Literature

C. E. Shannon: Communication Theory and Secrecy Systems, Bell System Technical Journal, 1949.

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

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.

A. Beutelspacher: Kryptologie. Vieweg, 1991.

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

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	17.40	E	15.87
T	9.59	N	9.78	A	9.42
A	8.05	I	7.55	I	8.41
O	7.94	S	7.27	S	7.90
N	7.19	R	7.00	T	7.26
I	7.18	A	6.51	N	7.15
S	6.59	T	6.15	R	6.46
R	6.03	D	5.08	U	6.24

An Encrypted Text

F R Q V L G H U W K L V Q L F H F R Q W U L E X W L R Q

5 times: L

4 times: Q

3 times: F, R, W

2 times: V, H, U

1 times: G, K, E, X

0 times: A, B, C, D, I, J, M, N, O, P, S, T, Y, Z

Mono Alphabetical Substitution Ciphers

Caesar cipher (permutation by shifting)

Other permutations, for example:

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

MAGDEBURG $\Longrightarrow$ XGWIFRMPW

Affine Ciphers – Example

α	A	B	C	D	E	F	G	H	I
$\varphi(\alpha)$	0	1	2	3	4	5	6	7	8
$(3 \cdot \varphi(\alpha) + 5) \bmod 26$	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
$(3 \cdot \varphi(\alpha) + 5) \bmod 26$	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
$(3 \cdot \varphi(\alpha) + 5) \bmod 26$	7	10	13	16	19	22	25	2
$v_{(3,5)}(\alpha)$	H	K	N	Q	T	W	Z	C