Einführung in Kryptographie und Datensicherheit Übung 2

Tilman Bender Matrikelnummer: 108011247244

29. Oktober 2011

Aufgabe 3

a)

Siehe 1

Tabelle 1: Stubstitutionstabelle für $k = 10$

Klartext	Position	Neue Position	Geheimtext
a	0	$0 + 10 \equiv 10 \mod 26$	K
b	1	$1 + 10 \equiv 11 \mod 26$	L
c	2	$2 + 10 \equiv 12 \mod 26$	M
d	3	$3 + 10 \equiv 13 \mod 26$	N
e	4	$4 + 10 \equiv 14 \mod 26$	O
f	5	$5 + 10 \equiv 15 \mod 26$	P
g	6	$6 + 10 \equiv 16 \mod 26$	Q
h	7	$7 + 10 \equiv 17 \mod 26$	R
i	8	$8 + 10 \equiv 18 \mod 26$	S
j	9	$9 + 10 \equiv 19 \mod 26$	T
k	10	$10 + 10 \equiv 20 \mod 26$	U
l	11	$11 + 10 \equiv 21 \mod 26$	V
m	12	$12 + 10 \equiv 22 \mod 26$	W
n	13	$13 + 10 \equiv 23 \mod 26$	X
o	14	$14 + 10 \equiv 24 \mod 26$	Y
p	15	$15 + 10 \equiv 25 \mod 26$	Z
q	16	$16 + 10 \equiv 0 \mod 26$	A
r	17	$17 + 10 \equiv 1 \mod 26$	B
s	18	$18 + 10 \equiv 2 \mod 26$	C
t	19	$19 + 10 \equiv 3 \mod 26$	D
u	20	$20 + 10 \equiv 4 \mod 26$	E
v	21	$21 + 10 \equiv 5 \mod 26$	F
w	22	$22 + 10 \equiv 6 \mod 26$	G
x	23	$23 + 10 \equiv 7 \mod 26$	H
y	24	$24 + 10 \equiv 8 \mod 26$	I
z	25	$25 + 10 \equiv 9 \mod 26$	J

b)

Siehe 2.

Tabelle 2: Shift-Chiffre mit k=10 angewendet

d	a	t	e	n	s	i	c	h	e	r	h	e	i	t
N	K	D	O	X	C	S	M	R	O	B	R	O	S	D

c)

Die Shift-Chiffre ist lediglich ein Spezialfall der Substitionschiffre bei dem die Substitutionsregeln nach einem bestimmten Schema generiert wurden. Damit ist die Shift-Chiffre auch für Frequenzanalyse anfällig. Streng genommen könnte man sogar behaupten, dass die Shift-Chiffre bei großen Alphabeten etwas unsicherer ist, da ein Angreifer der die Substitutionsregeln für mehrere im Alphabet aufeinander folgende Buchstaben kennt daraus auf die allgemeine Regel (den Shift-Offset) schließen könnte.

d)

Ja das erhöhen des Offsets mit jedem Buchstaben erhöht die Sicherheit gegenüber der Frequenzanalyse. Diese beruht darauf, dass zwei Vorkommen eines Buchstabens des Klartext-Alphabets immer mit dem selben Buchstaben des Chiffre-Alphabets ersetzt werden und so die statistischen Eigenschafen des Klartexts auf den Chiffretext übergehen. Durch das Verschieben des Offsets erhält der Chiffre-Text eine andere Häufigkeitsverteilung als der Klartext.