UNIKASSEL VERSITÄT

Angewandte Informations Sicherheit

Historical Ciphers Systems
Top 10 Open Problems

May 5, 2016

George Lasry
george.lasry@ais.uni-kassel.de

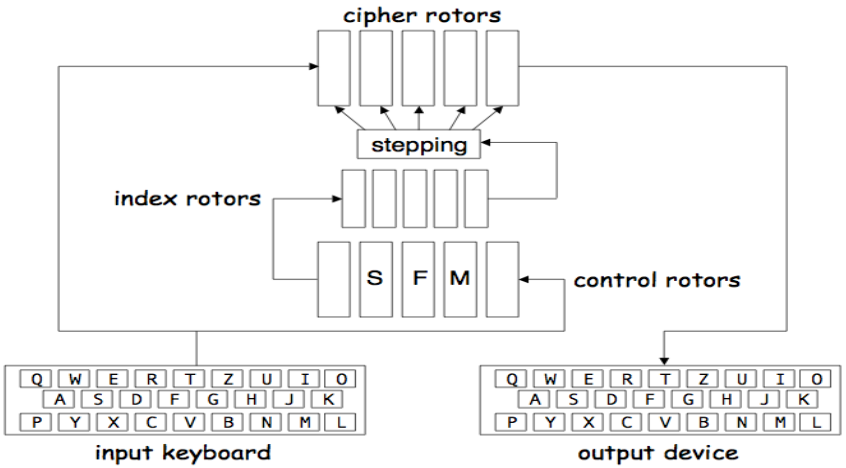
Open Problems - Criteria

- **Generic method vs. deciphering a document**
- **System details are known**
  - For many there are simulators
- **Published methods vs. classified**
- **General vs. special case solutions**
  - Ciphertext only vs. known plaintext
  - Single message vs. in-depth messages
  - Short vs. long messages
  - Long vs. short keys
- **Brute force not feasible**
  - But computer most likely required

Top 10 Open Problems

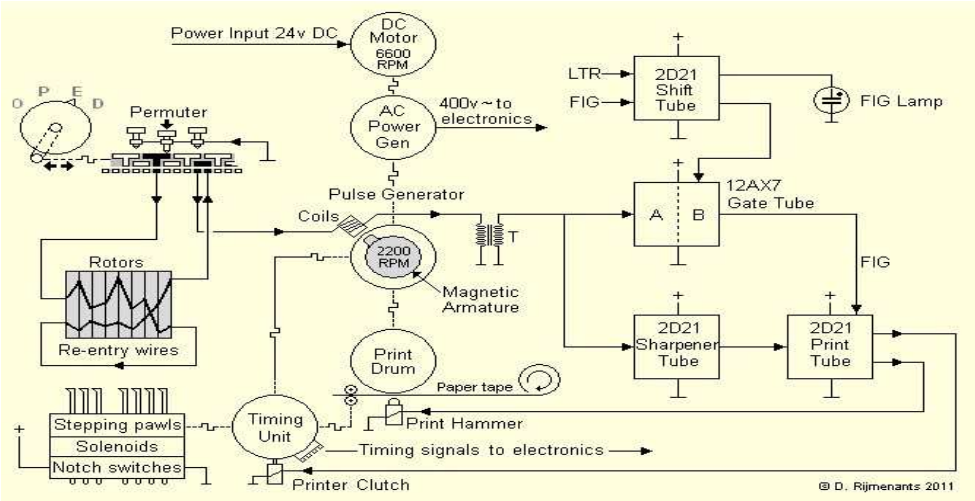
1. SIGABA
2. KL-7
3. Siemens T52D “Sturgeon”
4. Hagelin CX-52
5. Fialka
6. Lorenz SZ42 “Tunny” – Ψ_1 limitation
7. Hagelin M-209 – short messages
8. Double Transposition – long random keys
9. Enigma – short message
10. Chaocipher – single message

Problem 1: SIGABA (US)



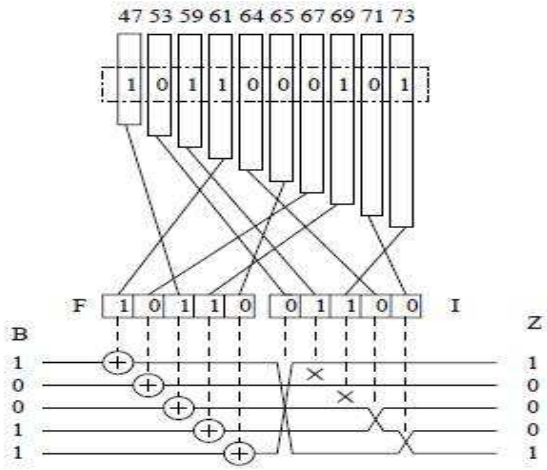
- **Possible keys (WWII): $2^{96} = 10^{29}$**
- **Best published: known-plaintext $2^{60} = 10^{18}$ steps**

Problem 2: KL-7 (US)



- **Details of the machine known (+ simulator)**
- **Best published cryptanalytic method: None!**

Problem 3: Siemens & Halske T52D

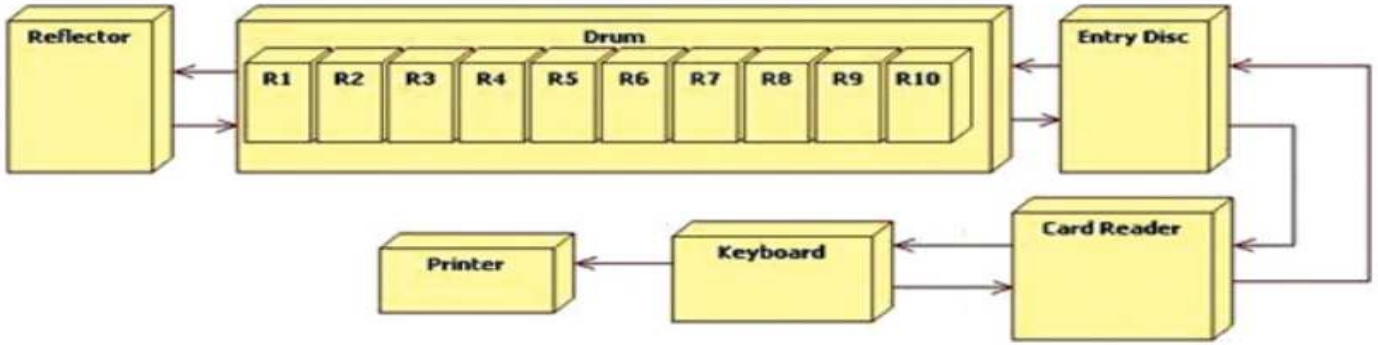


- Successor of T52a/b/c: Irregular wheel stepping
- Possible key settings: $2^{73} = 10^{24}$
- Best published method: > 5 messages in depth

Problem 4: Hagelin CX-52

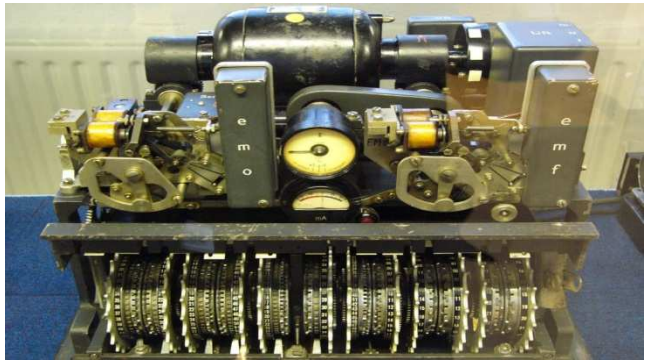
- Successor of C38/M209: Irregular wheel stepping
- Possible key settings: $2^{439} = 10^{132}$
- Best published method: Known-plaintext

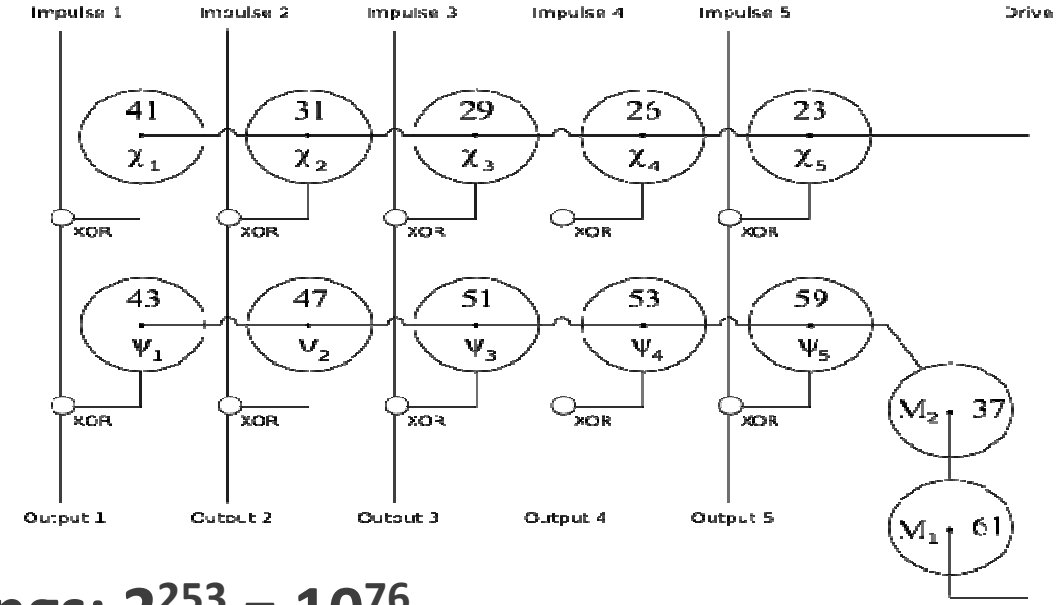
Problem 5: Fialka M-125 (Russia)



- Possible key settings: $2^{250} = 10^{75}$
- Best published method: None!

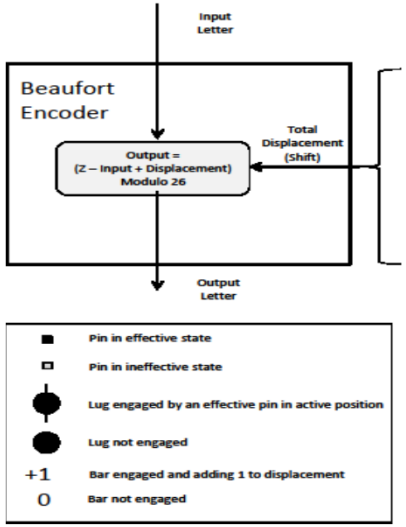
Problem 6: Lorenz SZ42 “Tunny” - Ψ1 stepping limitation

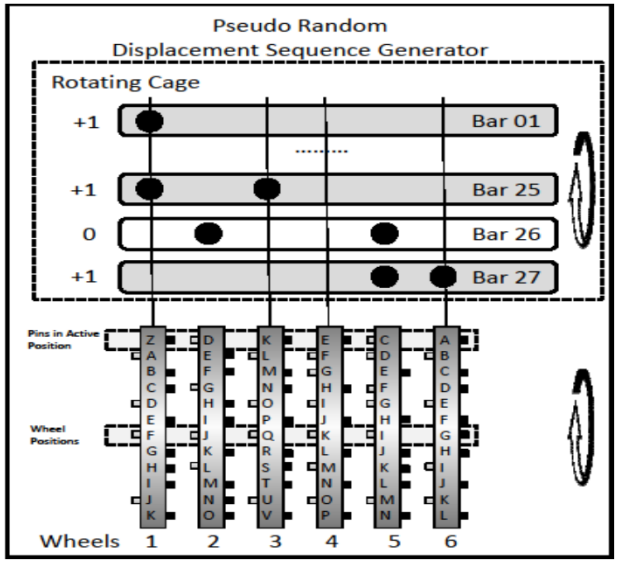




- Possible Ψ wheel settings: $2^{253} = 10^{76}$
- Best published method: None!

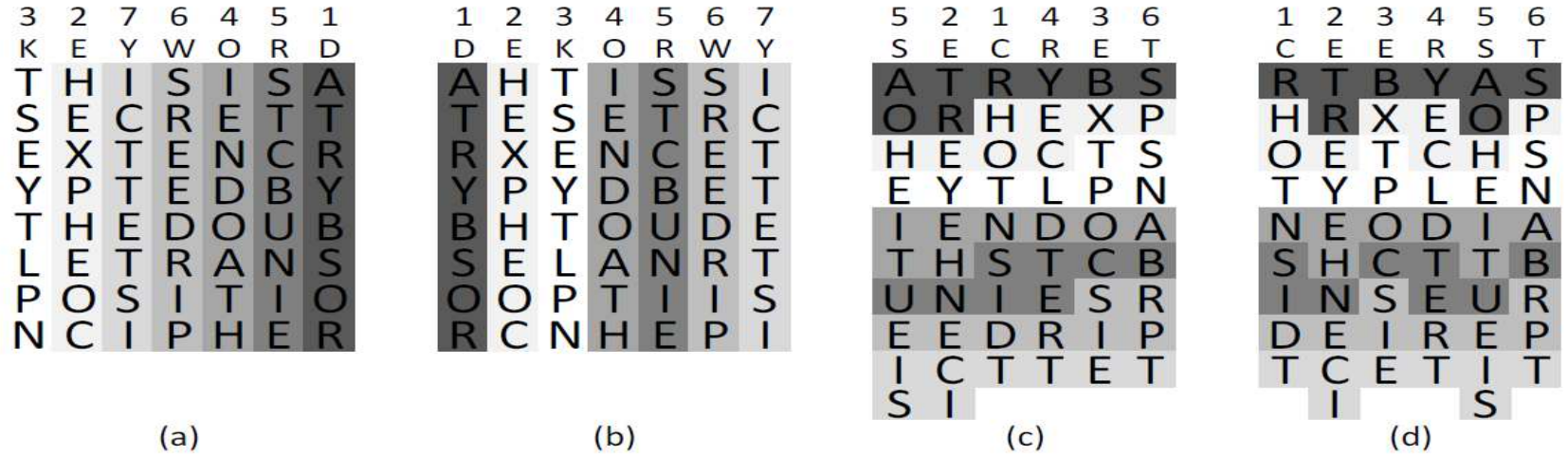
Problem 7: Hagelin M-209 - Short Messages (<500 letters)





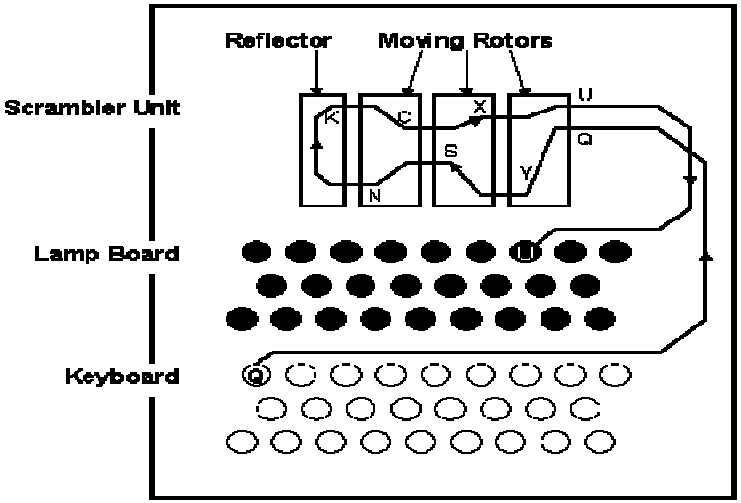
- **Possible key settings: $2^{169} = 10^{50}$**
- **Best published method: 750-1000 letters**

Problem 8: Double Transposition - Random Long Keys (>25)



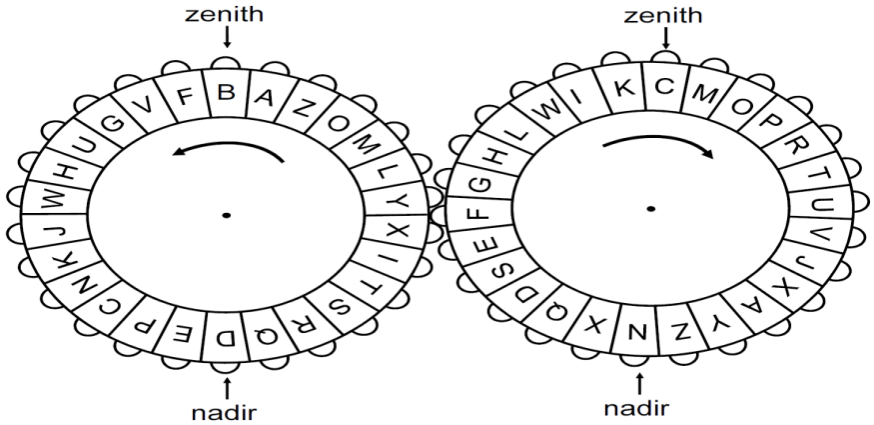
- **Possible key settings: $2^{162} = 10^{48}$**
- **Best published method: Lengths of keys = ~20**
  - Efficient dictionary attack for non-random keys

Problem 9: Enigma - Short Message (<70)



- **Possible key settings: $2^{76} = 10^{23}$**
- **Best published method: Hillclimbing, > 70-80**
  - Known-plaintext attack (Turing Bombe)

Problem 10: Chaocipher - Single Message



- **Possible key settings: $2^{173} = 10^{23}$**
- **Best published method: None for single message**
  - Only methods for known-plaintext, or in-depth messages

Additional Open Problems

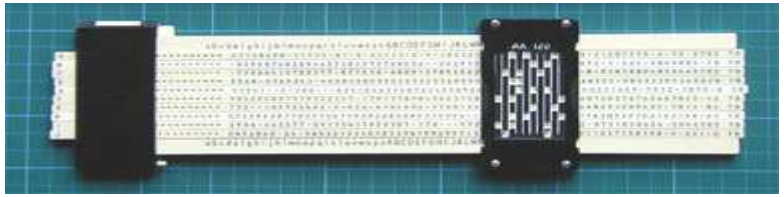
11. GRANIT

- DDR/STASI (1950-60s)
- Subs. + Double Transposition

	0	1	2	3	4	5	6	7	8	9
	K	A	T	N	I	S	B	C		
8	D	E	F	G	H	L	M	O	P	Q
9	R	U	V	W	X	Y	Z	zs	.	,

12. Reihenshieber

- West Germany (1950-60s)
- Sliding strips + pattern



13. Rasterschlüssel

- Germany WWII
- Subs. + Transposition

Rasterschlüssel 44 — **25 August 1944**

cd	ad	eb	ca	ab	ee	cb	bd	dd	dc	aa	bc	ee	ec	be	db	cc	ac	ea	ba	ae	da	ed	bb	de	
2	13	24	6	18	3	14	12	5	22	8	7	15	11	21	1	17	20	25	16	4	9	19	10	23	
■	o	■	■	r	r	■	■	e	■	■	w	■	■	q	f	n	■	■	■	t	■	c	■	■	ca
k	o	■	r	■	■	r	■	e	■	■	■	e	■	e	■	v	■	e	■	■	■	r	■	■	bd
■	■	■	m	■	u	■	t	l	■	i	■	■	q	■	■	u	■	m	■	e	■	■	■	i	cc
n	s	■	a	■	q	■	t	■	■	■	u	■	■	h	■	r	■	■	b	■	e	■	■	■	ac

UNIKASSEL VERSITÄT

Angewandte Informations Sicherheit

Thank You

May 5, 2016
George Lasry
University of Kassel, Germany
george.lasry@ais.uni-kassel.de