Angriff über wahrscheinliches Wort der Länge $k \cdot n$:

- bei richtiger Lage x und y bekannt in $y = xT + t$ für k verschiedene x und y
- zusammenfassen der Gleichungungen

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_k \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} T + \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} t = \begin{pmatrix} x_1 & 1 \\ x_2 & 1 \\ \vdots & \vdots \\ x_k & 1 \end{pmatrix} \begin{pmatrix} T \\ t \end{pmatrix}$$

- nach T, t auflösbar, falls $k \geq n + 1$, also Mindestlänge des wahrscheinlichen Wortes $= (n + 1) \cdot n = n^2 + n$
- falls wahrscheinliches Wort länger als nötig: Gleichungssystem überbestimmt; Ausschluss falscher Lage falls keine Lösung

5 Transposition

- die Zeichen des Klartextes werden beibehalten, aber in der Reihenfolge geändert
- einfachste Verfahren schreiben Nachricht z.B. waagerecht in Zeilen vorgegebener Länge lesen Senkrecht heraus

```
m  a  n  k  o  e  n
n  t  e  s  t  a  t
t  d  e  s  s  e  n
a  u  c  h  d  i  a
g  o  n  a  l  h  e
r  a  u  s  l  e  s
e  n
```

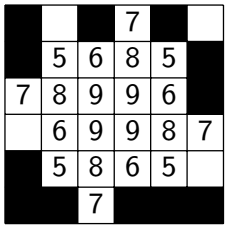
  $\Rightarrow$ `MNTAG REATD UOANN EECNU KSSHA SOTSD LLEAE IHENT NAES`
- letzte Zeile wird häufig mit Blendern aufgefüllt – unnötig, da Empfänger Länge der Nachricht kennt

5.1 Drehraster

- Raster erlauben sukzessive unterschiedliche Teilmengen des Textes auszulesen

  KCRCHZNIUHTEREAN

- decodieren durch Schreiben in die Raster
- Drehraster: ein Raster, das in 90°-Schritten gedreht wird, statt mehrere verschiedene Raster
- Konstruktion:
  - numeriere Quadranten rotationssymmetrisch
  - wähle zu jeder Zahl einen Quadranten; hier ist das Loch, in den übrigen Quadranten deckt das Raster ab



5.2 Spalten-Transpositionen

- Spalten-Transpositionen erlauben Einführung von Schlüsseln
- zeilenweise Schreiben, spaltenweise lesen, aber Reihenfolge der Spalten gemäß Schlüssel
- Beispiel: Schlüssel=2 4 1 3

1	2	3	4		2	4	1	3
e	s	w	a		s	a	e	w
r	s	c	h	⇒	s	h	r	c
o	n	d	u		n	u	o	d
n	k	e	l		k	l	n	e

  ⇒ SSNKAHULERONWCDE

- für Kryptanalyse äquivalent: zeilenweises Auslesen nach Umordnen, Blocktransposition
  ⇒ SAEWSHRCNUODKLNE

- gemischte Zeilen-Spalten-Transpositionen permutieren mit einem weiteren Schlüssel auch die Zeilen
- Beispiel: Schlüssel=2 4 1 3 und 3 4 2 1

	1	2	3	4			2	4	1	3			2	4	1	3
1	e	s	w	a		1	s	a	e	w		3	n	u	o	d
2	r	s	c	h	⇒	2	s	h	r	c	⇒	4	k	l	n	e
3	o	n	d	u		3	n	u	o	d		2	s	h	r	c
4	n	k	e	l		4	k	l	n	e		1	s	a	e	w

  ⇒ NKSSULHAONRDECW
- oder gemischte Zeilen-Block-Transposition
  ⇒ NUODKLNESHRCSAEW
- sei X die $(l \times k)$-Matrix des Klartextes und π_1, π_2 Permutationsmatrizen der Größe l bzw. k

Spaltentransposition	$(X\pi_2)^T$
Blocktransposition	$X\pi_2$
Zeilen-Spalten-Transposition	$(\pi_1 X \pi_2)^T$
Zeilen-Block-Transposition	$\pi_1 X \pi_2$

- doppelte Spalten-Transposition ist bei $l = k$ äquivalent zu Zeilen-Block-Transposition: $((X\pi_1)^T\pi_2)^T = \pi_2^T X \pi_1$

5.3 Angriff über Bigramm-Häufigkeiten

- Geheimtext SSOAT HCDRI ENEBE NIFSC EIATR IIRSO SRUZE EPNHZ THTSV ELUN sei zu entschlüsseln
- Länge 49, Vermutung 7×7-Quadrat mit Spaltentransposition

S	D	E	I	S	E	T
S	R	N	A	O	P	S
O	I	I	T	S	N	V
A	E	F	R	R	H	E
T	N	S	I	U	Z	L
H	E	C	I	Z	T	U
C	B	E	R	E	H	N

- beginne mit einer Spalte, bestimme Bigrammhäufigkeiten bei Kombination mit allen anderen Spalten, multipliziere alle Häufigkeiten einer Spalte
  - erste zu dritter Spalte:
    $99\% \cdot 7\% \cdot 1\% \cdot 15\% \cdot 50\% \cdot 1\% \cdot 1\% = 5{,}20 \cdot 10^{-16}$
  - erste zu sechster Spalte (Maximum):
    $99\% \cdot 22\% \cdot 64\% \cdot 20\% \cdot 26\% \cdot 47\% \cdot 242\% = 8{,}24 \cdot 10^{-10}$
- usw. ergibt sich die Reihenfolge 1., 6., 5., 7. Spalte

- wir haben bis jetzt

S	E	S	T	D	E	I
S	P	O	S	R	N	A
O	N	S	V	I	I	T
A	H	R	E	E	F	R
T	Z	U	L	N	S	I
H	T	Z	U	E	C	I
C	H	E	N	B	E	R

- hier geht es nicht mehr gut weiter; wir arbeiten rückwärts von der ersten Spalte und rekonstruieren

D	I	E	S	E	S	T
R	A	N	S	P	O	S
I	T	I	O	N	S	V
E	R	F	A	H	R	E
N	I	S	T	Z	U	L
E	I	C	H	T	Z	U
B	R	E	C	H	E	N

- auch zusätzliche Zeilentransposition hätte bis hierhin keine Probleme bereitet; die richtige Sortierung der Zeilen wäre jetzt leicht zu rekonstruieren

5.4 Multiples Anagrammieren

- ähnlich wie bei Superimposition: verwende statt Periodizität mehrere Geheimtexte zum gleichen Schlüssel
- in der Regel mögliche Reihenfolge, sodass alle Texte sinnvoll, schnell eindeutig
- Beispiel: `CINCHAHRT` und `ATBCHUBSE`
  - zweites `C` von `CINCHAHRT` passt nicht zum zweiten `H`, da in `ATBCHUBSE` dann `CB` entsteht, also:

C	H	C	H	I	N	A	R	T
C	H	A	B	T	B	U	S	E

  - vor `CH` in beiden Texten Vokal oder `S` zu erwarten, also nur

A	C	H	C	H	I	N	R	T
U	C	H	A	B	T	B	S	E

  - vor zweiten `CH` ebenfalls Vokal zu erwarten, also nur

A	C	H	I	C	H	N	R	T
U	C	H	T	A	B	B	S	E

  - von hier aus schnell zu

N	A	C	H	R	I	C	H	T
B	U	C	H	S	T	A	B	E

- bei längeren Texten mehrere parallele Texte nötig, aber selber Ansatz