

Historical cryptography

WESTERN UNION TELEGRAM

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

GERMAN LEGATION
MEXICO CITY

130	13042	13401	8501	115	3528	416	17214	6491	11310
18147	18222	21560	10247	11518	23677	15605	3494	14036	
98092	5905	11311	10392	10371	0302	21290	5161	59695	
23571	17504	11269	18276	18101	0317	0228	17694	4473	
22284	22200	19452	21589	87893	5569	13918	8958	12137	
1333	4725	4458	5905	17165	13851	4458	17149	14471	6706
13850	12224	0929	14991	7382	15857	67893	14218	36477	
5870	17553	67893	5870	5454	16102	15217	22801	17138	
21601	17388	7446	23638	18222	6719	14331	15021	23845	
3166	23552	22096	21604	4797	9497	22466	20855	4377	
23410	18140	22280	5905	13347	20420	39689	13732	20657	
0929	5275	18507	52262	1340	22049	13339	11265	22295	
10439	14814	4178	6992	8784	7632	7357	0926	52282	11267
21100	21272	9346	9559	22464	15874	18502	18500	15857	
2188	5376	7381	98092	16127	13486	9350	9220	76036	14219
5144	2831	17920	11347	17142	11264				
10482	97556	3569	3670						

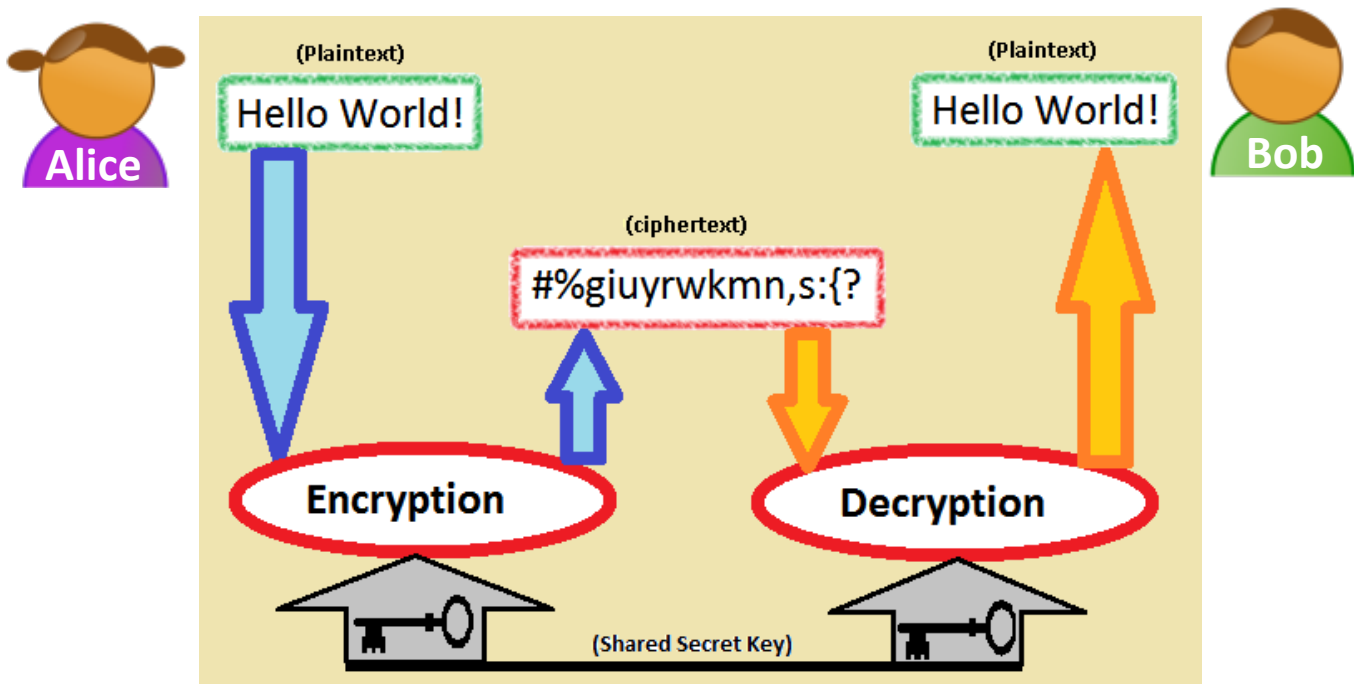
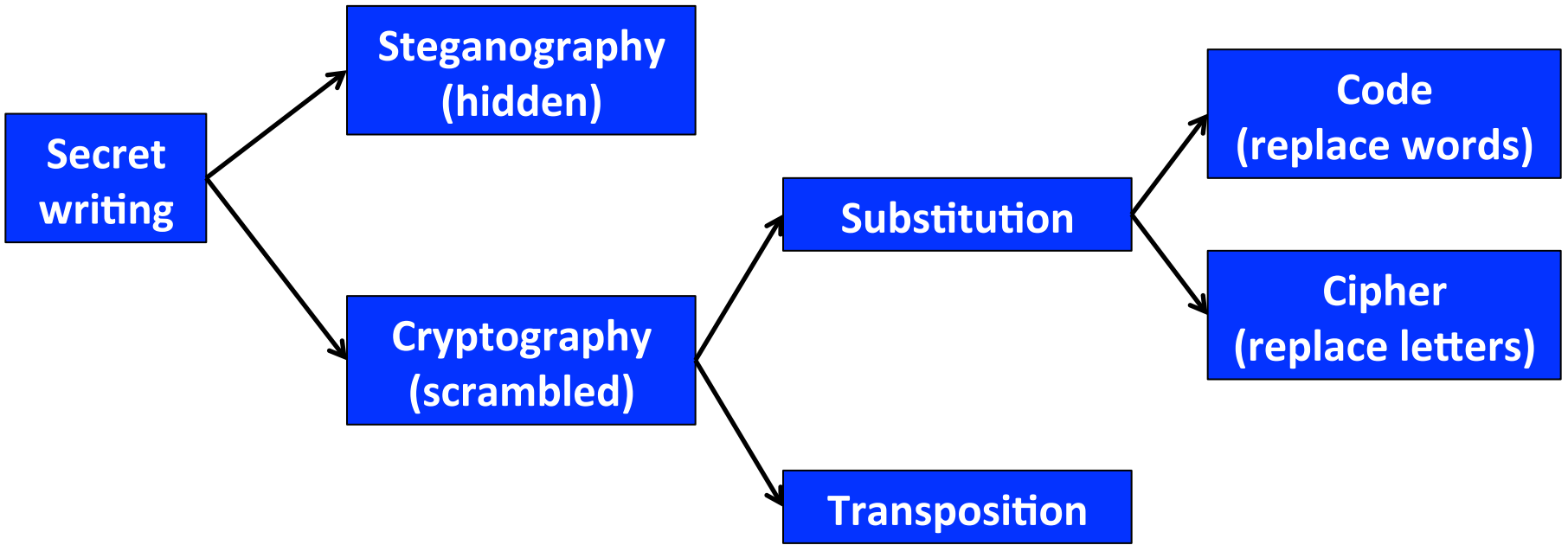
Charge German Embassy.



Handwritten text in a cursive script, likely a cipher or code, written on aged paper. The text is arranged in several lines and appears to be a message or document related to the historical cryptography context.

Overview

- Historical cryptography
 - Monoalphabetic substitution ciphers
 - Breaking them
 - Some improvements
 - The cipher of Mary Queen of Scots
 - Polyalphabetic substitution ciphers
 - Unbreakable encryption
 - WWI
 - Zimmerman telegram
 - WWII
 - Rise of the cipher machines
 - Engima



Monoalphabetic ciphers

- Monoalphabetic cipher
 - Use a **fixed substitution** over entire message
- Assigning substitutions
 - Option 1: **Caesar shift** cipher
 - Option 2: Completely **random**
 - 26! ways to assign \approx
400,000,000,000,000,000,000,000,000
 - But **hard to remember** a completely random assignment
 - Option 3: Based on **key phrase**
 - Shared secret: "ugly black swan"

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
U	G	L	Y	B	A	C	K	S	W	N	D	E	F	H	I	J	M	O	P	Q	R	T	V	X	Z

Breaking a monoalphabetic cipher



LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFEMVEWHKVSTYLXZIXLIKII
XPIJVSZEYPERRGERIMWQLMGLMXQERIWGSPRIHMXQEREKIETXMJTPRGEVEKEIT
REWHEXXLEXMZITWAWSQWXSWEEXTVEPMRXRSJGSTVRIEYVIEXCVMUIMWERMW
XMJMGC SMWXSJOMIQXLIVIQIVIXQSVSTWHKPEGARCSXRWIEVSWIIBXVIZMXFSJ
XLIKEGAEWHEPSWYSWIWIEVXLI SXLIVXLIRGEPIRQIVIIBGI IHMWYPFLEVHEWH
YPSRRFQMXLEPPXLI ECCIEVEWGISJKTVWMRLIHYS PHXLIQIMYLYXSJXLIMWRIGX
QEROIVFVI ZEVAEKPIEWHXEAMWYEPPXLMWYRMWXSGSWRMHIVEXMSWMGSTPHLEV
HPFKPEZINTCMXIVJSVLMRSCMWMWSVIRCI GXMWYMX



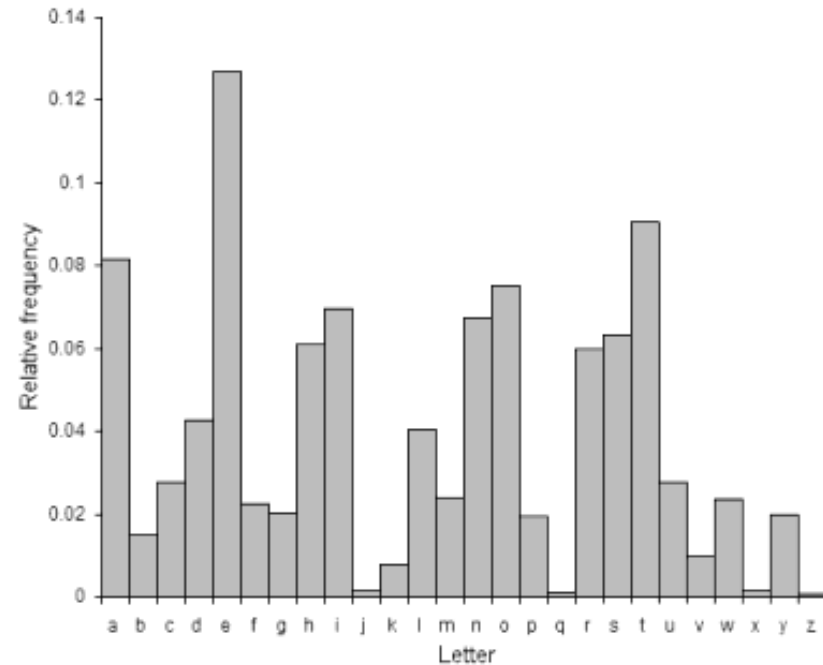
Eve counts up frequency of:
single letters
letter pairs (bigrams)
letter triples (trigrams)

...

Breaking a monoalphabetic cipher: step 1

LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFEMVEWHKVESTYLXZIXLIKII
 XPIJVSZEYPERRGERIMWQLMGLMXQERIWGPSRIHMXQEREKIETXMJTPRGEVEKEIT
 REWHEXXLEXMZITWAWSQWXSWEEXTVEPMRXRSJGSTVRIEYVIEXCVMUIMWERGMIW
 XMJMGC SMWXSJOMIQXLIVIQIVIXQSVSTWHKPEGARCSXRWIEVSWIIBXVIZMXFSJ
 XLIKEGAEWHEPSWYSWIWIEVXLI SXLIVXLIRGEPIRQIVIIBGIIHMYWPFLEVHEWH
 YPSRRFQMXLEPPXLIIECCIEVEWGISJKTVWMRLIHYS PHXLIQIMYLSJXLIMWRIGX
 QEROIVFVI ZEVAEKPIEWHXEAMWYEPPXLMWYRMWXS GSWRMHIVEXMSWMGSTPHLEV
 HPFKPEZINTCMXIVJSVLMRSCMWMMSWVIRCIGXMWYMX

ciphertext	plaintext	
I	e	most common letter
XL	th	most common bigram
XLI	the	most common trigram
E	a	second most common letter



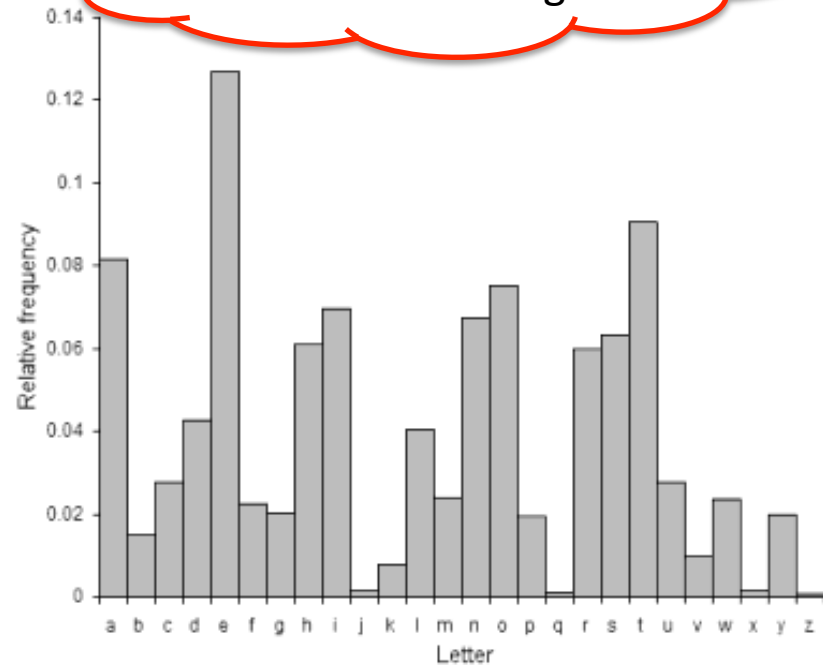
Letter distribution in English.

Breaking a monoalphabetic cipher: step 1

heVeTCSWPeYVaWHaVSRQmthaYVaOeaWHRtatePFaMVaWHKVSTYhtZetheKee
 tPeJVSZaYPaRRGaReMWQhMGhMtQaReWGPSReHMTQaRaKeaTtMJTPRGaVaKaET
 RaWHatthattmZeTWAWSQWtSwatTVaPMRtRSJGSTVReaYVeatCVMUeMWaRGMeW
 tMJMGCsMwTsJOMeQtheVeQeVetQSVSTWHKPaGARCStRWeaVSWeeBtVeZMtFSJ
 theKaGAaWHaPSWYSWeWeaVtheStheVtheRGaPeRQeVeeBGeeHMWYPFhaVHaWH
 YPSRRFQMthaPPtheaCCeaVaWGeSJKTvWMRheHYSPhtheQeMYhtSJtheMwReGt
 QaROeVFVeZaVAaKPeaWHtaAMWYaPPthMWYRMWtSGSWRMHeVaTMSWMGSTPHhaV
 HPFKPaZeNTCMteVJSVhMRSCMwMSWVerCeGtMWYMt

Eve now has a partially decoded message.

ciphertext	plaintext	
I	e	most common letter
XL	th	most common bigram
XLI	the	most common trigram
E	a	second most common letter



Letter distribution in English.

Breaking a monoalphabetic cipher: step 2

heVeTCSWPeYVaWHaVSRReQMthaYVaOea**WRtate**PFaMVaWHKVSTYhtZetheKee
 tPeJVSZaYPaRRGaReMWQhMGhMtQaReWGPSReHMTQaRaKeaTtMJTPRGaVaKaeT
 RaW**HatthattMZe**TWAWSQWtSWatTVaPMRtRSJGSTVReaYVeatCVMUeMWaRGMew
 tMJMGCSMWtSJOMeQtheVeQeVetQSVSTWHKPaGARCStRWeaVSWeeBtVeZMtFSJ
 theKaGAaWHaPSWYSWeWeaVtheStheVtheRGaPeRQeVeeBGeeHMWYPFhaVHaWH
 YPSRRFQMthaPPtheaCCeaVaWGeSJKTVMWRheHYSPhtheQeMYhtSJtheMWRReGt
 QaROeVFVeZaVAaKPeaWHtaAMWYaPPthMWYRMWtSGSWRMHeVaTMSWMGSTPHhaV
 HPFKPaZeNTCMteVJSVhMRSCMWSWVerCeGtMWYMt

ciphertext	plaintext	cipher fragment	plaintext guess
V	r	heVe	here
R	s	Rtate	state
M	i	atthattMZe	atthattime
Z	m	atthattMZe	atthattime



Eve can now use her knowledge of language to make further guesses...

Breaking a monoalphabetic cipher

hereTCSWPeYraWHarSseQithaYraOeaWHstatePFairaWHKrSTYhtmetheKee
tPeJrSmaYPassGaseiWQhiGhitQaseWGPSseHitQasaKeaTtiJTpsGaraKaeT
saWHatthattimeTWAWSQWtSWatTraPistsSJGSTRseaYreatCriUeiWasGiew
tiJiGCSiWtSJOieQthereQeretQsrSTWHKPaGAsCStsWearSweeBtremiTFSJ
theKaGAaWHaPSWYSWeWeartheStherthesGaPesQereeBGeeHiWYPFharHaWH
YPSssFQithaPPtheaCCearaWGeSJKTrWisheHYSPHtheQeiYhtSJtheiWseGt
QasOerFremarAaKPeaWHtaAiWYaPPthiWYsiWtSGSWsiHeratiSWiGSTPHhar
HPFKPameNTCiterJSrhisSCiWiSWresCeGtiWYit

and so on...



Decoded monoalphabetic cipher

hereuponlegrandarosewithagraveandstatelyairandbroughtmethebee
tlefromaglasscaseinwhichitwasencloseditwasabeautifulscarabaeu
sandatthattimeunknowntonaturalistsofcourseagreatprizeinascien
tificpointofviewthereweretworoundblackspotsnearoneextremityof
thebackandalongoneneartheotherthescaleswereexceedinglyhardand
glossywithalltheappearanceofburnishedgoldtheweightoftheinsect
wasveryremarkableandtakingallthingsintoconsiderationicouldhar
dlyblamejupiterforhisopinionrespectingit

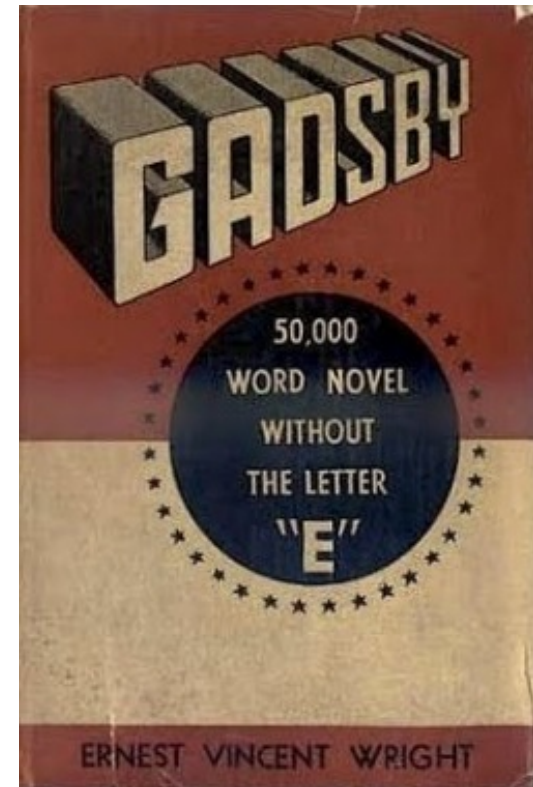
Hereupon Legrand arose, with a grave and stately air, and brought me the beetle from a glass case in which it was enclosed. It was a beautiful scarabaeus, and, at that time, unknown to naturalists—of course a great prize in a scientific point of view. There were two round black spots near one extremity of the back, and a long one near the other. The scales were exceedingly hard and glossy, with all the appearance of burnished gold. The weight of the insect was very remarkable, and, taking all things into consideration, I could hardly blame Jupiter for his opinion respecting it.

Or use some code from the Internet...

```
c:\Dropbox\mtech\websci\resources>simpsub2.exe
Name of sample ("learning") file: moby.txt
Name of cipher file: mono2.txt
Is the cipher formatted with spaces? (y/n): n
Reading sample file...
Analyzing sample file...
Reading cipher file...
Analyzing cipher file...
Initial closeness is 1.487429, PLEASE WAIT...
DONE! Func value=0.866612
Key is: abcdefghijklmnopqrstuvwxyz
       ekghijylmdapzws cnvrxt oqbfu
hereuponlegrandarosewithagraveandstatelyairandbroughtmeth
ebeetlefromaglasscaseinwhichitwasencloseditwasabeautifuls
carabaeusandatthattimeunknown tonaturalists ofcourseagreatp
rizeinascientificpointofviewthereweretworoundblackspotsne
aroneextremityofthebackandalongoneneartheotherthescaleswe
reexceedinglyhardandglossywithalltheappearanceofburnished
goldtheweightoftheinsectwasveryremarkableandtakingallthin
gsintoconsiderationicouldhardlyblamequpiterforhisopinionr
espectingit
```

Shoring up monoalphabetic ciphers

- Improved resistance to frequency analysis:
 - Insert nulls, symbols that represent nothing
 - e.g. cipher alphabet 1-99, 73 numbers represent nulls
 - Mespall thangs on pirpus
 - Screws up frequency, humans can correct
 - Use code words
 - Need to exchange large dictionary of codes
 - Capture of codebook destroys security
 - Homophonic substitution
 - Multiple cipher symbols per plaintext symbol
 - Nomenclature
 - Small list of words or syllables
 - Cipher alphabet with homophones



Homophonic substitution

- Improved resistance to frequency analysis:
 - Homophonic substitution
 - For each plaintext symbol, **set of cipher symbols**
 - Set **size proportional to frequency** in the language

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
09	48	13	01	14	10	06	23	32	15	04	26	22	18	00	38	94	29	11	17	08	34	60	28	21	02
12	81	41	03	16	31	25	39	70			37	27	58	05	95		35	19	20	61		89		52	
33		62	45	24			50	73			51		59	07			40	36	30	63					
47			79	44			56	83			84		66	54			42	76	43						
53				46			65	88					71	72			77	86	49						
67				55			68	93					91	90			80	96	69						
78				57										99					75						
92				64															85						
				74															97						
				82																					
				87																					
				98																					

Mary Queen of Scots

- **Babington Plot**

- Mary imprisoned for 18 years
- Gilbert Gifford double agent
 - "recruited" to communicate with Mary
- Detoured letters via Walsingham
- Anthony Babington and company
 - Rescue Mary
 - Assassinate Elizabeth
 - Wanted blessing of Mary



Mary Queen of Scots



Elizabeth I



Francis Walsingham

Mary's nomenclature

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92
93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115
116	117	118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138
139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161
162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184
185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230
231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253
254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276
277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299
300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322
323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345
346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368
369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391
392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414
415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437
438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460
461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483
484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506
507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523	524	525	526	527	528	529
530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546	547	548	549	550	551	552
553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571	572	573	574	575
576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597	598
599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621
622	623	624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644
645	646	647	648	649	650	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667
668	669	670	671	672	673	674	675	676	677	678	679	680	681	682	683	684	685	686	687	688	689	690
691	692	693	694	695	696	697	698	699	700	701	702	703	704	705	706	707	708	709	710	711	712	713
714	715	716	717	718	719	720	721	722	723	724	725	726	727	728	729	730	731	732	733	734	735	736
737	738	739	740	741	742	743	744	745	746	747	748	749	750	751	752	753	754	755	756	757	758	759
760	761	762	763	764	765	766	767	768	769	770	771	772	773	774	775	776	777	778	779	780	781	782
783	784	785	786	787	788	789	790	791	792	793	794	795	796	797	798	799	800	801	802	803	804	805
806	807	808	809	810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825	826	827	828
829	830	831	832	833	834	835	836	837	838	839	840	841	842	843	844	845	846	847	848	849	850	851
852	853	854	855	856	857	858	859	860	861	862	863	864	865	866	867	868	869	870	871	872	873	874
875	876	877	878	879	880	881	882	883	884	885	886	887	888	889	890	891	892	893	894	895	896	897
898	899	900	901	902	903	904	905	906	907	908	909	910	911	912	913	914	915	916	917	918	919	920
921	922	923	924	925	926	927	928	929	930	931	932	933	934	935	936	937	938	939	940	941	942	943
944	945	946	947	948	949	950	951	952	953	954	955	956	957	958	959	960	961	962	963	964	965	966
967	968	969	970	971	972	973	974	975	976	977	978	979	980	981	982	983	984	985	986	987	988	989
990	991	992	993	994	995	996	997	998	999	1000	1001	1002	1003	1004	1005	1006	1007	1008	1009	1010	1011	1012

Character	Meaning	Character	Meaning	Character	Meaning
○	A	7	X	ff, r, u, d.	Nulles
‡	B	8	Y	σ	Dowbleth
\	C	9	Z	z	And
##	D	3	For	d	Wyr
α	E	4	With	ρ	Send
□	F	4	That	∫	Ire
θ	G	4	If	‡	Receave
∞	H	3	But	∫	Bearer
I	I	∫	Where	I	I
δ	K	∫	As	∫	Pray
λ	L	∫	Of	∫	You
∥	M	8	The	∫	Mte
φ	N	X	From	∫	Your Name
∇	O	∞	By	∞	Myne
S	P	∫	So	∫	What
∩	Q	X	Not	∫	Is
f	R	∫	When	∫	Say
Δ	S	∫	There	∫	Me
ε	T	∫	This	∫	My
C	U	X	In	∫	Which

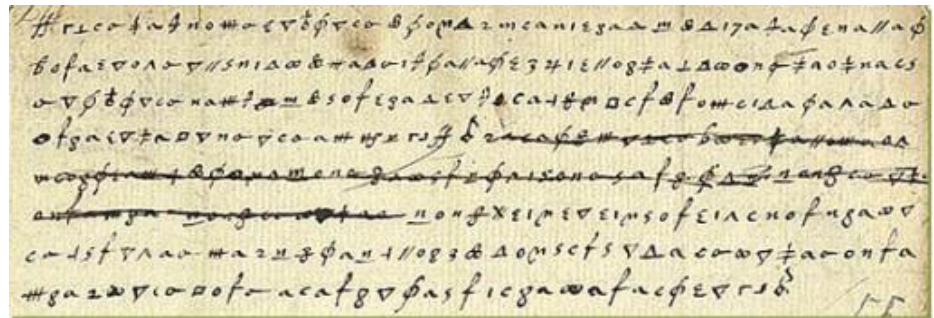
The plot

- Babington plot

- Gifford delivers message from Mary to Babington
- Babington replies with outline of plot

"Myself with ten gentlemen and a hundred of our followers will undertake the delivery of your royal person from the hands of your enemies. For the dispatch of the usurper, from the obedience of whom we are by the excommunication of her made free, there be six noble gentlemen, all my private friends, who for the zeal they bear to the Catholic cause and your Majesty's service will undertake that tragical execution"

- Mary replies endorsing plan
- Walsingham forges postscript to Mary's letter asking Babington to name names





Den VIII february werde onthallt Maria
 Stuart Schots Coninginne & leuende Roomsche Catho-
 lyck hebbende gesocht veel ontus ten aen te sieften haer seloem
 mee ten te maekken van Engeland t' doodsck haer vanden daet
 of te parlement velenmetyck vonden verhoont, Anno 1587.
 C. Metten XIII fol XIII en XIII. v.

Polyalphabetic cipher

- Monoalphabetic cipher
 - Single set of substitutions for all letters

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
U	G	L	Y	B	A	C	K	S	W	N	D	E	F	H	I	J	M	O	P	Q	R	T	V	X	Z

- Polyalphabetic cipher
 - Multiple sets of substitutions
 - Switch between them during encryption
 - 1460s, Leon Alberti hits on idea of using 2+ sets

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
U	G	L	Y	B	A	C	K	S	W	N	D	E	F	H	I	J	M	O	P	Q	R	T	V	X	Z
T	H	E	Q	U	I	C	K	B	R	O	W	N	F	X	J	M	P	S	V	L	A	Z	Y	D	G

Polyalphabetic cipher

- 1586, **Vigenère cipher**, "Le Chiffre Indéchiffrable"
 - Letters Caesar shifted, change based on keyword

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y



Blaise de Vigenère

Plaintext	attackatdawn
Key	LEMONLEMONLE
Ciphertext	LXFOPVEFRNHR

Breaking the Vigenère Cipher

- Vigenère cipher

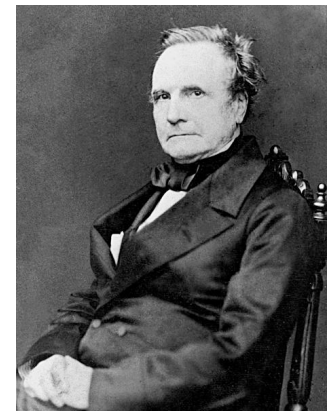
- Much better at hiding letter frequency info

- But key repeats:

- If you know length, an interwoven set of Caesar ciphers

Key:	ABCDABCDABCDABCDABCDABCDABCD
Plaintext:	CRYPTO ISSHORTFOR CRYPTO GRAPHY
Ciphertext:	CSASTP KVSIQUTGQU CSASTP IUAQJB

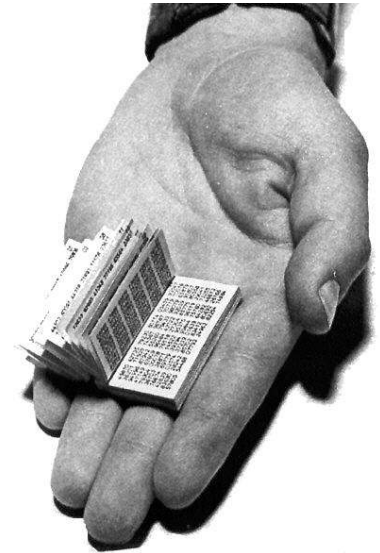
- Distance between repeats = 16
- Suggests key length if 16, 8, 4, 2, or 1
- Find additional repeats to narrow lengths
- Frequency analyze each interwoven set



Charles Babbage

Unbreakable encryption

- One-time pad, 1882
 - Use a **key as long as the message**
 - Choose key (truly) randomly
 - Use key once and only once
 - **Provably secure**



	H	E	L	L	O	message
	7 (H)	4 (E)	11 (L)	11 (L)	14 (O)	message
+	23 (X)	12 (M)	2 (C)	10 (K)	11 (L)	key
=	30	16	13	21	25	message + key
=	4 (E)	16 (Q)	13 (N)	21 (V)	25 (Z)	message + key (mod 26)
	E	Q	N	V	Z	ciphertext

	E	Q	N	V	Z	ciphertext
	4 (E)	16 (Q)	13 (N)	21 (V)	25 (Z)	ciphertext
-	23 (X)	12 (M)	2 (C)	10 (K)	11 (L)	key
=	-19	4	11	11	14	ciphertext - key
=	7 (H)	4 (E)	11 (L)	11 (L)	14 (O)	ciphertext - key (mod 26)
	H	E	L	L	O	message

Breaking one-time pads?

- Try all possible keys

- 26^{length} = big

- Also: generates all possible text sequences

Correct key

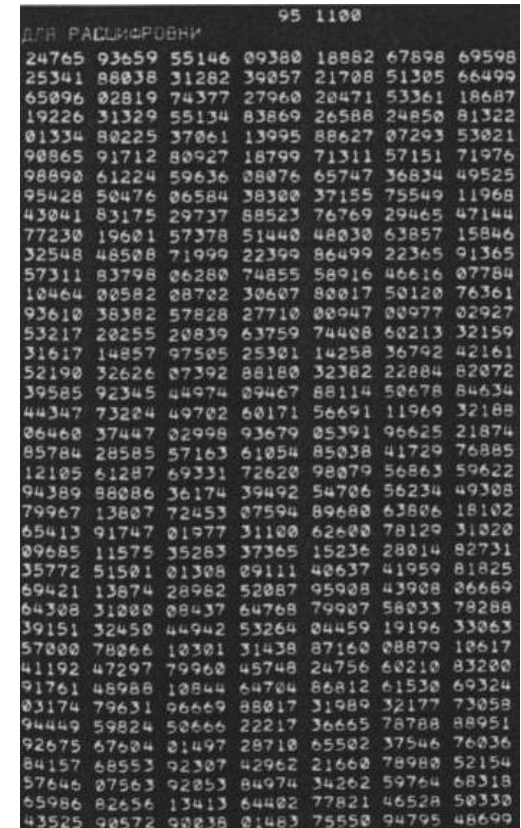
	E	Q	N	V	Z	ciphertext	
	4 (E)	16 (Q)	13 (N)	21 (V)	25 (Z)	ciphertext	
-	23 (X)	12 (M)	2 (C)	10 (K)	11 (L)	key	
=	-19	4	11	11	14	ciphertext - key	
=	7 (H)	4 (E)	11 (L)	11 (L)	14 (O)	ciphertext - key (mod 26)	
	H	E	L	L	O	message	

Some other key

	E	Q	N	V	Z	ciphertext	
	4 (E)	16 (Q)	13 (N)	21 (V)	25 (Z)	ciphertext	
-	19 (T)	16 (Q)	20 (U)	17 (R)	8 (I)	possible key	
=	-15	0	-7	4	17	ciphertext-key	
=	11 (L)	0 (A)	19 (T)	4 (E)	17 (R)	ciphertext-key (mod 26)	
	L	A	T	E	R	possible message	

Unbreakable encryption

- Problems with one-time pads:
 - Must **distribute** pads securely
 - Must use **truly random numbers**
 - Not pseudo-random
 - Not random typing on a keyboard
 - Must **never reuse** the same key



95 1100

0/В	РАСШИФРОВКИ						
24765	93659	55146	09380	18882	67898	69598	
25341	88038	31282	39057	21708	51305	66499	
65096	02819	74377	27960	20471	53361	18687	
19226	31329	55134	83869	26588	24850	81322	
01334	80225	37061	13995	88627	07293	53021	
90865	91712	80927	18799	71311	57151	71976	
98890	61224	59636	08076	65747	36834	49525	
95428	50476	06584	38300	37155	75549	11968	
43041	83175	29737	68523	76769	29465	47144	
77230	19601	57378	51440	48030	63857	15846	
32548	48508	71999	22399	86499	22365	91365	
57311	83798	06280	74855	58916	46616	07784	
10464	00582	08702	30607	80017	50120	76361	
93610	38382	57828	27710	00947	00977	02927	
53217	20255	20839	63759	74408	60213	32159	
31617	14857	97505	25301	14258	36792	42161	
52190	32626	07392	88180	32382	22884	82072	
39585	92345	44974	09467	88114	50678	84634	
44347	73204	49702	60171	56691	11969	32188	
06460	37447	02998	93679	05391	96625	21874	
85784	28585	57163	61054	85038	41729	76885	
12105	61287	69331	72620	98079	56863	59622	
94389	88086	36174	39492	54706	56234	49308	
79967	13807	72453	07594	89680	63806	18102	
65413	91747	01977	31100	62600	78129	31020	
09685	11575	35283	37365	15236	28014	82731	
35772	51501	01308	09111	40637	41959	81825	
69421	13874	28982	52087	95908	43908	06669	
64308	31000	08437	64768	79907	58033	78288	
39151	32450	44942	53264	04459	19196	33063	
57000	78066	10301	31438	87160	08879	10617	
41192	47297	79960	45748	24756	60210	83200	
91761	48988	10844	64704	86812	61530	69324	
03174	79631	96669	88017	31989	32177	73058	
94449	59824	50666	22217	36665	78788	88951	
92675	67604	01497	28710	65502	37546	76036	
84157	68553	92307	42962	21660	78980	52154	
57646	07563	92053	84974	34262	59764	68318	
65986	02656	13413	64402	77821	46528	50330	
43525	90572	90036	01483	75550	94795	48699	

"As a practical person, I've observed that one-time pads are theoretically unbreakable, but practically very weak. By contrast, conventional ciphers are theoretically breakable, but practically strong."

-Steve Bellovin

WWI: Zimmermann Telegram

- 1915, U-boat sinks Lusitania
 - 128 US Civilians killed
 - Germany promises to surface first
- 1916, new Foreign Minister
 - Arthur Zimmermann
- 1917, unrestricted submarine warfare
 - Zimmermann hatches plan
 - Keep American busy at home
 - Persuade Mexico to invade US and invite Japan to attack as well



Arthur Zimmermann

CLASS OF SERVICE DELIVERED
Per Day Message
Day Letter
Night Message
Night Letter

WESTERN UNION
TELEGRAM

NO. 53800
FILE

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

GERMAN LEGATION
MEXICO CITY

130	13042	13401	8501	115	3528	416	17214	8491	11310
18147	18222	21560	10247	11518	23677	13605	3494	14936	
98092	5905	11311	10392	10371	0302	21290	5161	39695	
23571	17504	11269	18276	18101	0317	0228	17694	4473	
23284	22200	19452	21589	87893	5569	13918	8958	12137	
1333	4725	4458	5905	17166	13851	4458	17149	14471	6706
13850	12224	0929	14991	7382	15857	67893	14218	36477	
5870	17553	87893	5870	5454	16102	15217	22801	17138	
21601	17388	7446	23638	18222	6719	14331	15021	23845	
3156	23552	22096	21604	4797	9497	22464	20855	4377	
23610	18140	22260	5905	13347	20420	39689	13732	20687	
6929	5275	18507	52262	1340	22049	13339	11265	22295	
10439	14814	4178	6992	8784	7832	7357	6926	52262	11267
21100	21272	9346	9559	22464	15874	18502	18500	15857	
2188	5376	7381	98092	16127	13486	9350	9220	76036	14219
5144	2831	17920	11347	17142	11264	7667	7762	15099	9110
10482	97556	3569	3670						

BEPHSTORFF.

Charge German Embassy.

TELEGRAM RECEIVED.

MAILED
Oct 1-8-58
WASHINGTON, State Dept.

By *Wm A. Eckhoff*

Date *Oct 27, 1951*

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIEGLERMAN.

Mechanization of secret writing

- Pencil and paper

- Security limited by what humans can do quickly and accurately in the heat of battle

- Enter the machine



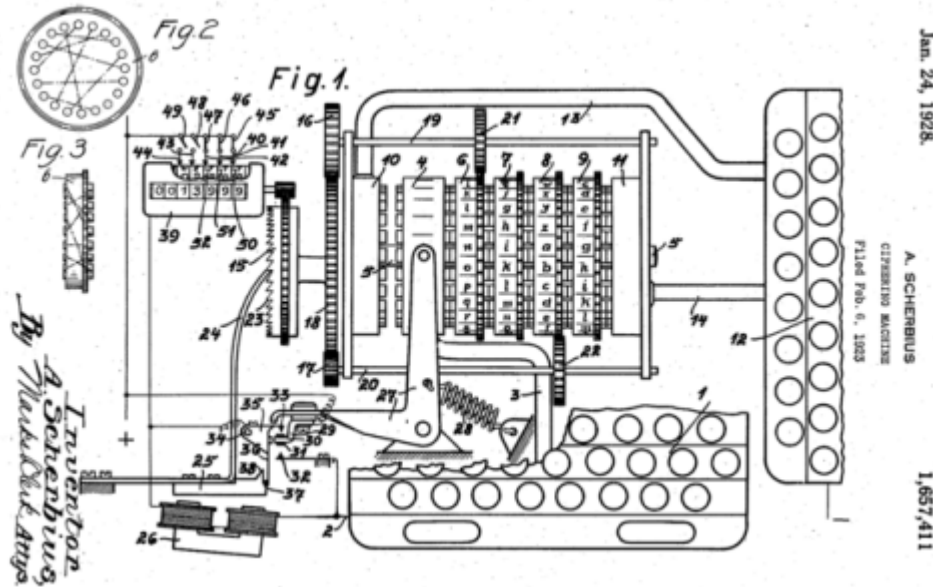
Thomas Jefferson's wheel cipher



Captain Midnight's Code-o-Graph

Enigma machine

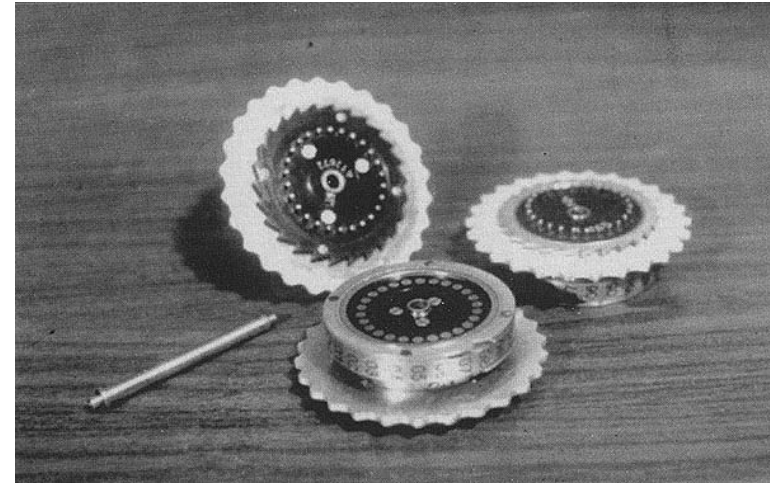
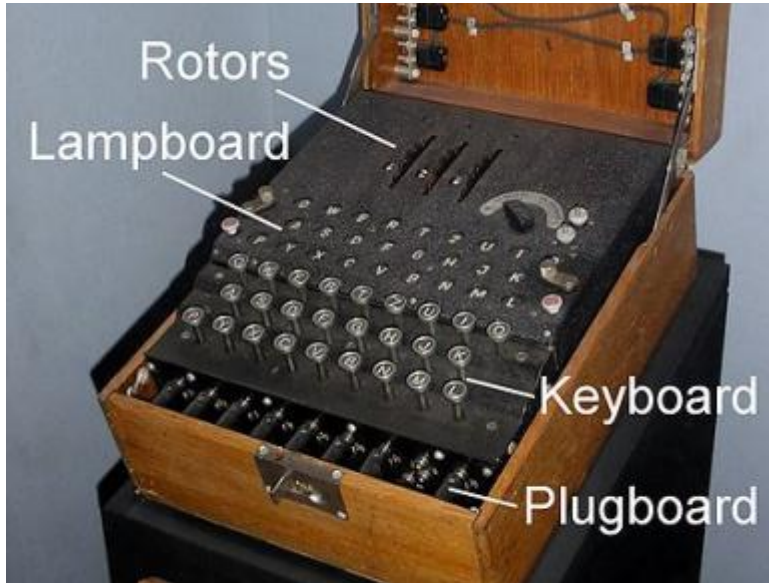
- Enigma cipher machine
 - 1918, patented by German engineer Arthur Scherbius



Arthur Scherbius

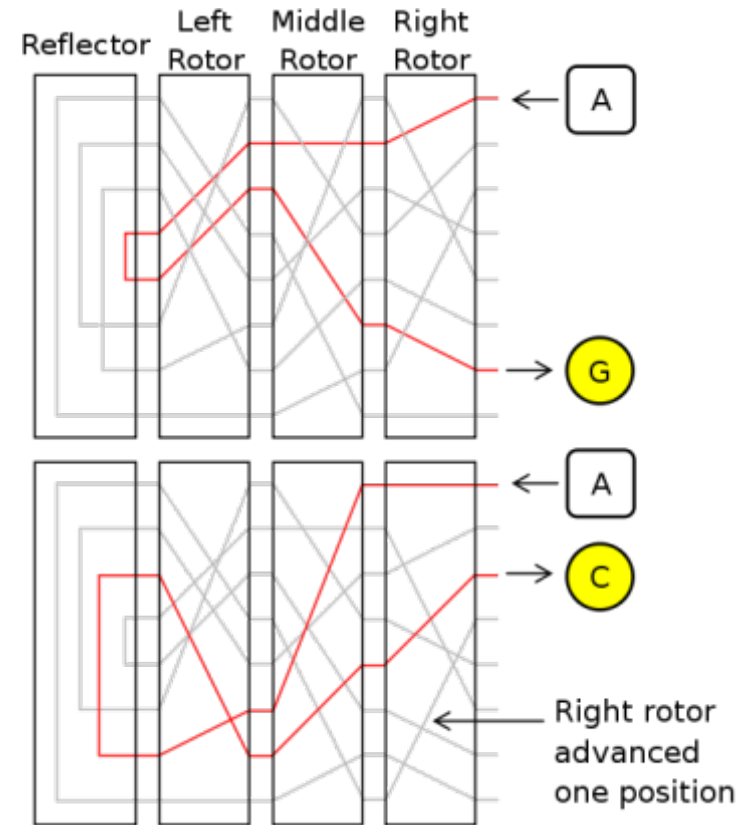
- A electrical/mechanical implementation of a polyalphabetic substitution cipher

ENIGMA



Enigma rotors

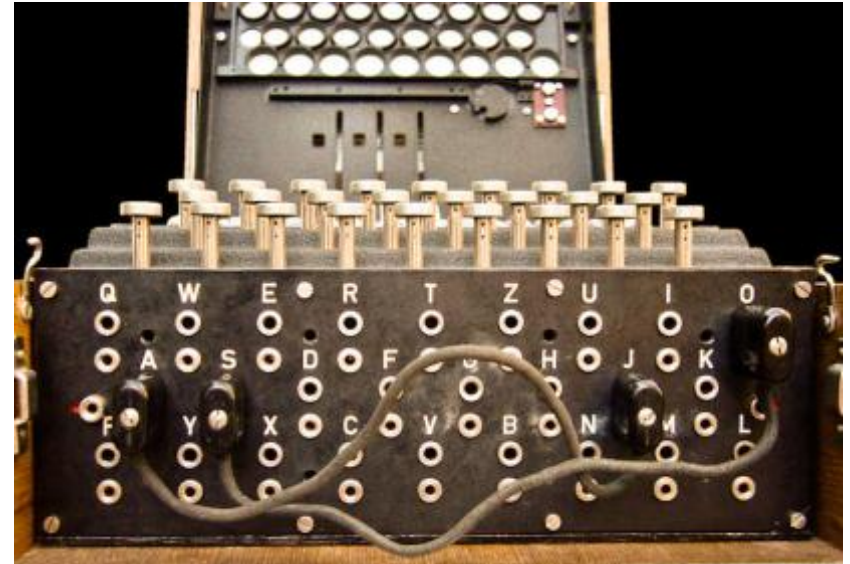
- Rotor (wheel, drum)
 - Monoalphabetic substitution cipher implemented via complex wiring pattern
 - Set to one of 26 initial positions
 - Geared to rotate after each letter
- Rotor set
 - 3 rotors in $3!=6$ possible orders
 - Eventually set increased to 3 out of 5
 - Navy used even more
 - Possible keys:
 - $3! * 26^3 = 6 * 17,576 = 105,456$



Enigma plugboard

- Plugboard

- Operator inserts cables to swap letters
- Initially 6 cables
 - Swaps 6 pairs of letters
 - Leaves 14 letters unswapped
- Possible configurations:
 - 100,391,791,500



- Total keys:

- $17,576 * 6 * 100,391,791,500 \approx 10,000,000,000,000,000$

Enigma

- **Enigma machine**
 - Sales initially slow
 - 1923, Germans find out about failures of communication security in WWI
 - 1925, Scherbius starts mass production
 - German military eventually buys 30,000 Enigma machines
 - 1929, Scherbius dies in carriage accident



Arthur Scherbius

Cracking the Enigma

- **Step 1: Espionage**

- Disgruntled Schmidt meets with French secret agent
- Sells Enigma user manuals
 - Allows replica to be constructed
 - Also codebook and daily key scheme
- French just give intelligence to Poles



Hans-Thilo Schmidt

"It is assumed in judging the security of the cryptosystem that the enemy has at his disposition the machine."

-German memorandum

Cracking the Enigma

- Step 2: Poles identify weakness

- German's had **day code** specifying:

- Configuration of rotors
- Settings of rotors
- Settings of plugboard

- Unique key per message:

- Send 3 letters, encrypted with day key
- Letters specify new setting of rotors
- New rotor setting then used for remainder of message
- Repeat the 3 initial letters twice



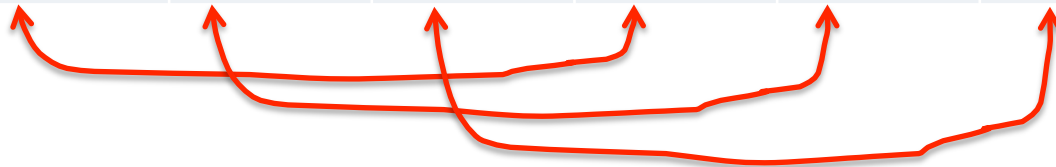
Marian Rejewski

Repetition is the enemy of security!

Cracking the Enigma

- Find patterns in first 6 letters
 - 1st-4th, 2rd-5th, 3rd-6th are ciphers of same letter

Message	1st	2nd	3rd	4th	5th	6th
1	L	O	K	R	G	M
2	M	V	T	X	Z	E
3	J	K	T	M	P	E
4	D	V	Y	P	Z	X

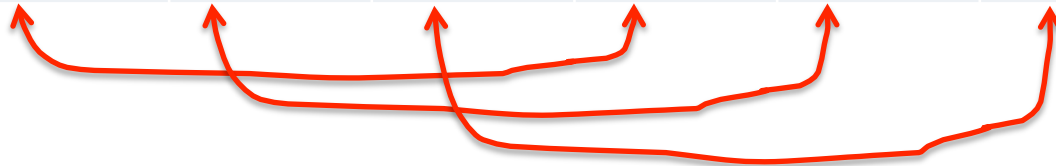


1 st	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4 th				P						M		R	X													

Cracking the Enigma

- Given enough messages:
 - Fill in full table of relations between 3 pairs

Message	1st	2nd	3rd	4th	5th	6th
1	L	O	K	R	G	M
2	M	V	T	X	Z	E
3	J	K	T	M	P	E
4	D	V	Y	P	Z	X



1 st	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4 th	F	Q	H	P	L	W	O	G	B	M	V	R	X	U	Y	C	Z	I	T	N	J	E	A	S	D	K

Fingerprinting a day key

- Find chains

- Chains change each day depending on day key

1 st	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4 th	F	Q	H	P	L	W	O	G	B	M	V	R	X	U	Y	C	Z	I	T	N	J	E	A	S	D	K

A → F → W → A	3 links
B → Q → Z → K → V → E → L → R → I → B	9 links
C → H → G → O → Y → D → P → C	7 links
J → M → X → S → T → N → U → J	7 links

- Also for 2nd-5th and 3rd-6th letter pairs

- # of chains and length, independent of plugboard

- Catalog 105,456 rotors settings using replica

WWII

- 1938, Germany increases Enigma security
 - Add two additional rotors, $C(5, 3) = 60$
 - 10 plugboard cables instead of 6
 - Poles couldn't build big enough "bombes"
 - Poles hand over research to British/French



US Navy bombe



Bletchley Park bombe

Bletchley Park

- **Government Code and Cypher School**
 - Height of WWII, 9000 people
 - Battled against improvements to Enigma
 - May 1, 1940 Germans stop repetition of msg key
 - Turing had already developed technique + machine to crack using "crib" instead of repetition of key



Alan Turing



Cribs

- Cribs
 - Some plaintext you suspect is in ciphertext
 - Ideally also the location
 - e.g. Germans usually broadcast weather at 6 am
 - "wetter" somewhere at start of message
 - German Navy had strongest crypto:
 - 3 rotors out of 8, reflector with 26 orientations
 - Avoided stereotypical messages
 - Allies:
 - Mine area to generate traffic
 - Grid reference as crib
 - Also, stole code books



Type VII U-boat

Summary

- History of Cryptography
 - Substitution ciphers
 - Monoalphabetic
 - Polyalphabetic
 - One-time pads
 - Provably unbreakable
 - (if used carefully)
 - Cryptography in WWI and WWII
 - Zimmerman telegraph
 - Enigma

