Literature

A. Beutelspacher: Kryptologie. Vieweg, 1991.

A. Salomaa, *Public-Key Cryptography*. Springer-Verlag, 1996.

D. Wätjen, Kryptographie. Grundlagen, Algorithmen, Protokolle. Spektrum-Verlag, 2003.

R. Merkle, M. Hellman: Hiding informations and signatures in trapdoor knapsacks. *IEEE Transactions on Information Theory* **IT-24** (1978) 525–530.

R.L. Rivest / A. Shamir / L. Adleman, A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM* **21** (1978) 120–126.

J. Kari, Observations concerning a public-key cryptosystem based on iterated morphisms. *Theor. Comp. Sci.* **66**(1989) 45–53.

Function φ

α	A	B	C	D	E	F	G	H	I
$\varphi(\alpha)$	0	1	2	3	4	5	6	7	8
α	J	K	L	M	N	O	P	Q	R
$\varphi(\alpha)$	9	10	11	12	13	14	15	16	17
α	S	T	U	V	W	X	Y	Z	
$\varphi(\alpha)$	18	19	20	21	22	23	24	25	

Remarks on the Distribution of Letters

English	%	German	%	French	%
E	12.31	E	18.46	E	15.87
T	9.59	N	11.42	A	9.42
A	8.05	I	8.02	I	8.41
O	7.94	R	7.14	S	7.90
N	7.19	S	7.04	T	7.26
I	7.18	A	5.38	N	7.15
S	6.59	T	5.22	R	6.46
R	6.03	U	5.01	U	6.24

An Encrypted Text I

F R Q V L G H U W K L V Q L F H Z U L W L Q J

5-mal : L

3-mal : Q

2-mal : F, H, U, T, W

1-mal : G, J, K, R, Z,

0-mal : A, B, C, D, E, I, M, N, O, P, S, T, X, Y

Affine Cryptosystems – Example

α	A	B	C	D	E	F	G	H	I
$\varphi(\alpha)$	0	1	2	3	4	5	6	7	8
$a \cdot \varphi(\alpha) + b \bmod 26$	5	8	11	14	17	20	23	0	3
$v_{(3,5)}(\alpha)$	F	I	L	O	R	U	X	A	D

α	J	K	L	M	N	O	P	Q	R
$\varphi(\alpha)$	9	10	11	12	13	14	15	16	17
$a \cdot \varphi(\alpha) + b \bmod 26$	6	9	12	15	18	21	24	1	4
$v_{(3,5)}(\alpha)$	G	J	M	P	S	V	Y	B	E

α		S	T	U	V	W	X	Y	Z
$\varphi(\alpha)$	18	19	20	21	22	23	24	25	
$a \cdot \varphi(\alpha) + b \bmod 26$	7	10	13	16	19	22	25	2	
$v_{(3,5)}(\alpha)$	H	K	N	Q	T	W	Z	C	

A Fairplay Table

G	R	E	I	F
S	W	A	L	D
B	C	H	K	M
N	O	P	Q	T
U	V	X	Y	Z

Vigenère Table

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
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	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	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

An Encrypted Text II

U E Q P C V C K A H V N R Z U R N L A O
K I R V G J T D V R V R I C V I D L M Y
I Y S B C C O J Q S Z N Y M B V D L O K
F S L M W E F R Z A V I Q M F J T D I H
C I F P S E B X M F F T D M H Z G N M W
K A X A U V U H J H N U U L S V S J I P
J C K T I V S V M Z J E N Z S K A H Z S
U I H Q V I B X M F F I P L C X E Q X O
C A V B V R T W M B L N G N I V R L P F
V T D M H Z G N M W K R X V R Q E K V R
L K D B S E I P U C E A W J S B A P M B
V S Z C F U E G I T L E U O S J O U O H
U A V A G Z E Z I S Y R H V R Z H U M F
R R E M W K N L K V K G H A H F E U B K
L R G M B J I H L I I F W M B Z H U M P
L E U W G R B H Z O L C K V W T H W D S
I L D A G V N E M J F R V Q S V I Q M U
V S W M Z C T H I I W G D J S X E O W S
J T K I H K E Q

An Encrypted Text IIa

U E Q P C V C K A H V N R Z U R N L A O
K I R V G J T D V R V R I C V I D L M Y
I Y S B C C O J Q S Z N Y M B V D L O K
F S L M W E F R Z A V I Q M F J T D I H
C I F P S E B X M F F T D M H Z G N M W
K A X A U V U H J H N U U L S V S J I P
J C K T I V S V M Z J E N Z S K A H Z S
U I H Q V I B X M F F I P L C X E Q X O
C A V B V R T W M B L N G N I V R L P F
V T D M H Z G N M W K R X V R Q E K V R
L K D B S E I P U C E A W J S B A P M B
V S Z C F U E G I T L E U O S J O U O H
U A V A G Z E Z I S Y R H V R Z H U M F
R R E M W K N L K V K G H A H F E U B K
L R G M B J I H L I I F W M B Z H U M P
L E U W G R B H Z O L C K V W T H W D S
I L D A G V N E M J F R V Q S V I Q M U
V S W M Z C T H I I W G D J S X E O W S
J T K I H K E Q

Folge	Abstand
JTD	$50 = 2 \cdot 5^2$
VIQM	$265 = 5 \cdot 53$
TDMHZGNMWK	$90 = 2 \cdot 3^2 \cdot 5$
MWK	$75 = 3 \cdot 5^2$
ZHUM	$40 = 2^3 \cdot 5$
KAH	$128 = 2^7$

The Corresponding Plaintext II

D E N H O E C H S T E N O R G A N I S A
T I O N S S T A N D E R F U H R D I E K
R Y P T O L O G I E I N V E N E D I G W
O S I E I N F O R M E I N E R S T A A T
L I C H E N B U E R O T A E T I G K E I
T A U S G E U E B T W U R D E E S G A B
S C H L U E S S E L S E K R E T A E R E
D I E I H R B U E R O I M D O G E N P A
L A S T H A T T E N U N D F U E R I H R
E T A E T I G K E I T R U N D Z E H N D
U K A T E N I M M O N A T B E K A M E N
E S W U R D E D A F U E R G E S O R G T
D A S S S I E W A E H R E N D I H R E R
A R B E I T N I C H T G E S T O E R T W
U R D E N S I E D U R F T E N I H R E B
U E R O S A B E R A U C H N I C H T V E
R L A S S E N B E V O R S I E E I N E G
E S T E L L T E A U F G A B E G E L O E
S T H A T T E N

DEN HÖCHSTEN ORGANISA-
TIONSSTAND ERFUHR DIE
KRYPTOLOGIE IN VENEDIG, WO
SIE IN FORM EINER STAAT-
LICHEN BÜROTÄTIGKEIT
AUSGEÜBT WURDE. ES GAB
SCHLÜSSELSEKRETÄRE,
DIE IHR BÜRO IM DOGENPA-
LAST HATTEN UND FÜR IHRE
TÄTIGKEIT RUND ZEHN
DUKATEN IM MONAT BEKAMEN.
ES WURDE DAFÜR GESORGT,
DASS SIE WÄHREND IHRER
ARBEIT NICHT GESTÖRT
WURDEN. SIE DURFTEN IHRE
BÜROS ABER AUCH NICHT
VERLASSEN, BEVOR SIE EINE
GESTELLTE AUFGABE GELÖST
HATTEN.