آلن تورینگ، انیگما و تغییر مسیر جنگ جهانی دوم

دانشگاه ارومیه

دانشکده برق و کامپیوتر

بردیا طالبیان

پاییز ۱۴۰۲

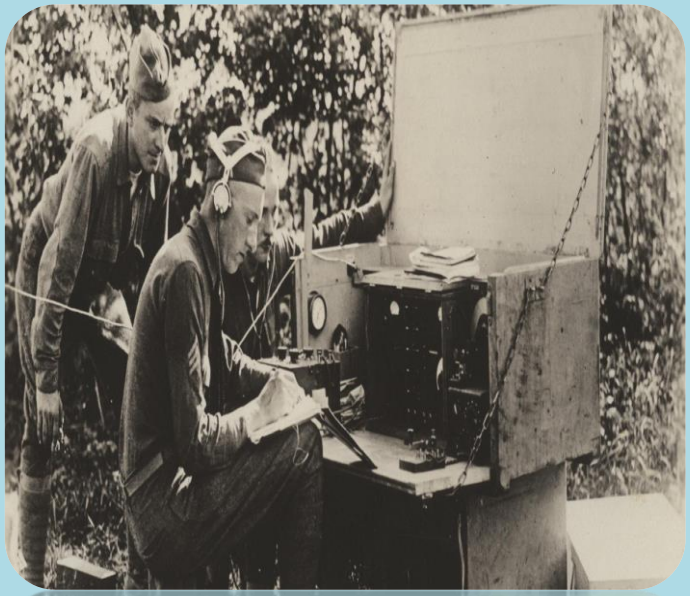
فهرست مطالب

مقدمه

- بررسی ریشه‌های دانش و فناوری در قرن بیست و یکم بدون در نظر گرفتن جنگ جهانی دوم، همچون دیدن قله یک کوه یخی بدون توجه به عمق آن است.
- در نیمه نخست قرن بیستم، جهان درگیر جنگ‌های متعددی گشت و علی‌رغم تمامی زشتی‌هایش سبب تحولات و پیشرفت‌های شگرفی در علوم و فناوری‌ها شد.
- مهمترین این تحولات، تولد کامپیوترها می‌باشد.

در این ارائه نگاهی خواهیم داشت بر نحوه کارکرد انیگما و شکسته شدن آن در جنگ جهانی دوم.

ارتباطات در میدان نبرد

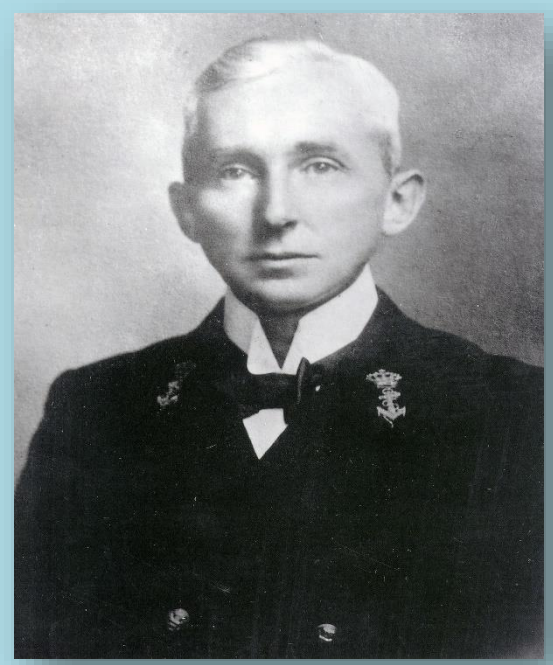


استفاده از رادیو در میدان نبرد توسط آمریکایی‌ها.

- انقلاب رادیو بی‌سیم در ارتباطات نظامی.
- اما توسط دشمن، پیام‌ها به راحتی شنود و خوانده می‌شدند.
- تکنولوژی رمزنگاری مربوط به صدها سال قبل می‌شد.
- تمامی رمزنگاری‌ها شکسته می‌شدند!
- اکنون، نیاز به ماشینی برای رمزنگاری بیش از همیشه احساس می‌شود...

جنگ جهانی اول، میدان را برای پیشرفت علم رمزنگاری هموار کرد.

اختراع روتور ماشین



تئو ون هنگل
(۱۹۳۹-۱۸۷۵)

۱۹۱۵: اختراع روتور ماشین توسط دو افسر نیروی دریایی هلند، ون هنگل و اشپنگلر.

۱۹۱۷: شروع به اختراع ماشینی مشابه در سرتاسر دنیا!

- ادوارد هیبرن در آمریکا.
- آروید دام در سوئد.
- هوگو کوخ در هلند
- آرتور شربیوس در آلمان.

سیر تحول انیگما

انیگما، برگرفته از واژه‌ای یونانی(αίνιγμα/amanigma) به معنای معما است.

آرتور شربیوس
(۱۸۷۸-۱۹۲۹)

۱۹۱۸: ساخت و طراحی انیگما توسط آرتور شربیوس.

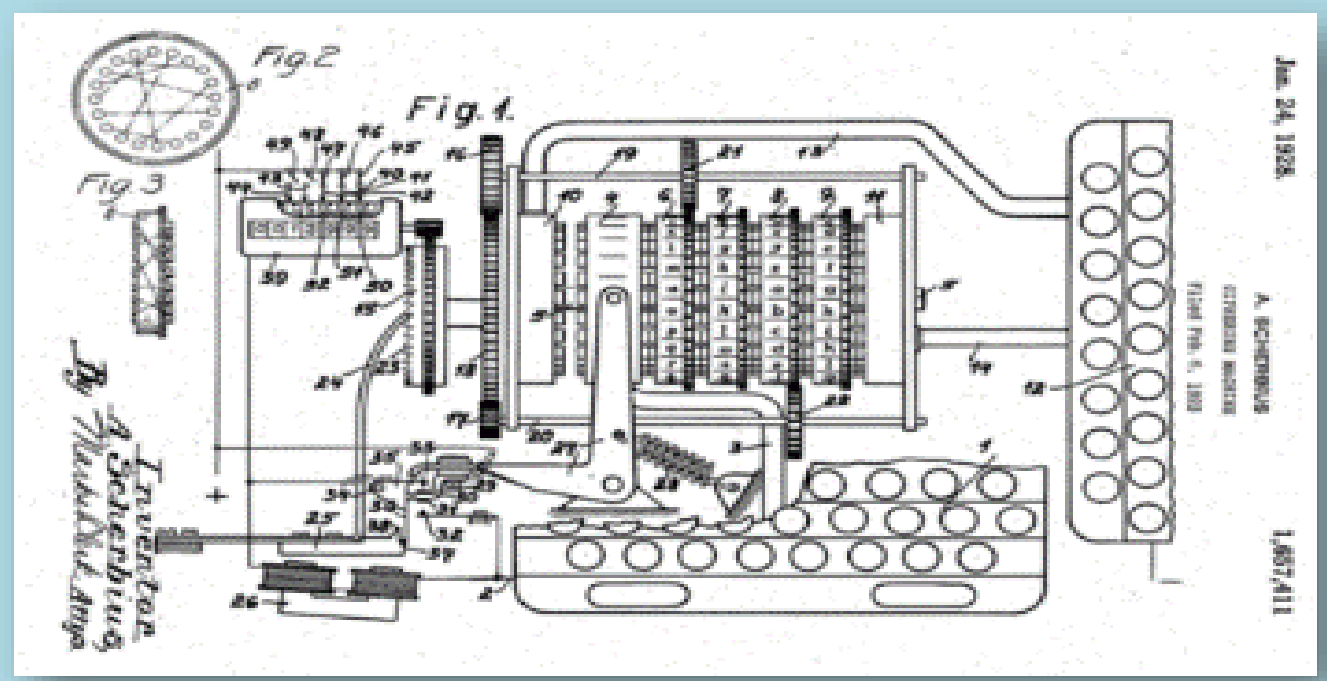
۱۹۲۳: توسعه ماشین و بهبود عملکرد آن.

۱۹۲۶: به کارگیری انیگما توسط نیروی دریایی آلمان.

۱۹۳۴-۴۵ : به کارگیری انیگما توسط تمام واحدهای نظامی آلمان.

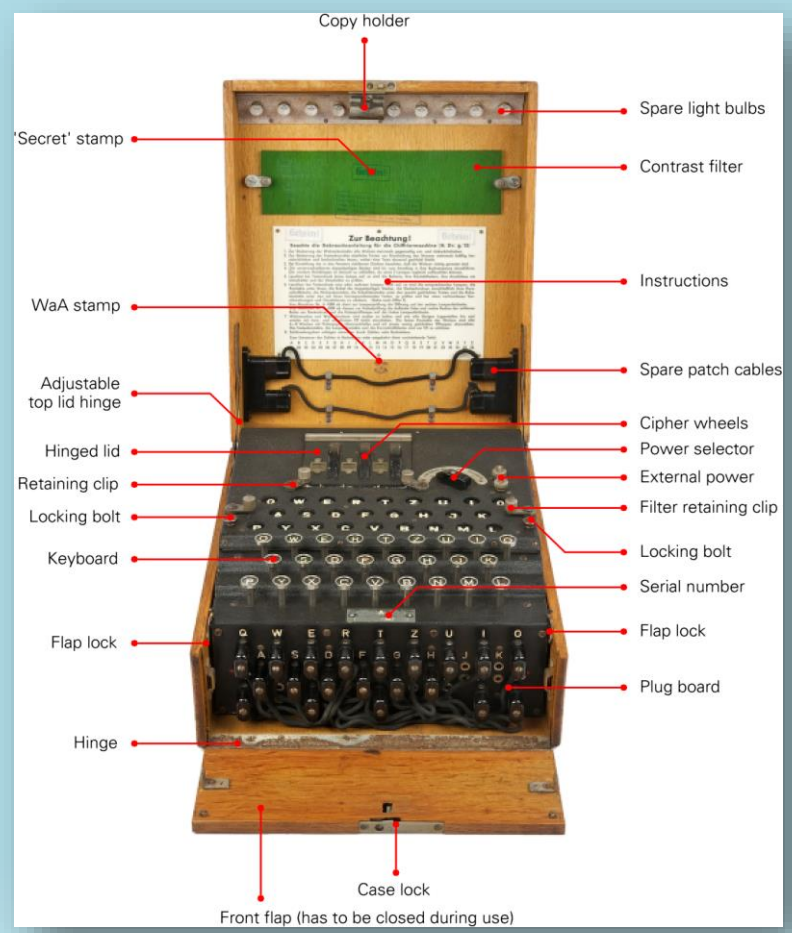
طرح اولیه‌ی انیگما

ثبت اختراع انیگما توسط شربیوس در سال ۱۹۲۸
U.S. Patent 1,657,411



انیگما یکی از قوی ترین رمزنگاری‌ها را در اختیار ارتش آلمان قرار داد و به گسترش ماشین جنگ نازی‌ها کمک کرد.

بررسی انیگما تایپ I



۱- سه روتر حاوی ۲۶ ورودی و پین در طرفین؛

۲- صفحه کلید و پنل لامپ به ترتیب استاندارد QWERTZ؛

۳- دارای یک پلاگین پوشانده شده توسط دریچه چوبی.

✓ پیچیده کردن هرچه بیشتر پیام.

دو ویژگی انیگما:

۱- عدم رمز شدن یک حرف به خودش.

۲- رمز شدن حروف یکسان به حروف مجزا.

اجزای انیگما

تنظیم حالت اولیه

پلاگ بورد

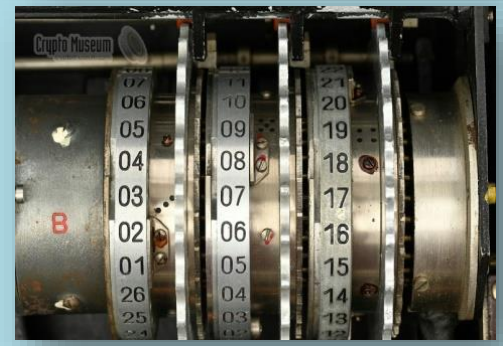
انکریپت یک حرف

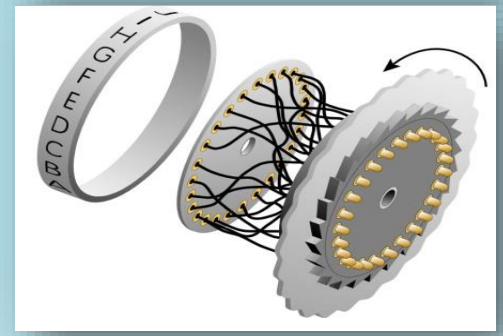
کیبورد و پنل لامپ

پیچیدگی پلاگبورد

تعداد کابل‌های پلاگبورد	گروه‌بندی حروف انتخاب شده (۲)	اتصالات برای هر مجموعه از حروف متصل (۳)	تمام حالات ممکن
	26! / ((2p!) X (26-2p)!)	(2p-1) X (2p-3) X (2p-5) X...X 1	(ستون 3) X (ستون 2)
0	1	1	1
1	325	1	325
2	14,950	3	44,850
3	230,230	15	3,453,450
4	1,562,275	105	164,038,875
5	5,311,735	945	5,019,589,575
6	9,657,700	10,395	100,391,791,500
7	9,657,700	135,135	1,305,093,289,500
8	5,311,735	2,027,025	10,767,019,638,375
9	1,562,275	34,459,425	53,835,098,191,875
10	**230,230**	**654,729,075**	**150,738,274,937,250**
11	14,950	13,749,310,575	205,552,193,096,250
12	325	316,234,143,225	102,776,096,548,125
13	1	7,905,853,580,625	7,905,853,580,625
کل حالات			532,985,208,200,576

نگاهی به روترهای انیگما





- ۲۶ ورودی برای هر روتر (نمایانگر حروف A تا Z).
- پل ارتباط صفحه کلید و لامپ‌ها.
- سیم‌کشی داخلی برای هر روتر و مابین هر روتر.
- چرخیدن یک پله‌ای سمت راست ترین روتر با فشردن کلید.
- چرخیدن روتر های بعدی پس از چرخش کامل روتر ماقبل.
- نتیجه: تولید حرف جدید در هر بار فشردن یک کلید.

انیگمای دارای ۳ روتر
ورماخت

انیگمای دارای ۴ روتر
کریگزمارین

ارسال پیام

ارسال پیام با انیگما شامل دو تنظیم است:

۱- کلید روزانه.

۲- کلید پیام.

تنظیم کلید روزانه شامل چندین مرحله می‌باشد:

۱- شیفت UKW به کنارین برای خارج کردن روترها.

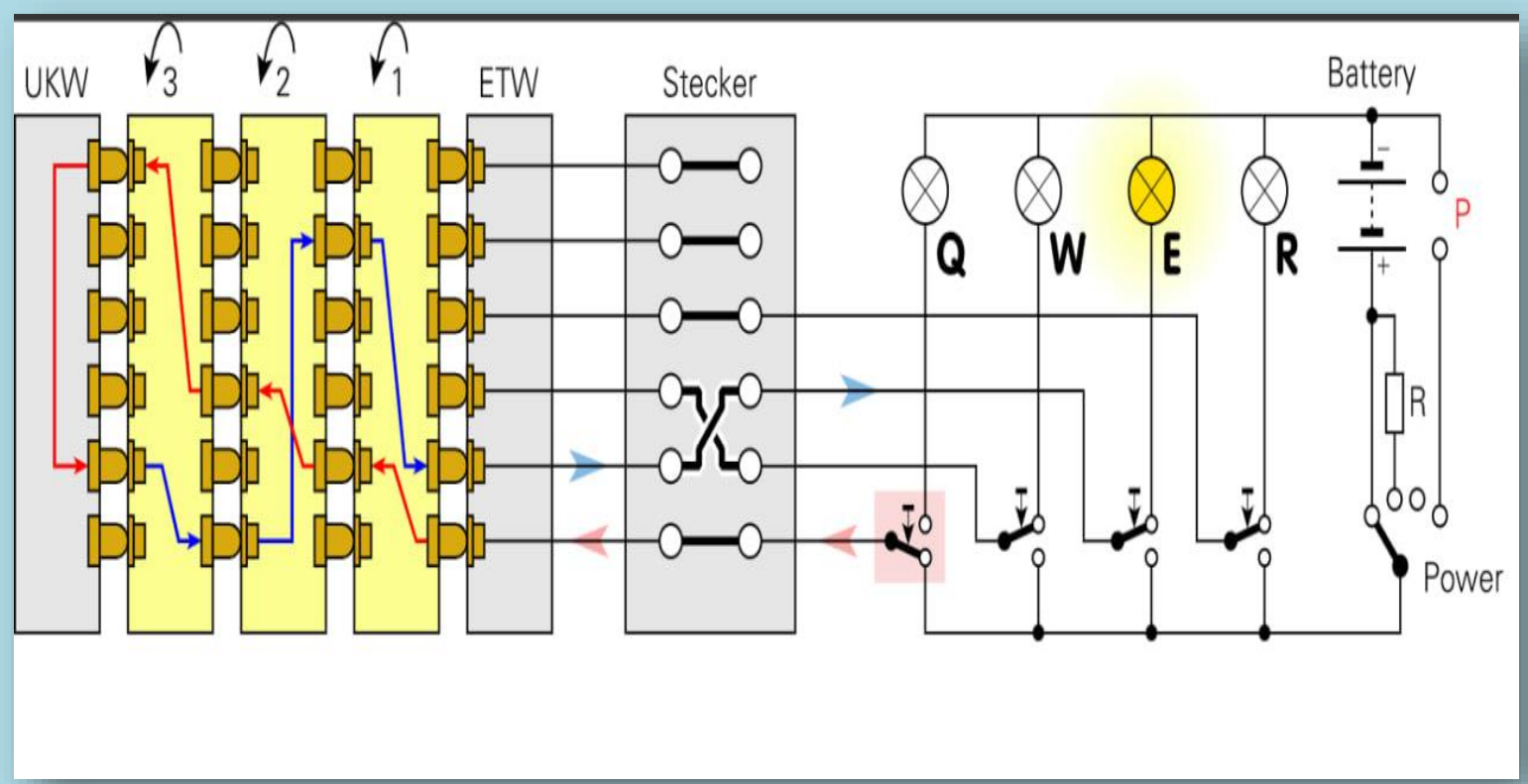
۲- انتخاب روترها و تنظیمشان.

۳- پیکر بندی پلاگین طبق کتابچه کد.

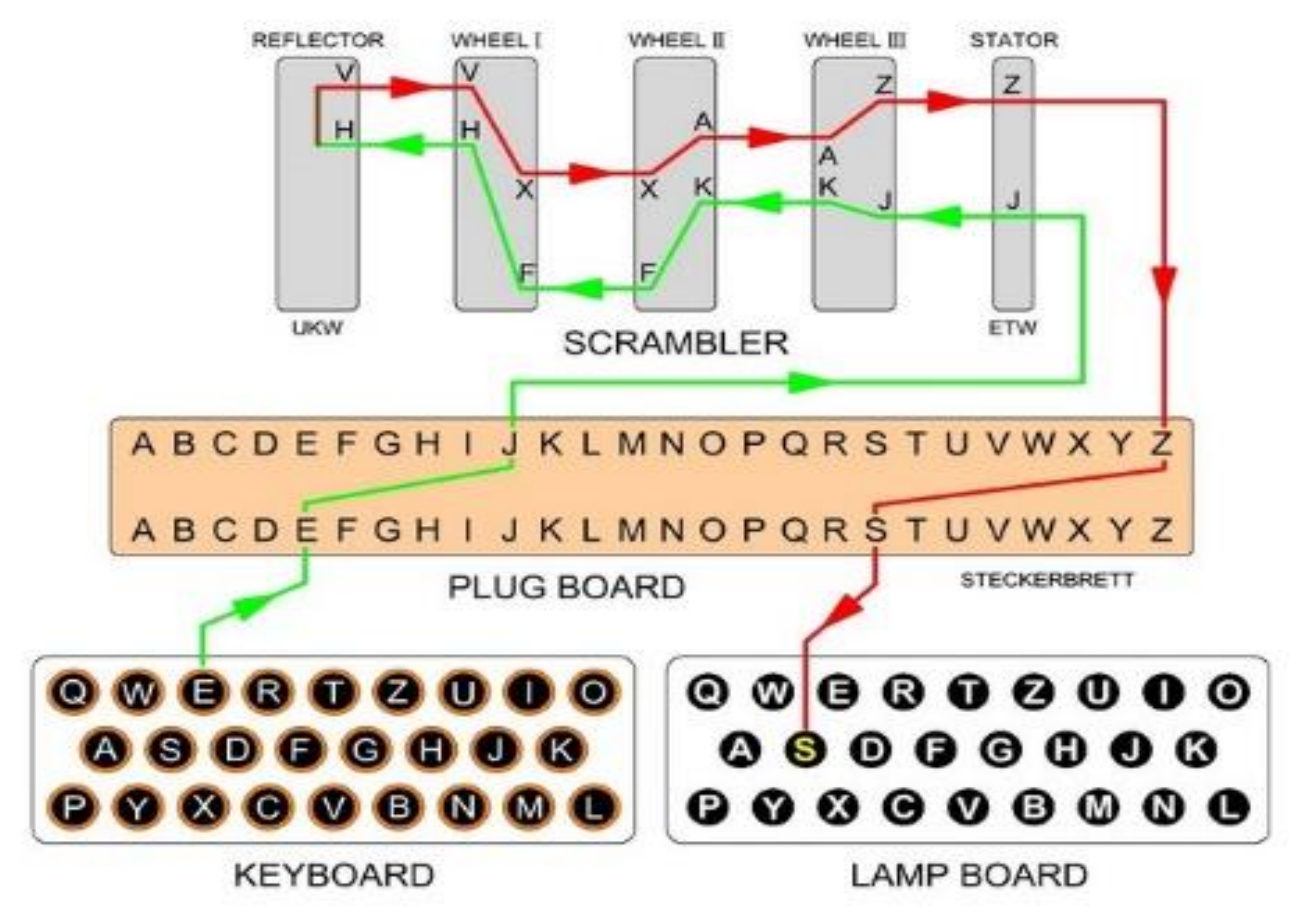
۴- انتخاب کلید سه حرفی منحصر به فرد.

۵- ارسال پیام رمزنگاری شده با کد مورس.

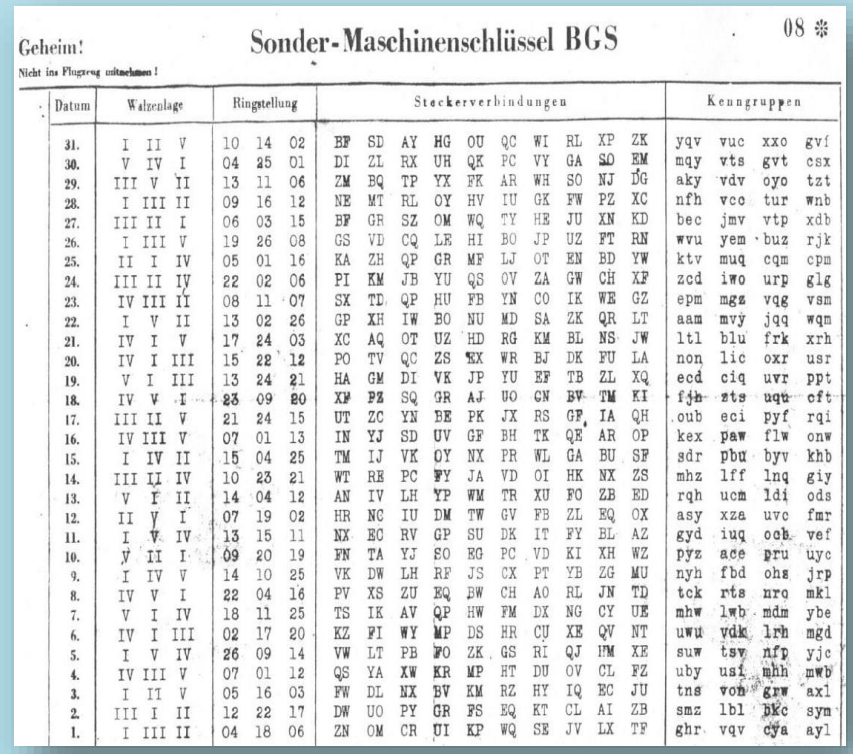
مدار ساده انیگما I



مسیر رمز شدن حروف



دریافت پیام



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

این تنظیمات با برگه‌ای به واحدهای مربوطه ارسال می‌گشت.

برای ارسال کننده و دریافت کننده لازم است که جزئیات زیر را هماهنگ کنند:

۱- از کدام روتورها و به چه ترتیبی استفاده شود.

۲- موقعیت پین‌های هر روتور.

۳- موقعیت شروع روتور در دستگاه.

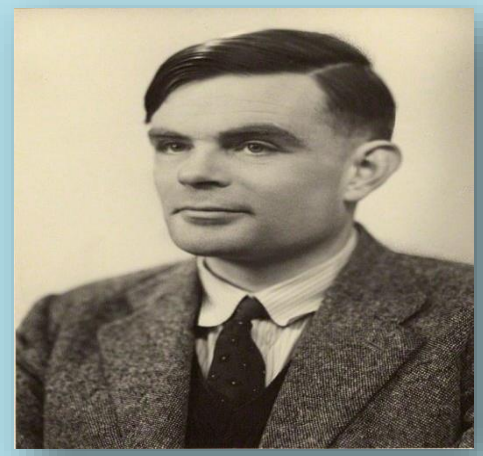
۴- از کدام بازتابنده استفاده شود.

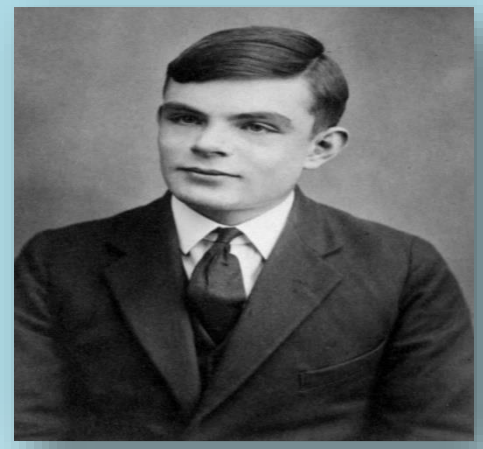
۵- تنظیمات پلاگبورد.

شکستن پیام

تعداد حالات ممکن برای شکستن انیگما برابر با عدد باورنکردنی ۱۵۸،۹۶۲،۵۵۵،۲۱۷،۸۲۶،۳۶۰،۰۰۰ بود.

پس...غیرممکن چگونه ممکن گشت؟





"هدف حل رمز به خودی خود نیست بلکه، کاهش تعداد حالات به عددی قابل مدیریت است که روش‌های دستی قابلیت حل آن را داشته باشند."

فهرست مطالب

خطر زیردریایی‌ها

- غرق نزدیک به ۳۰۰۰ کشتی متحدین توسط U-boatها.
- آلمان انتظار تسلیم بریتانیا را داشت.

نقاشی متعلق به سال ۱۹۴۱ توسط آدولف براک.

تنها چیزی که در دوران جنگ من را واقعا وحشت زده کرد، خطر زیردریایی‌ها بوده است.

ضعف‌های انیگما

فیلدمارشال گودریان درحال بازدید
از واحدهای رمزنگاری ورماخت

۱- ضعف طراحی و سهل‌انگاری اپراتور در انتخاب کلید رمز (QWE,ASDو...)

۲- لو رفتن ماشین انیگما و دفترچه‌های کد.

۳- کشف آن که هیچ حرفی در پروسه رمز شدن به خودش تبدیل نمی‌شود.

۴- اعتماد به نفس کاذب آلمانی‌ها.

شروع به شکستن کد

ماریان ریفسکی
(۱۹۰۵-۱۹۸۰)

۱۹۳۲: فروخته شدن کلیدهای انیگما توسط جاسوس آلمانی به فرانسه.

۱۹۳۳: ساخت ماشین بمبا توسط ریفسکی برای شکستن کلید روزانه.

۱۹۳۸: با پیچیده شدن انیگما لهستان از بریتانیا درخواست کمک کرد.

۱۹۳۹: شروع به کار آلن تورینگ در بلچلی پارک.

وظیفه تورینگ و ریاضی‌دان‌های دیگر در این مرکز شکستن رمز انیگما بود.

ماشین بمب – سرآغاز کامپیوترها

- ماشینی الکترومکانیکی دارای ۳۶ انیگما.
- ساخته شده توسط گوردن ولچمن و آلن تورینگ در سال ۱۹۴۰.
- هدف شکستن کد انیگما.

❖ **اساس کار:**

1. تفکر نیمه هوشمند.
2. حذف حالات متناقض.
3. حدس احتمال وجود کلمات (Crib).

ماشین بمب ساخته شده توسط ارتش آمریکا

حمله CRIB

1.

Q	F	Z	W	R	W	I	V	T	Y	R	E	S	X	B	F	O	G	K	U	H	Q	B	A	I	S	E	Z
W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B	I	S	K	A	Y	A					

2.

Q	F	Z	W	R	W	I	V	T	Y	R	E	S	X	B	F	O	G	K	U	H	Q	B	A	I	S	E	Z
	W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B	I	S	K	A	Y	A				

3.

Q	F	Z	W	R	W	I	V	T	Y	R	E	S	X	B	F	O	G	K	U	H	Q	B	A	I	S	E	Z
		W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B	I	S	K	A	Y	A			

4.

Q	F	Z	W	R	W	I	V	T	Y	R	E	S	X	B	F	O	G	K	U	H	Q	B	A	I	S	E	Z
			W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B	I	S	K	A	Y	A		

5.

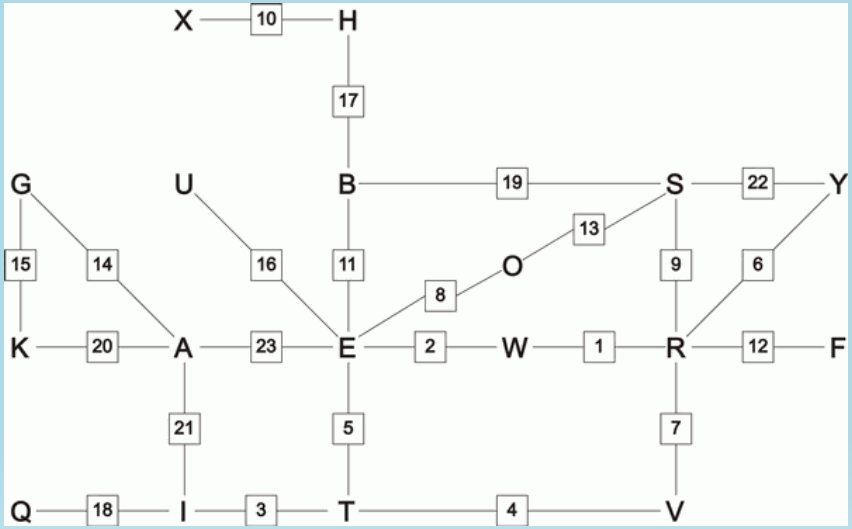
Q	F	Z	W	R	W	I	V	T	Y	R	E	S	X	B	F	O	G	K	U	H	Q	B	A	I	S	E	Z
				W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B	I	S	K	A	Y	A	

- کرایب استفاده شده در حمله نورماندی : WETTERVORHERSAGEBISKAYA
- بخشی از متن رمز شده : ...QFZWRWIVTYRESXBFOGKUHQBAISEZ...

گراف CRIB

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
R	W	I	V	T	Y	R	E	S	X	B	F	O	G	K	U	H	Q	B	A	I	S	E
W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B	I	S	K	A	Y	A

- مربع‌ها نشان‌دهنده درهم‌کننده‌ها است.
- اعداد در مربع‌ها، موقعیت‌های درهم‌کننده را نسبت به موقعیت درهم‌کننده‌ای که اولین جفت را تغییر داد، نشان می‌دهند.



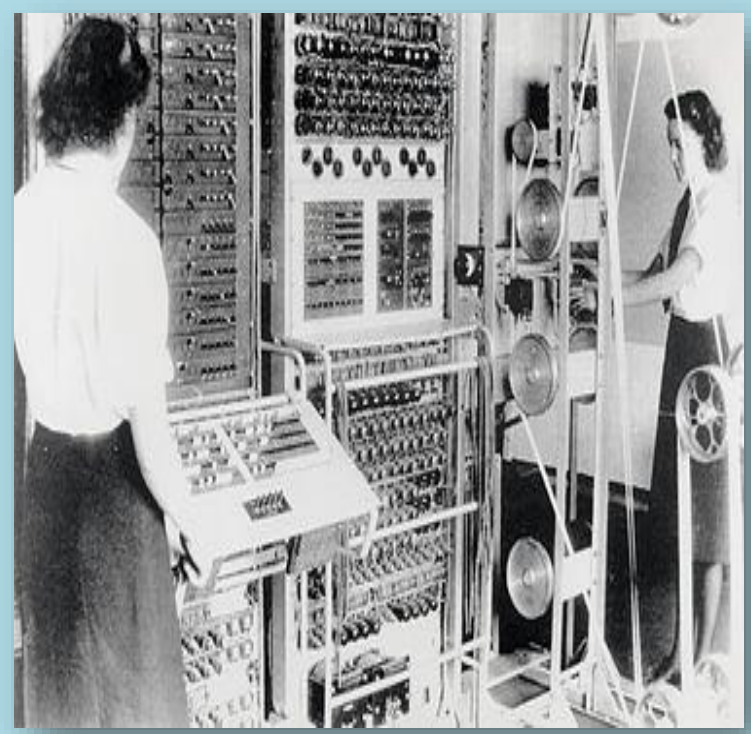
منوی CRIB

- ساخت منو توسط گراف.
- منوی بهتر، حذف تضاد بیشتر.
- چک کردن تنظیمات.
- توقف هنگام عدم وجود تناقض.
- گزارش احتمال وجود کلید کاندید به اپراتور.
- تجزیه و تحلیل کلید.
- اکثر توقف‌ها و کلیدها اشتباه بودند.
- بروزرسانی تنظیمات، ادامه شکستن کد.

نتیجه گیری کلی

❖ **تخمین زده می‌شود بخاطر کار تورینگ:**

- ✓ ۱۴ میلیون نفر نجات پیدا کرده،
- ✓ و جنگ ۲ سال زودتر تمام شده است.
- ✓ شکست متحدین در نبرد آتلانتیک.
- ✓ تبدیل موفقیت اولیه U-boatها به شکستی تمام عیار.
- ✓ غرق کشتی تدارکاتی ژنرال رومل در شمال آفریقا.
- ✓ ساخت اولین کامپیوتر قابل برنامه ریزی به نام کلوسوس.
- ✓ توسعه فناوری حوزه کامپیوتر و بوجود آمدن کامپیوترهای امروزی.
- ✓ پایه گذاری اساس هوش مصنوعی.



کامپیوتر کلوسوس

منابع

- [1] D. Kahn, *Seizing the Enigma*. Frontline Books, 2012.
- [2] “Enigma Cipher Machine,” *www.cryptomuseum.com*. https://www.cryptomuseum.com/crypto/enigma/index.htm
- [3] N. Cawthorne, *Alan Turing*. Arcturus Publishing, 2014.
- [4] S. Budiansky, *Battle of wits : the complete story of codebreaking in World War II*. New York: Free Press, 2000.
- [5] M. Smith, *Station X : the codebreakers of Bletchley Park*. London: Pan, 2004.
- [6] “The Enigma and the Bombe,” *www.ellsbury.com*. http://www.ellsbury.com/enigmabombe.htm
- [7] Wladyslaw Kozaczuk, *Enigma : how the German machine cipher was broken, and how it was read by the Allies in World War Two*. Frederick (Maryland): University Publications Of America, 1985.

سپاس از حسن توجه شما.