The History of Cryptography

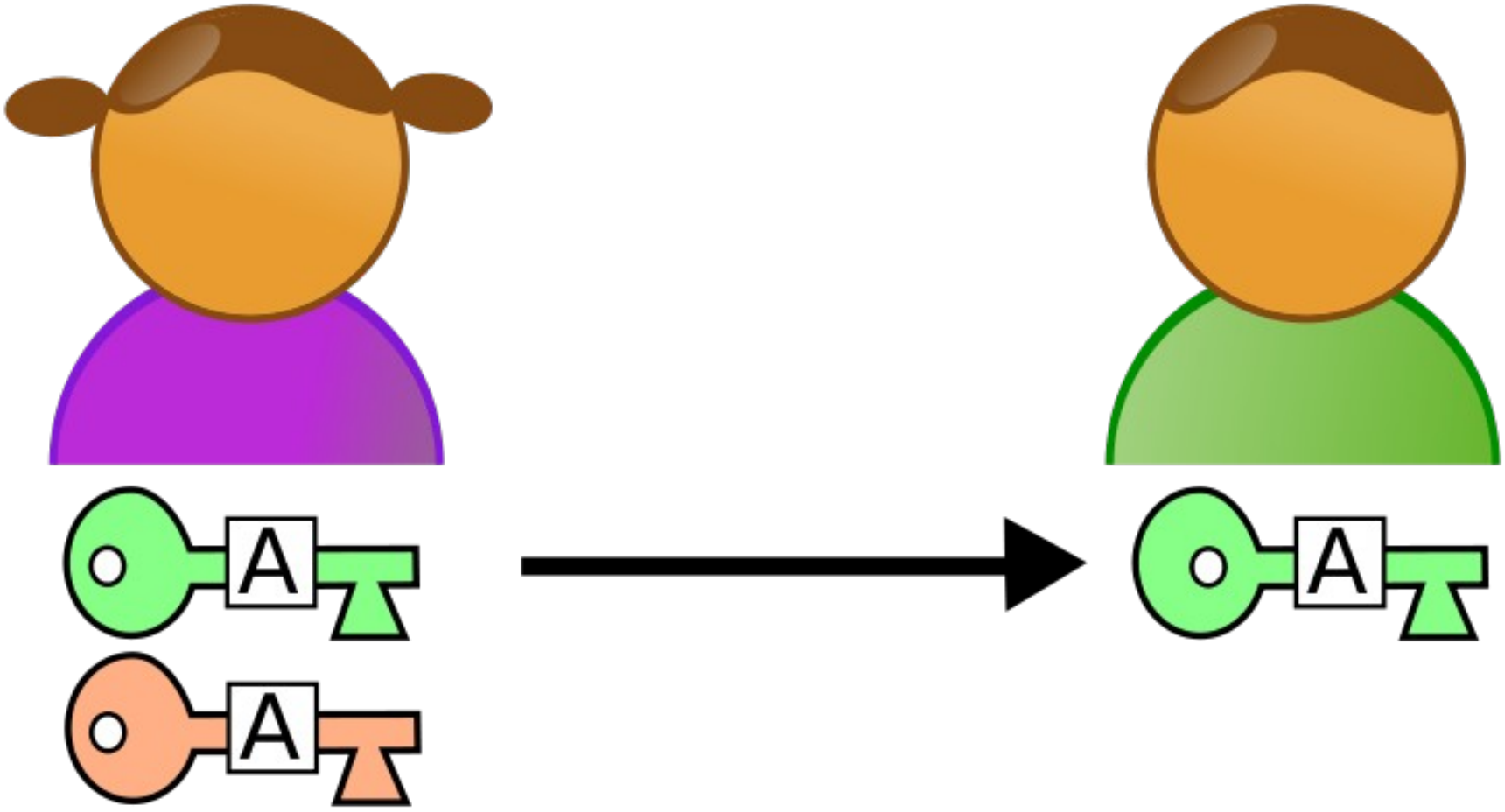
Portland Underground Grad School

Erik L. Arneson
http://arnesonium.com/crypto

Principal Concepts

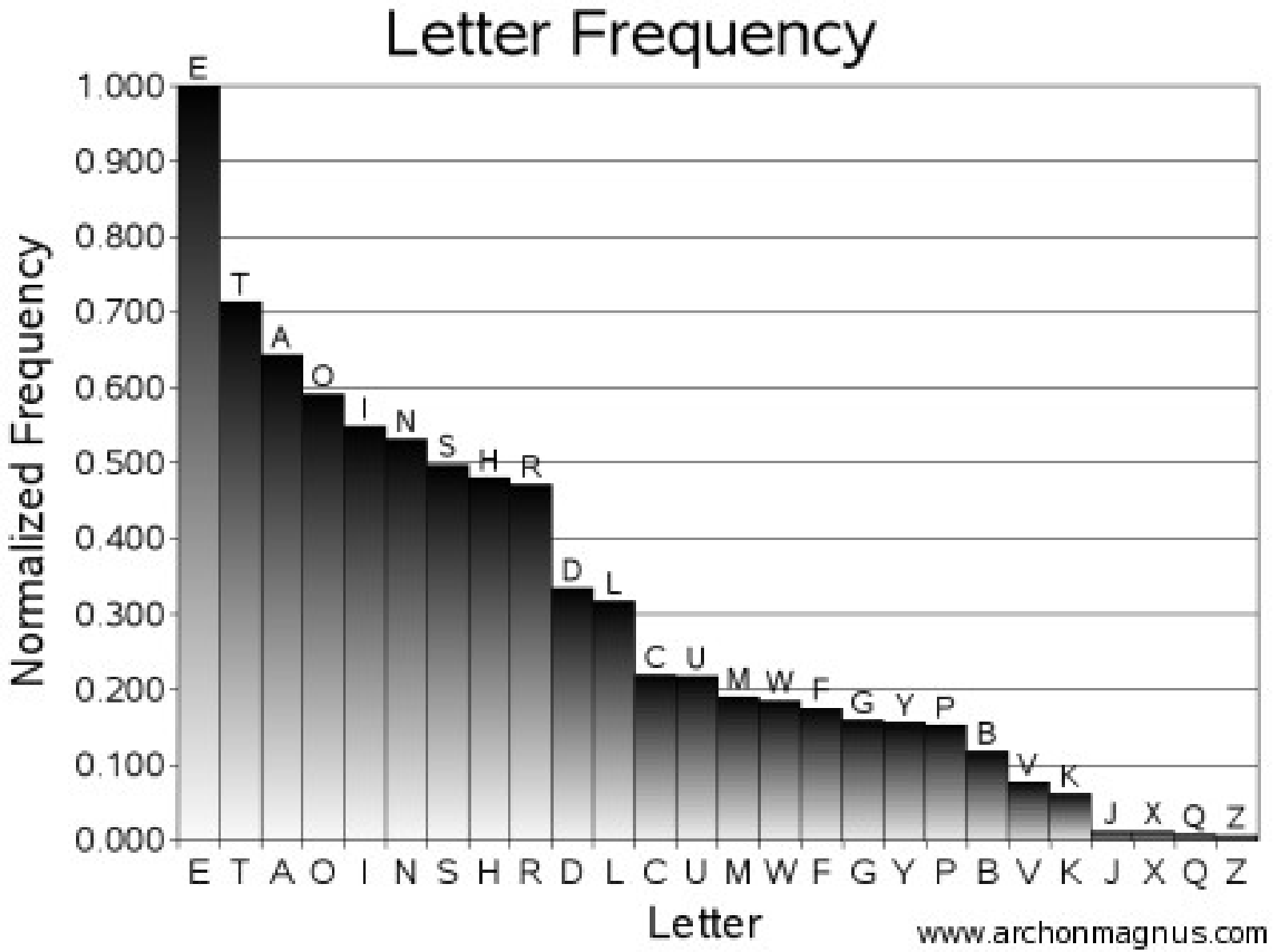
- Predictability and Randomness
- Security and Usability
- Identity and Trust
- Thinking Like an Attacker

Alice and Bob



Cryptanalysis

Frequency Analysis



Cracking Your Homework

Alberti Cipher

Voynich Manuscript

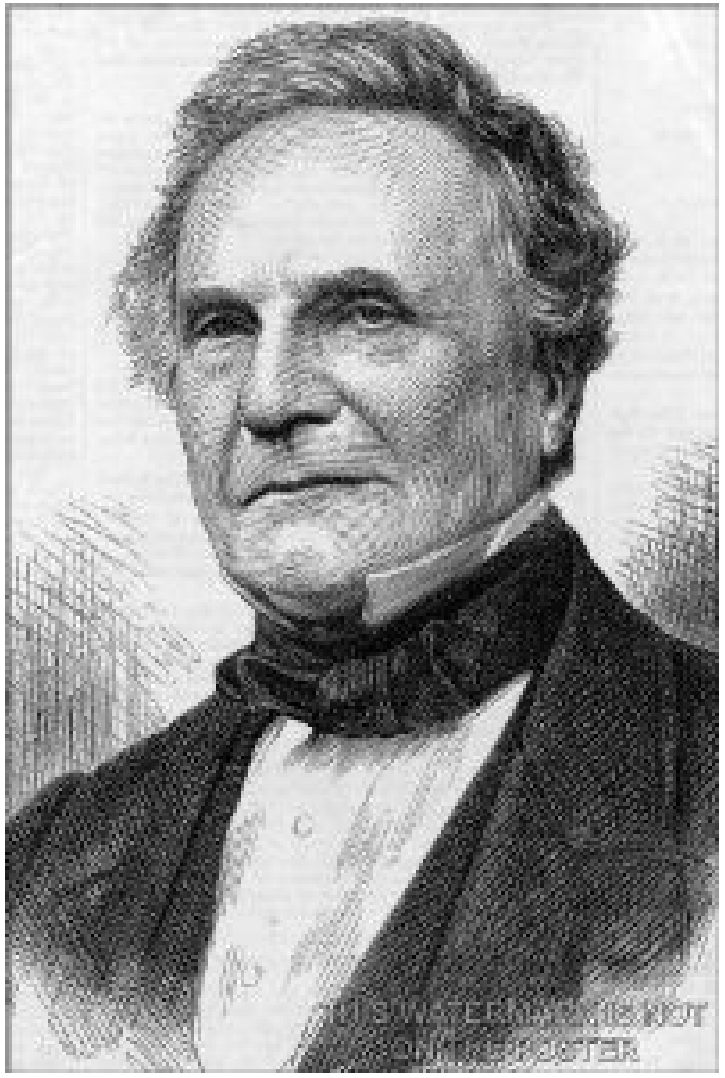
Johannes Trithemius

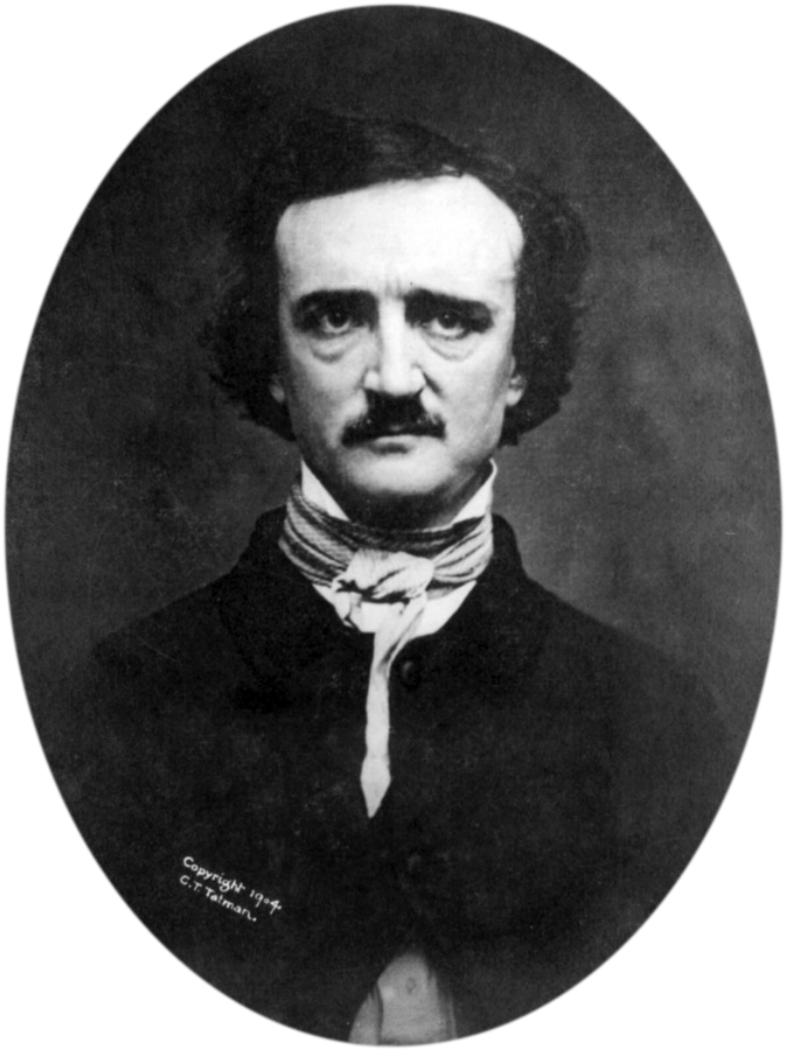
The Great Cipher

N	O	P	Q	R	S	T	V	X	Y	Z	&
811 702	117 238 359 500	219 338	407 595	511 733	355 527	340 618	141 163 284 164	205 436	518 639	820	279 448 615 827

genera,l,ux	35	lieu,x	668	Ob	19	presque	801
gens	55	limites	708	obei	59	preten,dre,tion	30
ger … 575	95	livre	728	objet,s	69	pretexte	841
ges	115	le Roy de	758	oblig,er,ation	89	pri	881
gla	155	le Prince, de	798	observ,er,ation	129	principa,l,ux	52
gle	215	le Duc de	838	obstacle,s	179	prisonnier,s	132
gli	275	le Marquis de	858	obtenir	225	pro	162
glo,ire	355	le Baron de	898	oc,casion	249	prochain	202
gna	375	le Sieur de	49	ocup,er	289	profit,er	262
gne … 645	455	loin	79	of	349	projet,s	282
gni	485	lon	119	office,ier,s	429	propos,ition,s	382
gno	505	lors	189	offre,s	449	provision,s	422
gouvern,er,ment	16	luy … 648	239	oient	499	prouv	442
gra,ce	405			oir	529	pru	462
grand	525	Ma … 868	298	oire	559	publi,er,c	512
gre	585	me … 779	339	oit	629	puis,sance	572
gri	625	mi	279	ol	669		
gro	665	mo	439	om	729	Qu	612
gua	695	mu	469	on,s	759	qua	692
gue	785	magasin,s	519	ont	789	qualite	722
guerre	825	main,s	549	op,pose,ition	819	quand	742
gui,de,s	895	mais … 159	579	or	849	quantité	762
		maitre,s	609	ordinaire,s	899	quarente	782
ha	26	mal,ade,s,ie,s	659	ordonn,er	20	quart,ier,s	822
he	56	mand,er	679	ordre,s	60	quatre	842
hi	156	maniere,s	719	or,s,t	100	que	862
ho	216	manque,r	739	os,t	130	quel,le,s	882
hu	266	marche,s	769	ou,r	160	question,s	23
haut	326	marqu,e,r	799	outre	210	qui … 50	53
habi,t,te,tant	486	marecha,l,ux	829	ouvr	240	qu'il	73
heur,e,s	656	mauvais	859			quinze	133
hier	796	meilleur	879	Pa	270	quo,n … 190	153

19th Century Cryptography

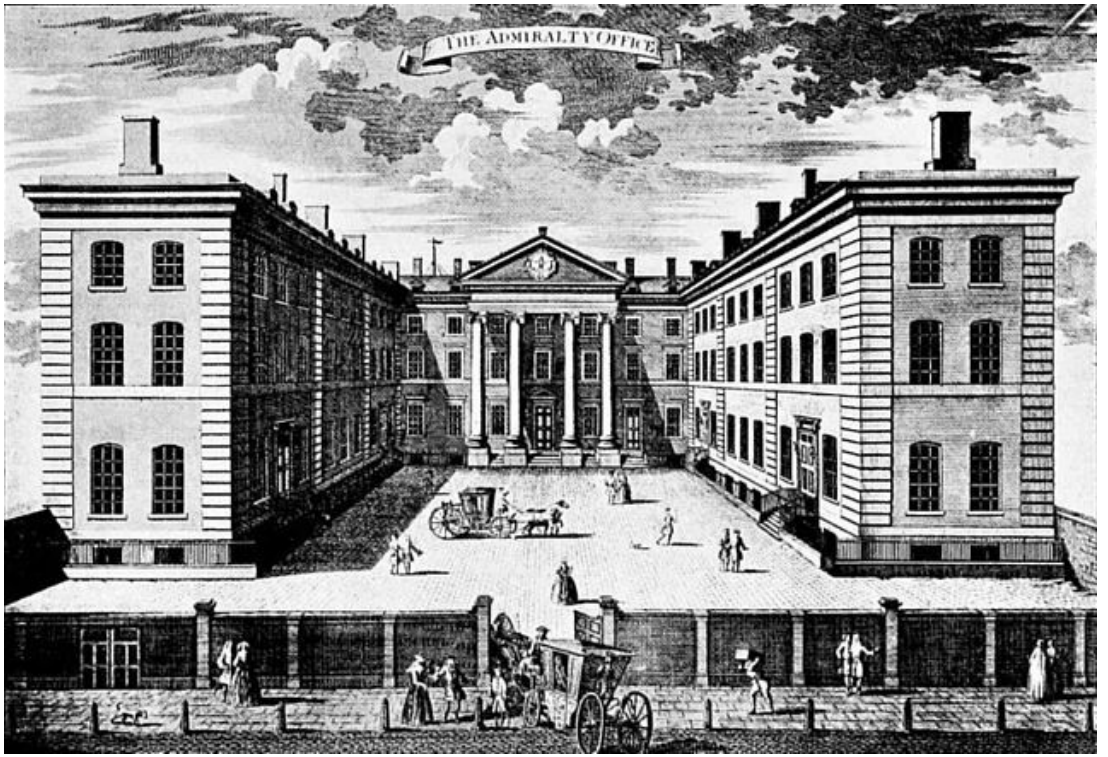




Playfair Cipher

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

World War I



Homework: Crack Your Homework

- Trade ciphertext homework with somebody who wasn't your partner.
- Crack it.