kompakt“
5. Bonus: Steganographie

# Cäsar-Verfahren

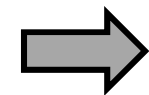
Verfahren: Substitution einzelner Zeichen

Schlüssel: Verschiebung um eine festgelegte (geheime) Anzahl von Buchstaben (hier: +1)

KTA	A	B	C	D	E	F	...	X	Y	Z
GTA	B	C	D	E	F	G	...	Y	Z	A

Verschlüsselung: C  $\rightarrow$  D und CAESAR  $\rightarrow$  DBFTBS

Entschlüsselung: J  $\rightarrow$  I und JOGP  $\rightarrow$  INFO



# Vigenère-Verfahren

Verfahren: Substitution einzelner Zeichen

Schlüssel: Cäsar-Verschlüsselung mit mehreren Alphabeten, z.B. Schlüsselwort: BLA

KTA	A	B	C	D	E	F	...	X	Y	Z
GTA	B									

KTA	A	B	C	D	E	F	...	X	Y	Z
GTA	L									

KTA	A	B	C	D	E	F	...	X	Y	Z
GTA	A									

# Vigenère-Verfahren

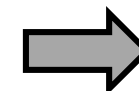
KTA	A	B	C	D	E	F	...	X	Y	Z
GTA	B	C	D	E	F	G	...	Y	Z	A

KTA	A	B	C	D	E	F	...	X	Y	Z
GTA	L	M	N	O	P	Q	...	I	J	K

KTA	A	B	C	D	E	F	...	X	Y	Z
GTA	A	B	C	D	E	F	...	X	Y	Z

KT	I	N	F	O	R	M	A	T	I	K
SW	B	L	A	B	L	A	B	L	A	B
GTA	J	Y	F	P	C	M	B	E	I	L

Hilfsmittel: 





# Verbesserung der Verschlüsselung

## Cäsar

KT	I	N	F	O	R	M	A	T	I	K
GT	J	O	G	P	S	N	B	U	J	L

## Vigenère

KT	I	N	F	O	R	M	A	T	I	K
SW	B	L	A	B	L	A	B	L	A	B
GT	J	Z	F	P	D	M	B	E	I	L

## One-Time-Pad

KT	I	N	F	O	R	M	A	T	I	K
SW	U	N	T	E	R	R	I	C	H	T
GT	C	A	Y	S	I	D	I	V	P	D

# Cäsar mit der Tabellenkalkulation



- Nutzung des ASCII
- Funktionen zur Umwandlung
- Erstellen einer Vorlage zur Verschlüsselung (Entschlüsselung)

# American Standard Code for Information Interchange – ASCII

0	32		64	@	96	`	128	€	160		192	À	224	à
1	33	!	65	A	97	a	129		161	ı	193	Á	225	á
2	34	"	66	B	98	b	130	,	162		194	Â	226	â
3	35	#	67	C	99	c	131	f	163		195	Ã	227	ã
4	36	\$	68	D	100	d	132	~	164		196	Ä	228	ä
5	37	%	69	E	101	e	133	...	165		197	Å	229	å
6	38	&	70	F	102	f	134	†	166	ı	198	Æ	230	æ
7	39	'	71	G	103	g	135	‡	167		199	Ç	231	ç
8	40	(	72	H	104	h	136	^	168		200	È	232	è
9	41	)	73	I	105	i	137		169		201	É	233	é
10	42	*	74	J	106	j	138	Š	170		202	Ê	234	ê
11	43	+	75	K	107	k	139	<	171	«	203	Ë	235	ë
12	44	,	76	L	108	l	140	Œ	172	¬	204	Ì	236	ì
13	45	-	77	M	109	m	141		173		205	Í	237	í
14	46	.	78	N	110	n	142	Ž	174		206	Î	238	î
15	47	/	79	O	111	o	143		175		207	Ï	239	ï
16	48	0	80	P	112	p	144		176		208	Ð	240	ð
17	49	1	81	Q	113	q	145	`	177		209	Ñ	241	ñ
18	50	2	82	R	114	r	146	/	178		210	Ò	242	ò
19	51	3	83	S	115	s	147		179		211	Ó	243	ó
20	52	4	84	T	116	t	148	~	180		212	Ô	244	ô
21	53	5	85	U	117	u	149	•	181		213	Õ	245	õ
22	54	6	86	V	118	v	150	-	182		214	Ö	246	ö
23	55	7	87	W	119	w	151	—	183		215	×	247	÷
24	56	8	88	X	120	x	152	ˆ	184		216	Ø	248	ø
25	57	9	89	Y	121	y	153	™	185		217	Ù	249	ù
26	58	:	90	Z	122	z	154	š	186		218	Ú	250	ú
27	59	;	91	[	123	{	155	>	187	»	219	Û	251	û
28	60	<	92	\	124		156	œ	188		220	Ü	252	ü
29	61	=	93	]	125	}	157		189		221	Ý	253	ý
30	62	>	94	^	126	~	158	ž	190		222	Þ	254	þ
31	63	?	95	_	127		159	Ÿ	191	¡	223	ß	255	ÿ

Dez	Hex	Okt	
64	0x40	100	@
65	0x41	101	A
66	0x42	102	B
67	0x43	103	C
68	0x44	104	D
69	0x45	105	E
70	0x46	106	F
71	0x47	107	G
72	0x48	110	H

<http://de.wikipedia.org/wiki/Ascii#ASCII-Tabelle>; 21.03.2011; 21:00

# Funktionen in der Tabellenkalkulation

- dienen der einfachen Eingabe von (sonst komplizierten) Formeln
- tragen einen vorgegebene Funktionsnamen

Beispiel:

$=A1+A2+\dots+A100 \rightarrow =\text{Summe}(A1:A100)$

Schreibweise:

$= \text{Funktionsname} (\text{Argument; Bedingung; } \dots)$

# Funktionen zur Umwandlung

= **CODE (Zeichen)**



Zellname

z. B. =CODE („A“) = 65

→ Umwandlung des „Buchstabens“ in eine Zahl zum Berechnen

= **ZEICHEN (Zahl)**

z.B. =ZEICHEN(72) = H

→ Umwandeln der Zahl in einen Buchstaben

# Kleine Helferlein – Tabellenkalkulation

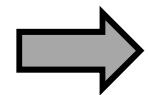
## Substitutionsverfahren

I	N	F	O	R	M	A	T	I	K
73	78	70	79	82	77	65	84	73	75
74	79	71	80	83	78	66	85	74	76
J	O	G	P	S	N	B	U	J	L

mithilfe der Tabellenkalkulation

- Klartext
- =CODE(A1) [I → 73]
- =A2+1 [73 → 74]
- =ZEICHEN(A3) [74 → J]

Zellname



# Funktionen zur Umwandlung

Problem:

=CODE („Z“) = 90

unter Einbeziehung der Verschiebungsweite

=ZEICHEN (90+1) = [

Lösung:

=WENN (Buchstabe+Verschiebungsweite>90;  
Buchstabe+Verschiebungsweite-26;  
Buchstabe+Verschiebungsweite)

Ohne Zwischenschritte:

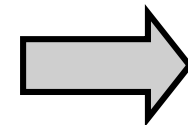
=WENN ((CODE(B3)+\$B\$5)>90;  
ZEICHEN(CODE(B3)+\$B\$5-26);  
ZEICHEN(CODE(B3)+\$B\$5))

# Kleine Helferlein – Textverarbeitung

- Ziel: Kennenlernen der Textverarbeitung
- Verschlüsselung: Substitution – Cäsar+1

KTA	A	B	C	D	E	F	...	X	Y	Z
GTA	B	C	D	E	F	G	...	Y	Z	A

- Suchen und Ersetzen
- $A \rightarrow B; B \rightarrow C; C \rightarrow D; \dots; Y \rightarrow Z; Z \rightarrow A$



AAAAAAAAAAAAAAAAAAAAA ☹️

- $A \rightarrow \#; Z \rightarrow A; Y \rightarrow Z; \dots; B \rightarrow C; A \rightarrow B = \# \rightarrow B$

TVDIFOVOEFSTFUAFO 😊



# Energizer

Aktivierungsspiele sind nicht der eigentliche Gegenstand des Unterrichts. Sie werden zu unterschiedlichen Zwecken und bei verschiedenen Gelegenheiten als pädagogisches Mittel in den Unterricht eingestreut, um ...

- sich zu entspannen
- „Dampf abzulassen“
- Ermüdungserscheinungen entgegenzuwirken
- ...

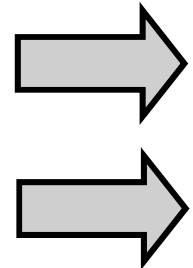
# Energizer - 3

## Freimaureralphabet

A B.	C D.	E F.
G H.	I J.	K L.
M N.	O P.	Q R.

~~S T.  
 U V. W X.  
 Y Z.~~   
LABBÉ

A = ⊐	H = ⊔	O = ⊐	V = ⊗
B = ⊑	J = ⊔	P = ⊐	W = <
C = ⊐	K = ⊔	Q = ⊐	X = <
D = ⊐	L = ⊐	R = ⊐	Y = ^
E = ⊐	M = ⊐	S = V	Z = ^
F = ⊐	N = ⊐	T = V	<small>LABBÉ</small>
G = ⊐	U = >		

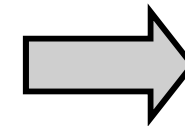


<http://www.labbe.de/zzebra/index.asp?themaId=472&titelId=1627>  
 (26.03.2011; 14:00)

# Kleine Helferlein - Cryptool

Quelle:

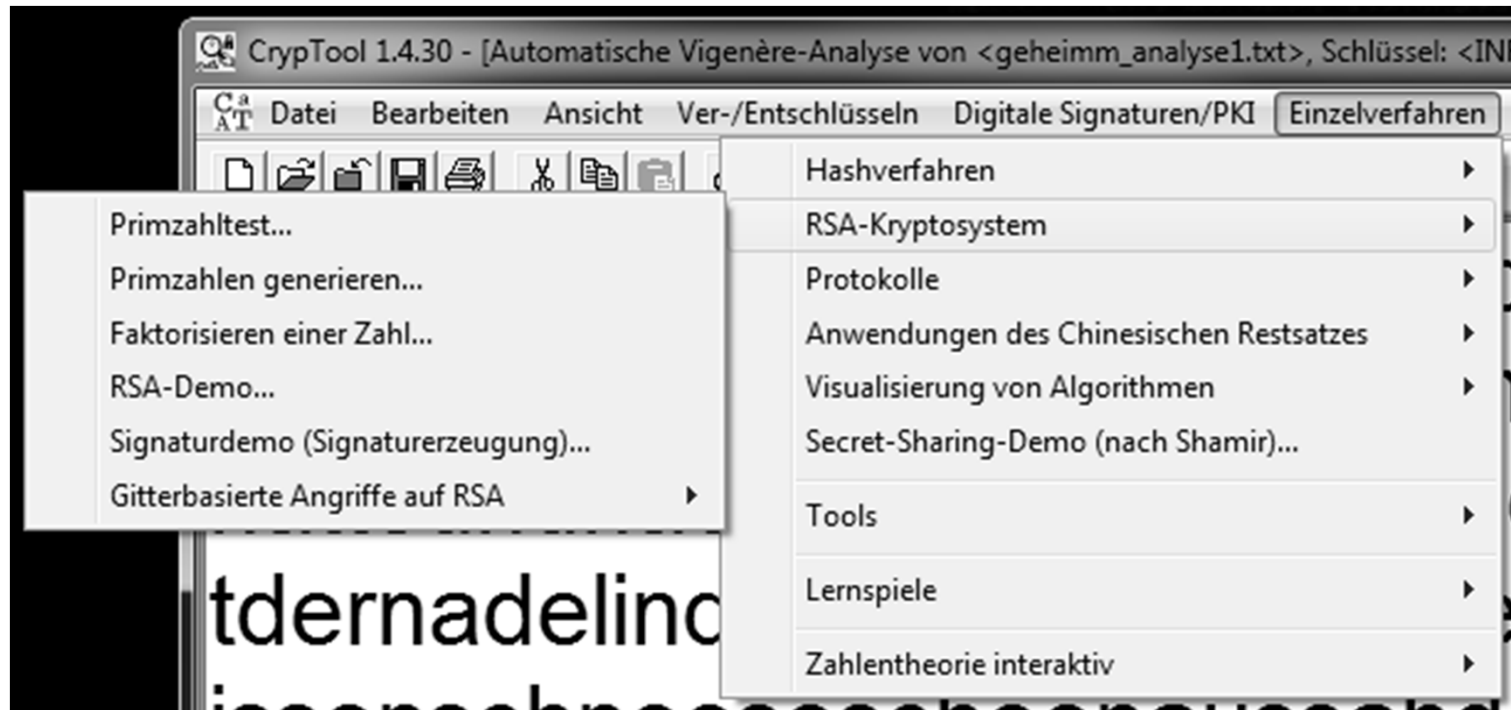
- <http://www.cryptool.org/>



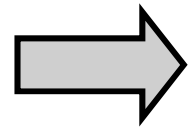
einige Möglichkeiten:

1. Verschlüsseln
2. Entschlüsseln
3. Knacken
4. und außerdem

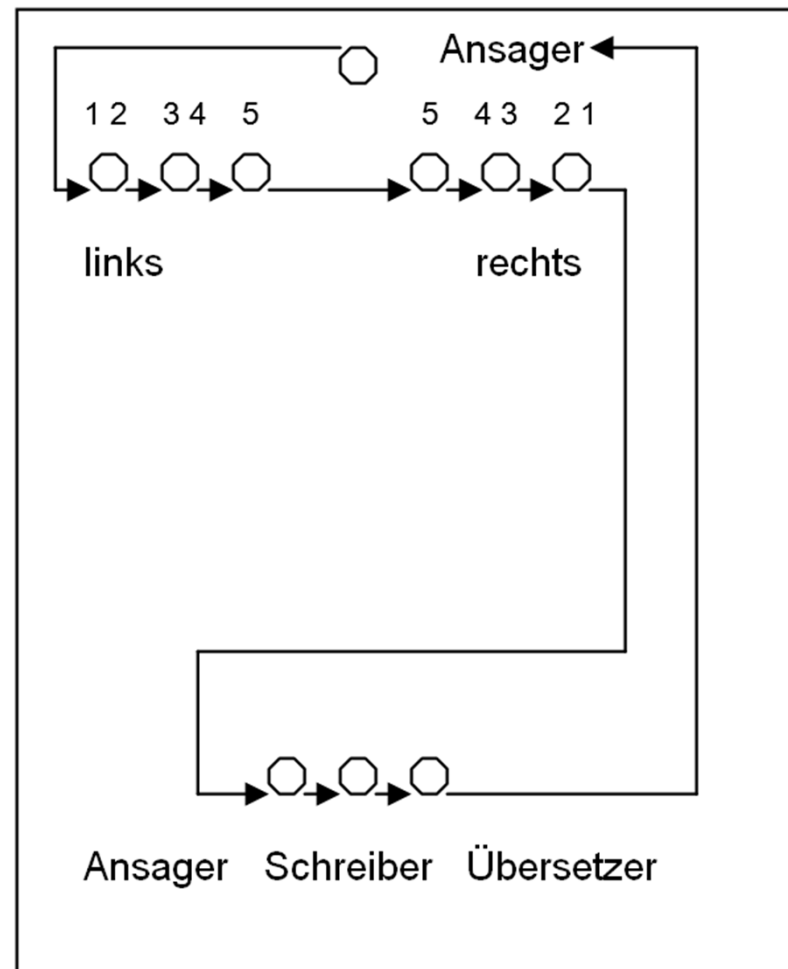
# Kleine Helferlein - Cryptool



# Energizer – Fackeltelegraph



# Energizer – Fackeltelegraph



# Inhalte

1. Was bei den Sachsen läuft ☺
2. Überblick
3. Klassische Verfahren
4. „Kryptographie kompakt“
5. Bonus: Steganographie

# Alternative: Projekt



[http://lehrerfortbildung-bw.de/kompetenzen/projektkompetenz/methoden\\_a\\_z/gruppenpuzzle](http://lehrerfortbildung-bw.de/kompetenzen/projektkompetenz/methoden_a_z/gruppenpuzzle)



# Inhalte

1. Was bei den Sachsen läuft ☺
2. Überblick
3. Klassische Verfahren
4. „Kryptographie kompakt“
5. Bonus: Steganographie

# Steganographie – Akrostiche

Inschrift auf einem Grabstein in Montreal (Kanada)  
gestiftet von John Laird McCaffery an seinen Freund

Free your body and soul  
Unfold your powerful wings  
Climb up the highest mountains  
Kick your feet up in the air  
You may now live forever  
On Return to the earth  
Unless you feel good where you are

