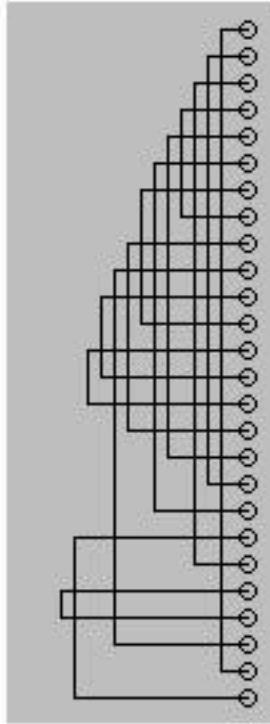


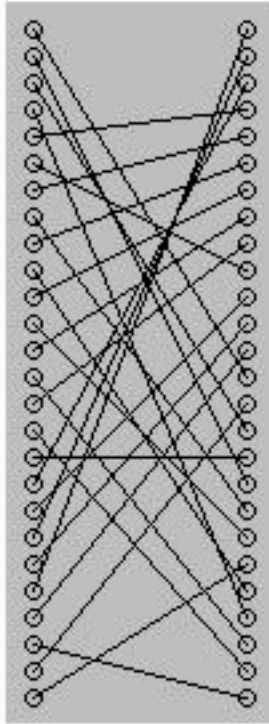
Breaking the Enigma

Yan Huang

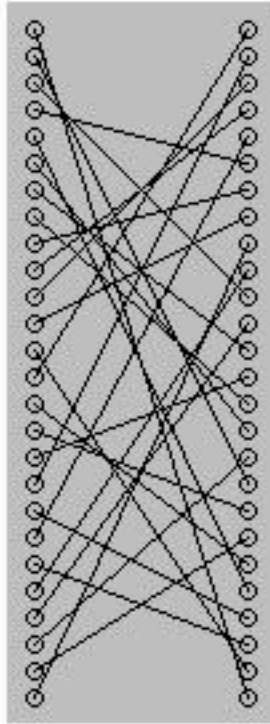




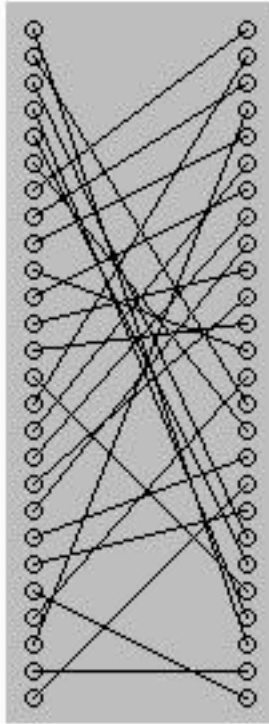
Reflector



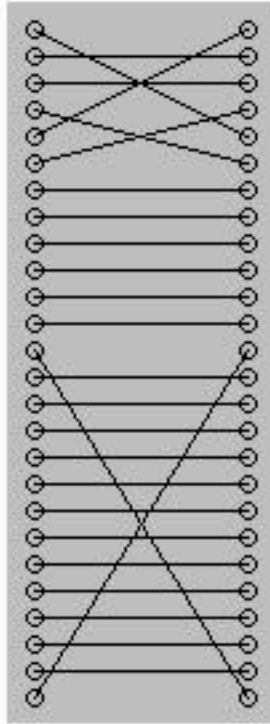
Wheel 1



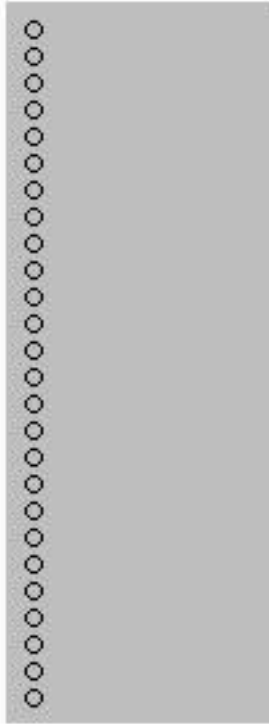
Wheel 2



Wheel 3



Plugboard







Keyboard &
Lightboard

Configurable Parts

- Rotors
- Reflectors
- Plugs
- Initial rotor position

What makes Enigma Hard to Break?

- Rotors 
- Reflectors 
- Plugs 
- Initial rotor position 

Kerckhoff's Principle

Open Design

Base security on of *the secrecy of randomness*, rather than the obscurity of the mechanisms.



Threat Modeling

- Ciphertext-only attack
- Known-plaintext attack
- Chosen-plaintext attack
- Chosen-ciphertext attack

Possible number of Keys

Initial rotor settings

$$26^3$$

Possible number of choices of wheels

$$C_5^3 = \binom{5}{3}$$

Plugboard settings (assume 6 plugs)

$$\frac{P(26, 12)}{26^6 \cdot 6!}$$

Ciphertext-Only Attack

- If the only missing information is the initial rotor setting
- Given a ciphertext c
 1. Guess a key k
 2. Decrypt c with k to obtain m
 3. If m makes sense, output (k, m)

“Making Sense”?

- Human scanning
 - expensive
- Statistical tests
 - Chi-Square
 - Index of Coincidence

Key Schedule

Geheim!

Sonder-Maschinenschlüssel BGS

08 *

Nicht ins Flugzeug mitnehmen!

Datum	Walzenlage	Ringstellung	Steckerverbindungen														Kenngruppen																		
31.	I II V	10 14 02	BF	SD	AY	HG	OU	QC	WI	RL	XP	ZK	yqv	vuc	xxo	gvf	DI	ZL	RX	UH	QK	PC	VY	GA	SO	EM	mgy	vts	gvt	csx					
30.	V IV I	04 25 01	ZM	BQ	TP	YX	FK	AR	WH	SO	NJ	DG	aky	vdv	oyo	tzt	NE	MT	RL	OY	HV	IU	GK	FW	PZ	XC	nfh	vcc	tur	wnb					
29.	III V II	13 11 06	BF	GR	SZ	OM	WQ	TY	HE	JU	XN	KD	bec	jmv	vtp	xdb	GS	VD	CQ	LE	HI	BO	JP	UZ	FT	RN	wvu	yem	buz	rjk					
28.	I III II	09 16 12	KA	ZH	QP	GR	MF	LJ	OT	EN	BD	YW	ktv	muq	cqm	cpm	PI	KM	JB	YU	QS	OV	ZA	GW	CH	XF	zed	iwo	urp	glg					
27.	III II I	06 03 15	SX	TD	QP	HU	FB	YN	CO	IK	WE	GZ	epm	mgz	vqg	vsm	GP	XH	IW	BO	NU	MD	SA	ZK	QR	LT	aam	mvj	jqj	wqm					
26.	I III V	19 26 08	XC	AQ	OT	UZ	HD	RG	KM	BL	NS	JW	ltl	blu	frk	xrh	PO	TV	QC	ZS	EX	WR	BJ	DK	FU	LA	non	lic	oxr	usr					
25.	II I IV	05 01 16	HA	GM	DI	VK	JP	YU	EF	TB	ZL	XQ	ecd	ciq	uvr	ppt	18.	IV V I	23 09 20	XF	PZ	SQ	GR	AJ	UO	CN	BV	TM	KI	fjh	zts	uqa	cft		
24.	III II IV	22 02 06	UT	ZC	YN	BE	PK	JX	RS	GF	IA	QH	oub	eci	pyf	rqi	17.	III II V	21 24 15	IN	YJ	SD	UV	GF	BH	TK	QE	AR	OP	kex	paw	flw	onw		
23.	IV III II	08 11 07	TM	IJ	VK	OY	NX	PR	WL	GA	BU	SF	sdr	pbu	byv	khh	16.	IV III V	07 01 13	WT	RE	PC	FY	JA	VD	OI	HK	NX	ZS	mhz	lff	lnq	giy		
22.	I V II	13 02 26	AN	IV	LH	YP	WM	TR	XU	FO	ZB	ED	rqh	ucm	ldi	ods	15.	I IV II	15 04 25	HR	NC	IU	DM	TW	GV	FB	ZL	EQ	OX	asy	xza	uvc	fmr		
21.	IV I V	17 24 03	NX	EC	RV	GP	SU	DK	IT	FY	BL	AZ	gyd	iuq	ocb	vef	14.	III II IV	10 23 21	FN	TA	YJ	SO	EG	PC	VD	KI	XH	WZ	pyz	ace	pru	üyc		
20.	IV I III	15 22 12	VK	DW	LH	RF	JS	CX	PT	YB	ZG	MU	nyh	fbd	ohs	jrp	13.	V I II	14 04 12	PV	XS	ZU	EQ	BW	CH	AO	RL	JN	TD	tck	rts	nro	mkl		
19.	V I III	13 24 21	TS	IK	AV	QP	HW	FM	DX	NG	CY	UE	mhw	lwb	mdm	ybe	12.	II V I	07 19 02	KZ	FI	WY	MP	DS	HR	CJ	XE	QV	NT	uwu	vdk	lrh	mgd		
18.	IV V I	23 09 20	VW	LT	PB	FO	ZK	GS	RI	QJ	HM	XE	suw	tsv	nfp	yjc	11.	I V IV	13 15 11	QS	YA	XW	KR	MP	HT	DU	OV	CL	FZ	uby	usi	mhh	mwb		
17.	III II V	21 24 15	FW	DL	NX	BV	KM	RZ	HY	IQ	EC	JU	tns	von	grw	axl	10.	V II I	09 20 19	DW	UO	PY	GR	FS	EQ	KT	CL	AI	ZB	smz	lbl	bkc	sym		
16.	IV III V	07 01 13	ZN	OM	CR	UI	KP	WQ	SE	JV	LX	TF	ghr	vqv	cya	ayl	9.	I IV V	14 10 25																
15.	I IV II	15 04 25																8.	IV V I	22 04 16															
14.	III II IV	10 23 21																7.	V I IV	18 11 25															
13.	V I II	14 04 12																6.	IV I III	02 17 20															
12.	II V I	07 19 02																5.	I V IV	26 09 14															
11.	I V IV	13 15 11																4.	IV III V	07 01 12															
10.	V II I	09 20 19																3.	I II V	05 16 03															
9.	I IV V	14 10 25																2.	III I II	12 22 17															
8.	IV V I	22 04 16																1.	I III II	04 18 06															
7.	V I IV	18 11 25																																	
6.	IV I III	02 17 20																																	
5.	I V IV	26 09 14																																	
4.	IV III V	07 01 12																																	
3.	I II V	05 16 03																																	
2.	III I II	12 22 17																																	
1.	I III II	04 18 06																																	

DECLASSIFIED
 Authority N12 005007
 By DE NARA Date 11/4/04

Enigma Use Procedure

- Setup the machine according to the Key Schedule
- Pick a 3-letter *indicator* key “at random” for this message only
 - e.g., “UBR” (or 21-2-18 if wheels are printed with numbers)
- Transmit the indicator key using the key picked from the key schedule. Repeat it to ensure it was received correctly.
- Setup the machine with the indicator key (use “UBR”)
- Transmit the rest of the message

Making Sense More Easily

- Once intercept an encryption
“hkyiagdvcgcvuiefdujtiqbfcqgfxpgdauooerbkesdnxgpptpb”
- when decrypted, it has to start with
“XYZXYZ*****” for some X, Y, Z

Missing Plugboard Setting

- Known-Plaintext Attack:

It is known that the word "EISENHOWER" appeared in an intercepted encrypted message "TGHISLDCINTH"

- Assume only one plug is used: 'E' -> 'T'

Missing Plugboard Setting

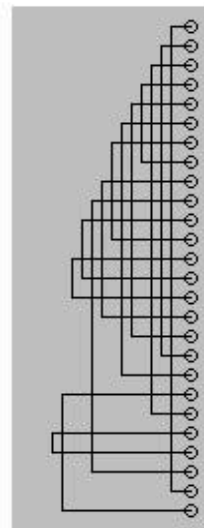
D Z E G F O H B ...
E I S E N H O W E R

- Known-Plaintext Attack

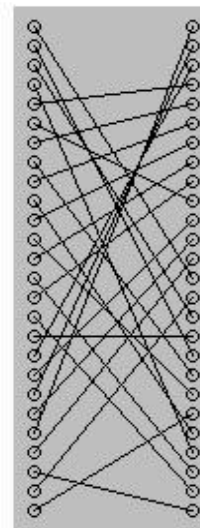
DIEGFOHBLSTSIJLABCEZPTNMIERYABCUXUQW

EISENHOWER

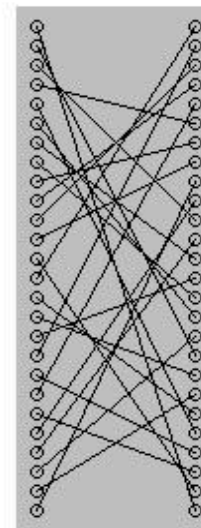
A Character never encrypts to itself!



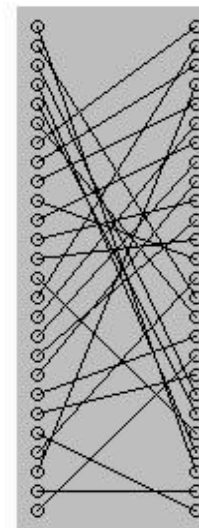
Reflector



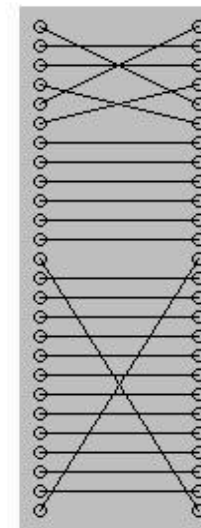
Wheel 1



Wheel 2



Wheel 3



Plugboard



Keyboard &
Lightboard

Missing Plugboard Setting

- Known-Plaintext Attack

DIEGFOHBLSTSIJLABCEZPTNMIERYABCUXUQW
EISENHOWER

A Character never
encrypts to itself!

Missing Plugboard Setting

- Known-Plaintext Attack

DIEGFOHBLSTSIJLABCEZPTNMIERYABCUXUQW

EISENHOWER

A Character never
encrypts to itself!

Missing Plugboard Setting

- Known-Plaintext Attack

DIEGFOHBLSTSIJLABCEZPTNMIERYABCUXUQW

EISENHOWER

A Character never
encrypts to itself!

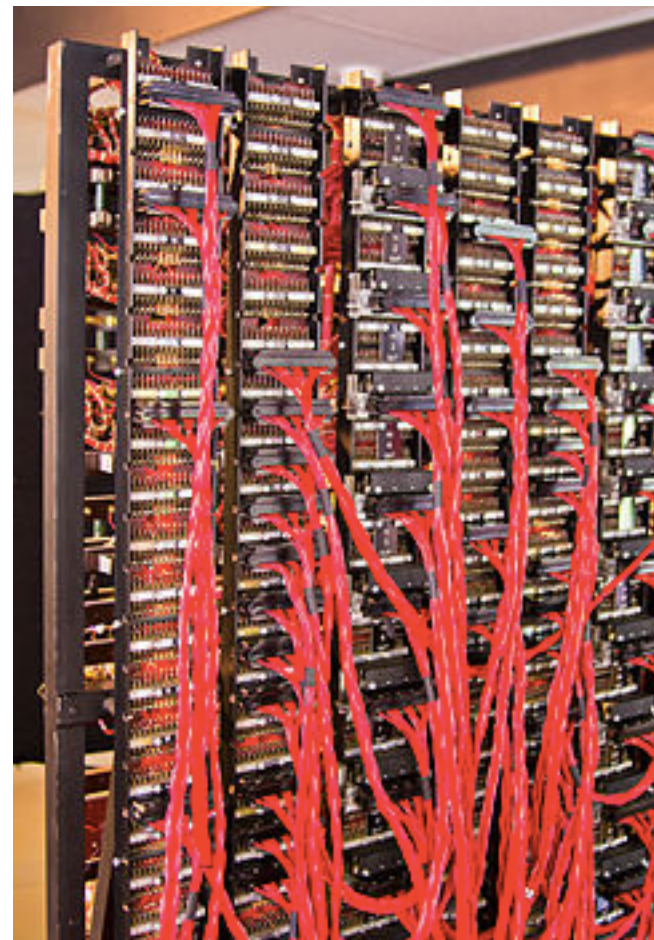
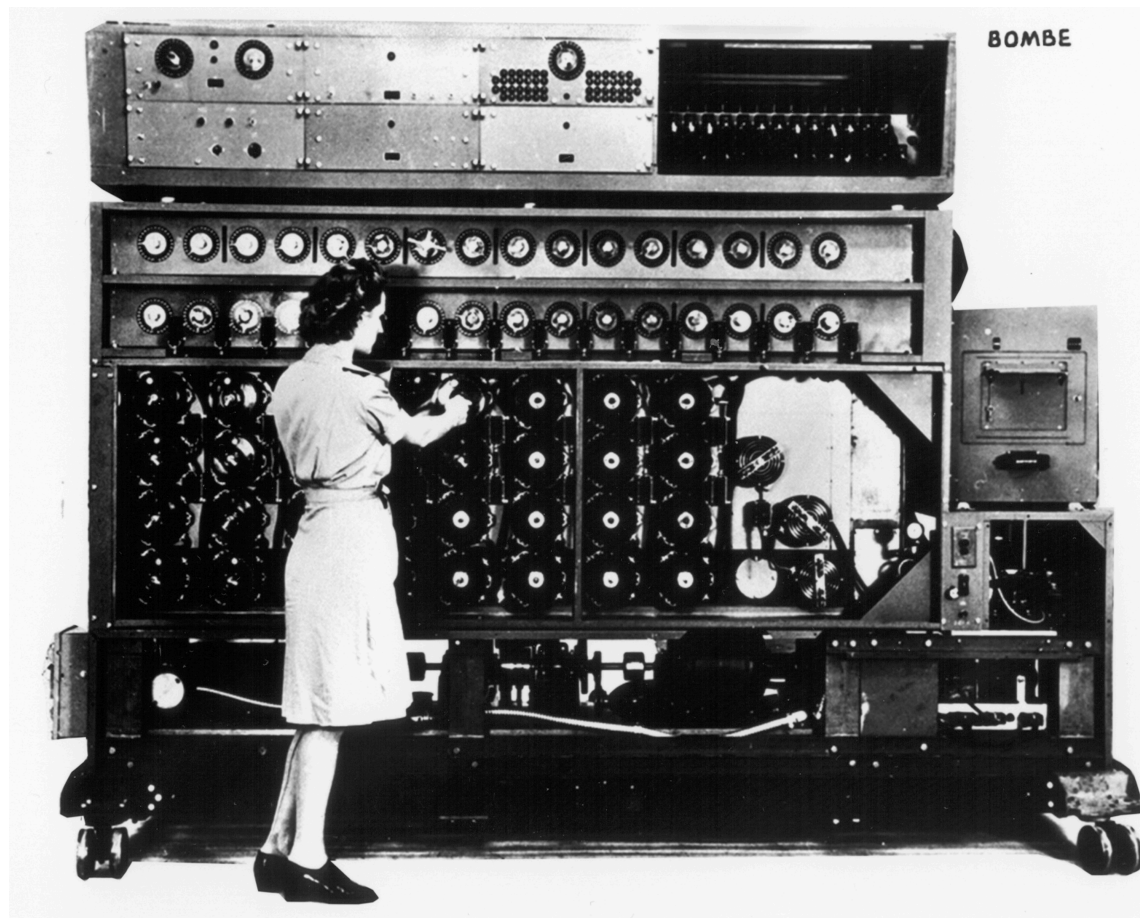
Possible fixes?

Reflector Wheel 1 Wheel 2 Wheel 3 Plugboard Keyboard &
Lightboard

More Vulnerabilities

- Operators choose poor message keys (e.g., “BER”, “LIN”, “HIT”, “LER”, “JJJ”, “QWE”)
- The mapping from message letters to ciphertext letters changes every step, but the change is independent of the message
 - Inspired modern ciphers to use *Modes of Operations* such as CBC (Cipher Blocks Chaining) mode.
- Modern substitutions of Enigma: AES, Salsa

The Turing Bombe



The Lorenz Cipher vs. The Colossus Computer

