Mathematical

Cryptography

LESSON 1 - History and why MATHS came in Cryptography

from Ancient Greek:
κρυπτός, romanized: kryptós "hidden, secret";
γράφειν graphein, "to write"

Frequent mistakes:

~~Crypthography~~ ~~Criptography~~ ~~Kryptography~~

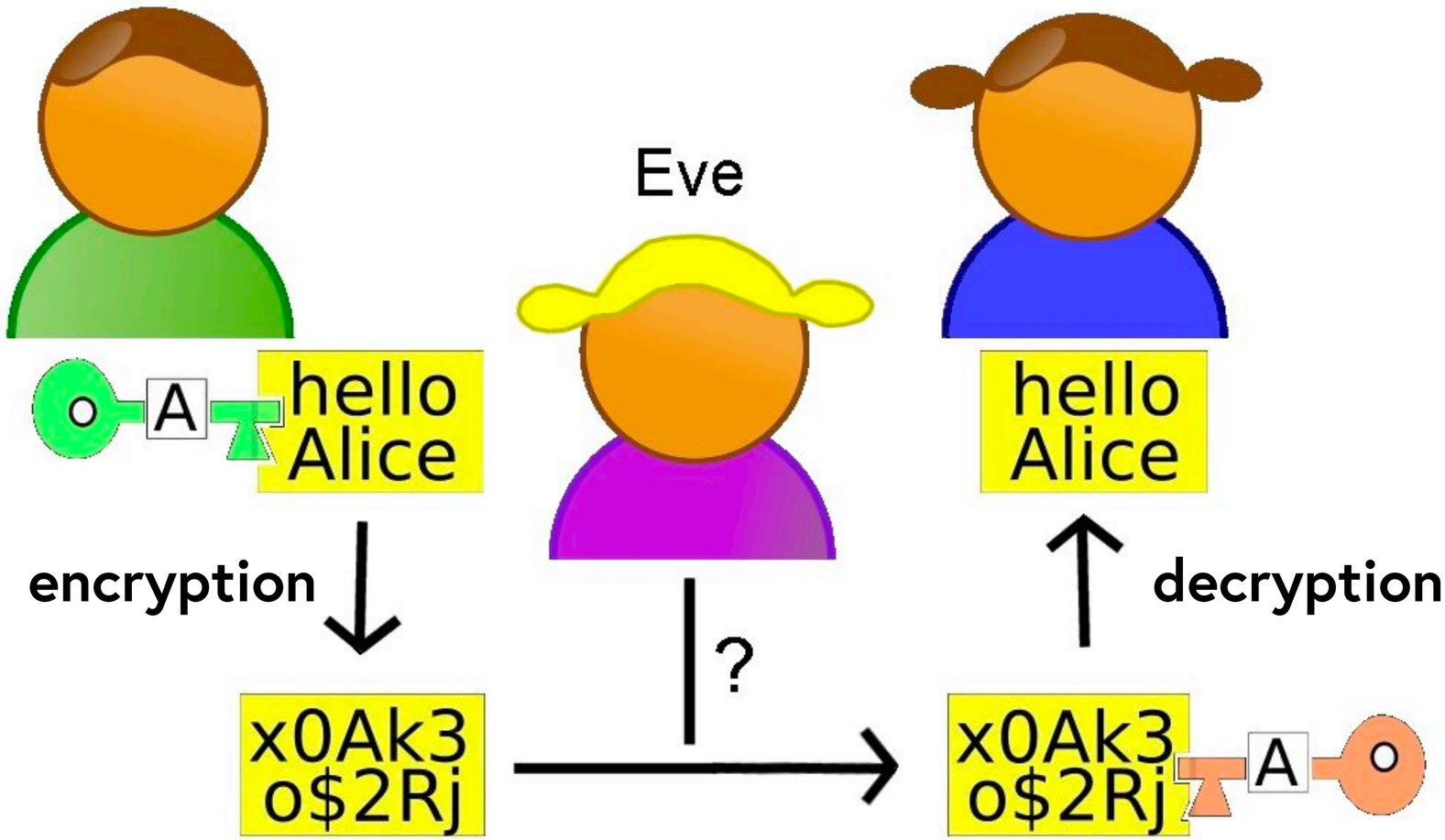
For thousands of years, kings, queens and generals have relied on efficient communication in order to govern their countries and command their armies. At the same time, they have all been aware of the consequences of their messages falling into the wrong hands, revealing precious secrets to rival nations and betraying vital information to opposing forces. It was the threat of enemy interception that motivated the development of codes and ciphers: techniques for disguising a message so that only the intended recipient can read it.

The desire for secrecy has meant that nations have operated codemaking departments, responsible for ensuring the security of communications by inventing and implementing the best possible codes. At the same time, enemy codebreakers have attempted to break these codes, and steal secrets. The history of codes and ciphers is the story of the centuries-old battle between codemakers and codebreakers.

Singh - The code book

Unit 1
Classical cryptography: monoalphabetic substitution ciphers

Cryptography



Terminology

Code: replace words with words

Example attack at dawn -> JUPITER

Cipher: replace letters with symbols/letters

Example Replace a with B, b with C,...
attack at dawn -> BUUBDL BU EBXO

notation in the course:

plaintext (small)
CIPHERTEXT (capital)

We use equally decipher/decoding with the same meaning. No one uses codes nowdays

Classical cryptography

Caesar cipher

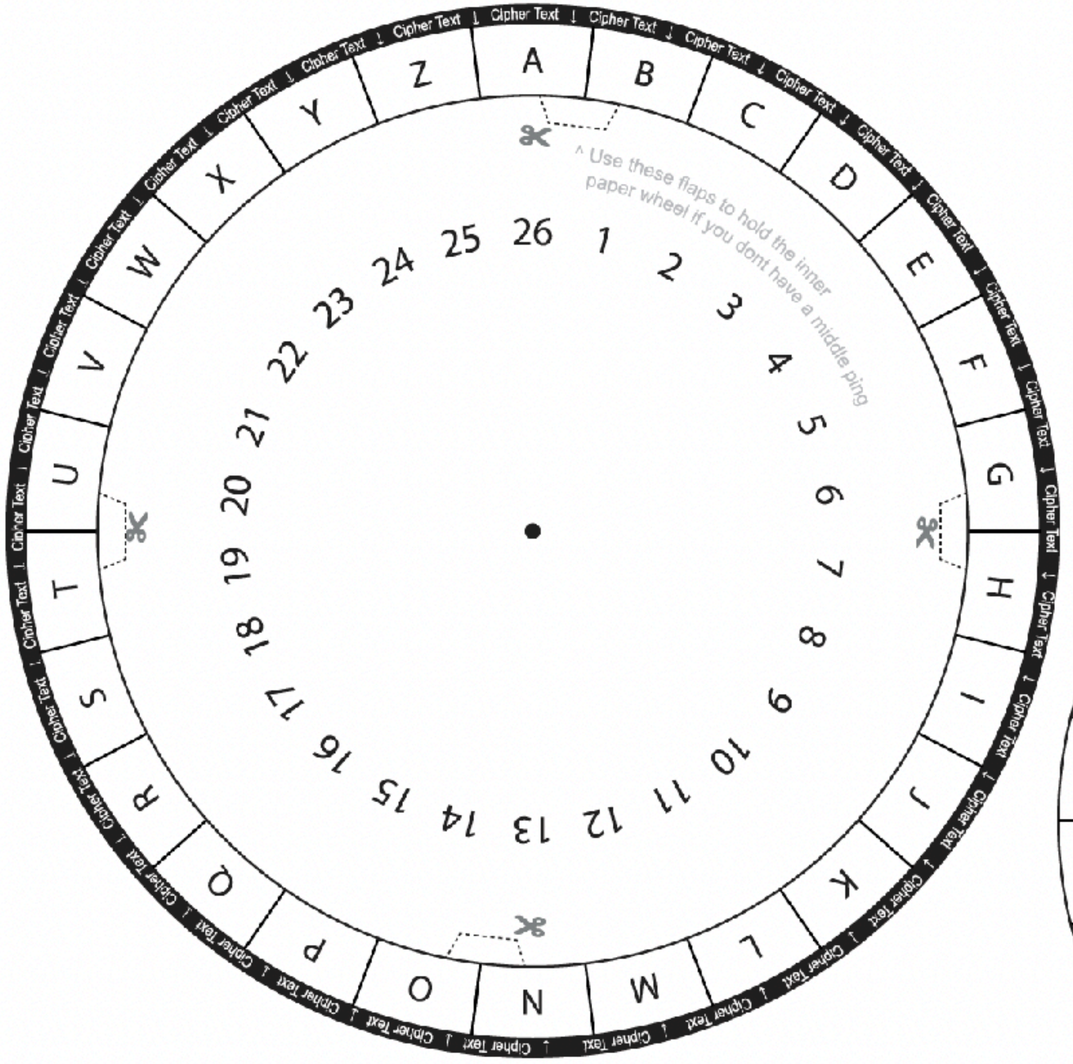
Letters are replaced with a letter that is a fixed number of letters beyond the current letter

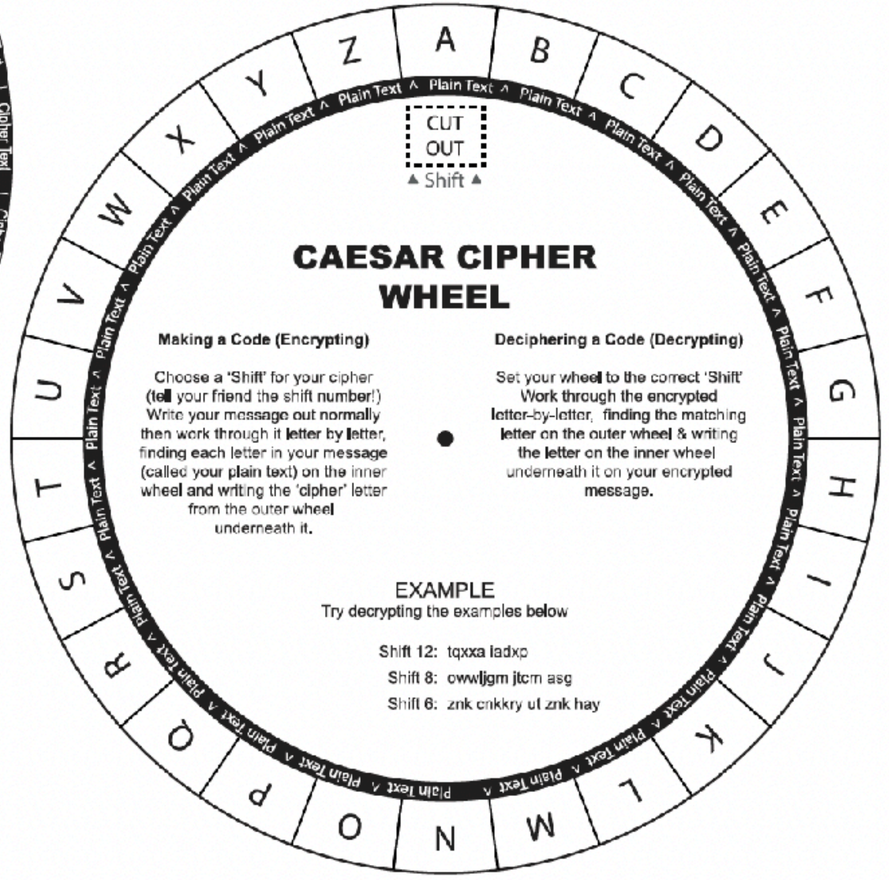
Example

Plain alphabet	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
Cipher alphabet	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

Plaintext	v	e	n	i,		v	i	d	i,		v	i	c	i												
Ciphertext	Y	H	Q	L,		Y	L	G	L,		Y	L	F	L												

Caesar Cipher Wheel





BOBMCKAY.com

http://bobmckay.com/coding for kids/caesar cipher wheel printable pdf/

Classical cryptography

Caesar cipher

Encrypt the following plaintext using a Caesar Cipher where a -> J (SHIFT Key:+9):

"a page of history is worth a volume of logic"

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
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

Answer: `J YJPN XO QRBCXAH RB FXACQ J EXUDVN XO UXPRL`

Classical cryptography

Caesar cipher

1) Decrypt DVVKZECFSSPRKKVE knowing that it is a Caesar cipher.

2) What is the key (which cipher letter corresponds to the plaintext a, what is the shift key?

Answer:

1) meet in lobby at ten
2) a->R (Shift key: +17)

Classical cryptography

Monoalphabetic substitution ciphers

Caesar cipher admits 26 distinct ciphers.

Now, admit you can make any rearrangement of the alphabet

Example

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

Classical cryptography

Monoalphabetic substitution ciphers

How many are the substitution ciphers?

$$26! = 26 \times 25 \times \cdots \times 2 \times 1$$

$$\text{Decimal digits: } \approx [\log_{10} 26!] + 1 = 26 + 1 = 27$$

Actually $26! = 403,291,461,126,605,635,584,000,000$

$$\text{new supercomputer (2022): } 10^{18} \text{ operations/s}$$

About 13 years!

A brute force attack is impossible!

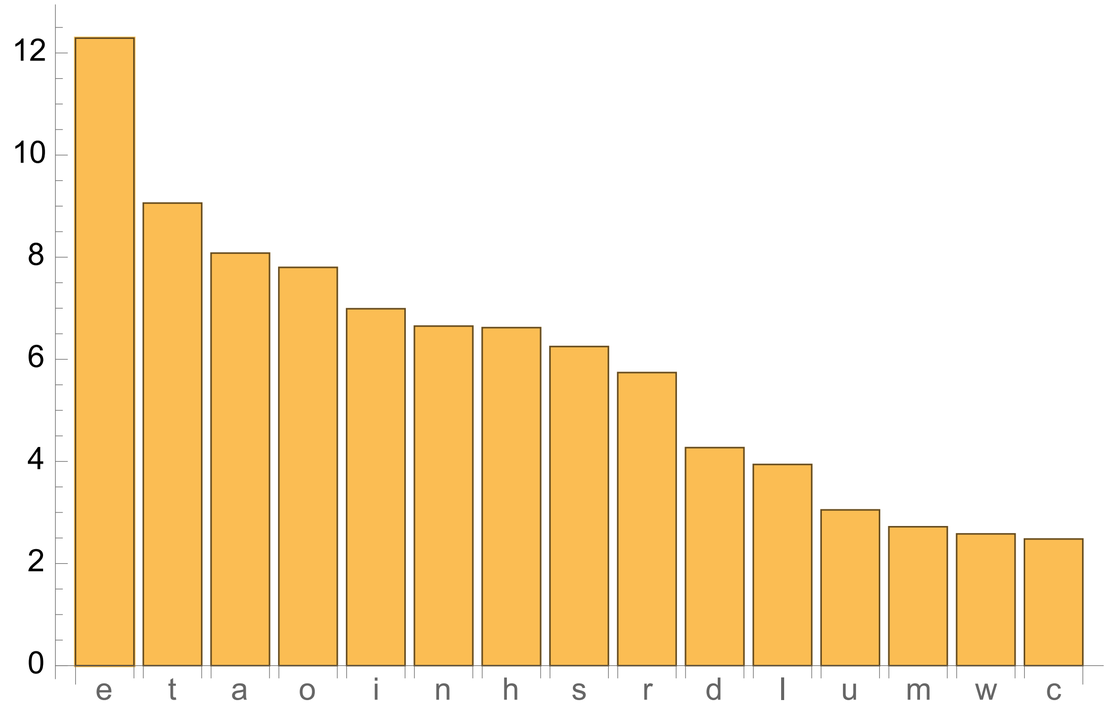
Substitution ciphers dominated the first millennium AD

Classical cryptography

decrypting monoalphabetic substitution ciphers

al Kindi: A Manuscript on Deciphering Cryptographic Messages **(IX AD, discovered in 1987)**

FREQUENCES OF LETTERS IN ENGLISH



A typical distribution of letters in English language text

decrypting monoalphabetic substitution ciphers

FREQUENCES OF DIGRAMS IN ENGLISH

The most frequent digrams:

th	he	an	re	er	in	on	at	nd	st	es	en	of	te	ed
168	132	92	91	88	86	71	68	61	53	52	51	49	46	46

Most common English bigrams (frequency per 1000 words)

Classical cryptography

decrypting monoalphabetic substitution ciphers with frequency analysis

Between A.D. 800 and 1200, Arab scholars enjoyed a vigorous period of intellectual achievement. At the same time, Europe was firmly stuck in the Dark Ages. While al-Kindī was describing the invention of cryptanalysis, Europeans were still struggling with the basics of cryptography. Frequency analysis in Europe began only around 1500!

No cryptography is better than bad cryptography: the example of Queen Mary of Scotland (1585)

Classical cryptography

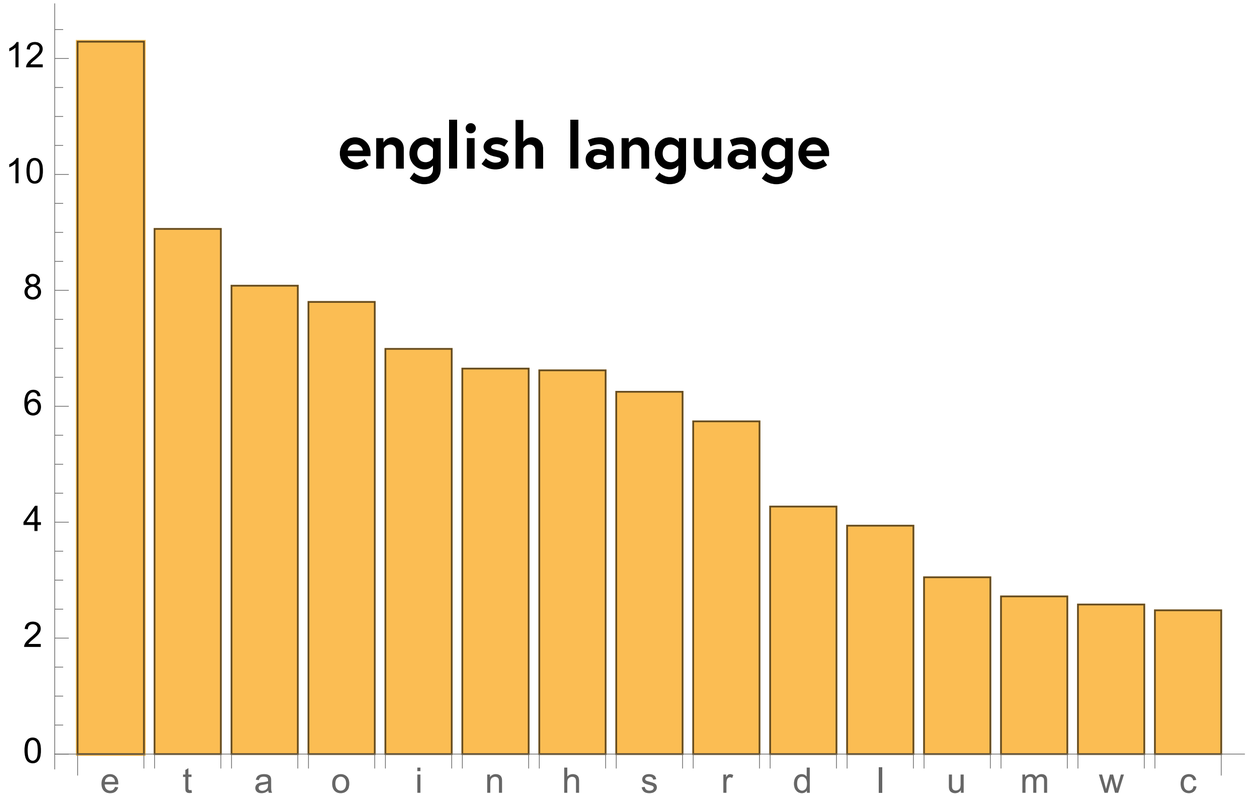
monoalphabetic ciphers: decryption by analyzing frequences

CIPHERTEXT

LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFEMVEWHKVSTYLXZIXLIKIIXPIJVSZEYPE
RRGERIMWQLMGLMXQERIWGPSRIHMXQEREKIETXMJTPRGEVEKEITREWHEXXLEXXMZITWA
WSQWXSWEXTVEPMRXRSJGSTVRIEYVIEXCVMUIMWERGMIWXMJMGCSMWXSJOMIQXLIVI
QIVIXQSVSTWHKPEGARCSXRWIEVSWIIBXVIZMXFSJXLIKEGAEWHEPSWYSWIWIEVXLISXLI
VXLIRGEPIRQIVIIBGIIHMWYPFLEVHEWHYPSRRFQMXLEPPXLIECCIEVEWGISJKTVWMRLIHYS
PHXLIQIMYLXSJXLIMWRIGXQEROIVFVIZEVAEKPIEWHXEAMWYEPPXLMWYRMWXSGSWRM
HIVEXMSWMGSTPHLEVHPFKPEZINTCMXIVJSVLMRSCMWMSWVIRCIGXMWYMX

Classical cryptography

decryption by analyzing frequences



Hypothesis 1: T~e, Z~t

decryption

Hypothesis 1: T~e, Z~t

tIOLEGXKLeQODLtGOFtKGRXEeNGXtGtIeHKOFEOHSeLQFRteEIFOJXeLGYLeEXKOFUEGDHXteKLQFREGD
HXteKFetVGKALVOtIYGEXLGFOFteKFetLeEXKOtNtIeEGXKLeOLeYYeEtOCeSNLHSOtOFtGtVGHQKtLYO
KLtOFtKGRXEOFUtIetIeGKNGYEKNHtGUKQHINOFESXROFUIGVDQFNESQLLOEQSQFRHGHXSQKQSUGKOtID
LVGKAeUReLKLQROUOtQSLOUFQtXKeLQFRLeEGFRHKGCOROFUREtQOSLGYKeQSOFteKFetLeEXKOtNHKGt
GEGSLQSUGKOtIDLQFRtIKeQtLeUOHLeECOKXLeLYOKeVQSSLIeFEeNGXVOSSSeQKFWGtItIeGKetOEQSQ
LHeEtLGYEGDHXteKQFRFetVGKALeEXKOtNQLVeSSQLIGVtIQttIeGKNOLQHHSOeROFtIeOFteKFettIOL
AFGVSeRUeVOSSIeSHNGXOFReLOUFOFUQFRReCeSGHOFULeEXKeQHHSOEQtOGFLQFRFetVGKAHKGtGEGSL
QLVeSSQLWXOSROFULeEXKeFetVGKAL

Let's try the two most frequent digrams...

frequences of 2-grams

T~e, Z~t

English	Ciphertext
th ->3.87%	? OF -> 2.85%
he ->3.69%	? ZI=tI -> 2.51%
in->2.36%	? LT=Le -> 2.2%

here O~i, F~n

here I~h

here L~n ?

Hypothesis 3:
I~h, O~i, F~n

tIOLEGXKLeQODLtGOFtKGRXEeNGXtGtIeHKOFEOHSeLQFRteEIFOJXeLGYLeEXKOFUEGDHXteKLQFREGD
HXteKFetVGKALVOtIYGEXLGFOFteKFetLeEXKOtNtIeEGXKLeOLeYYeEtOCeSNLHSOtOFtGtVGHQKtLYO
KLtOFtKGRXEOFUtIetIeGKNGYEKNHtGUKQHINOFESXROFUIGVDQFNESQLLOEQSQFRHGHXSQKQSUGKOtID
LVGKAeUReLKLQROUOtQSLOUFQtXKeLQFRLeEGFRHKGCOROFUREtQOSLGYKeQSOFteKFetLeEXKOtNHKGt
GEGSLQSUGKOtIDLQFRtIKeQtLeUOHLeECOKXLeLYOKeVQSSLIeFEeNGXVOSSSeQKFWGtItIeGKetOEQSQ
LHeEtLGYEGDHXteKQFRFetVGKALeEXKOtNQLVeSSQLIGVtIQttIeGKNOLQHHSOeROFtIeOFteKFettIOL
AFGVSeRUeVOSSIeSHNGXOFReLOUFOFUQFRReCeSGHOFULeEXKeQHHSOEQtOGFLQFRFetVGKAHKGtGEGSL
QLVeSSQLWXOSROFULeEXKeFetVGKAL

Hypothesis 4:
K~r, L~s

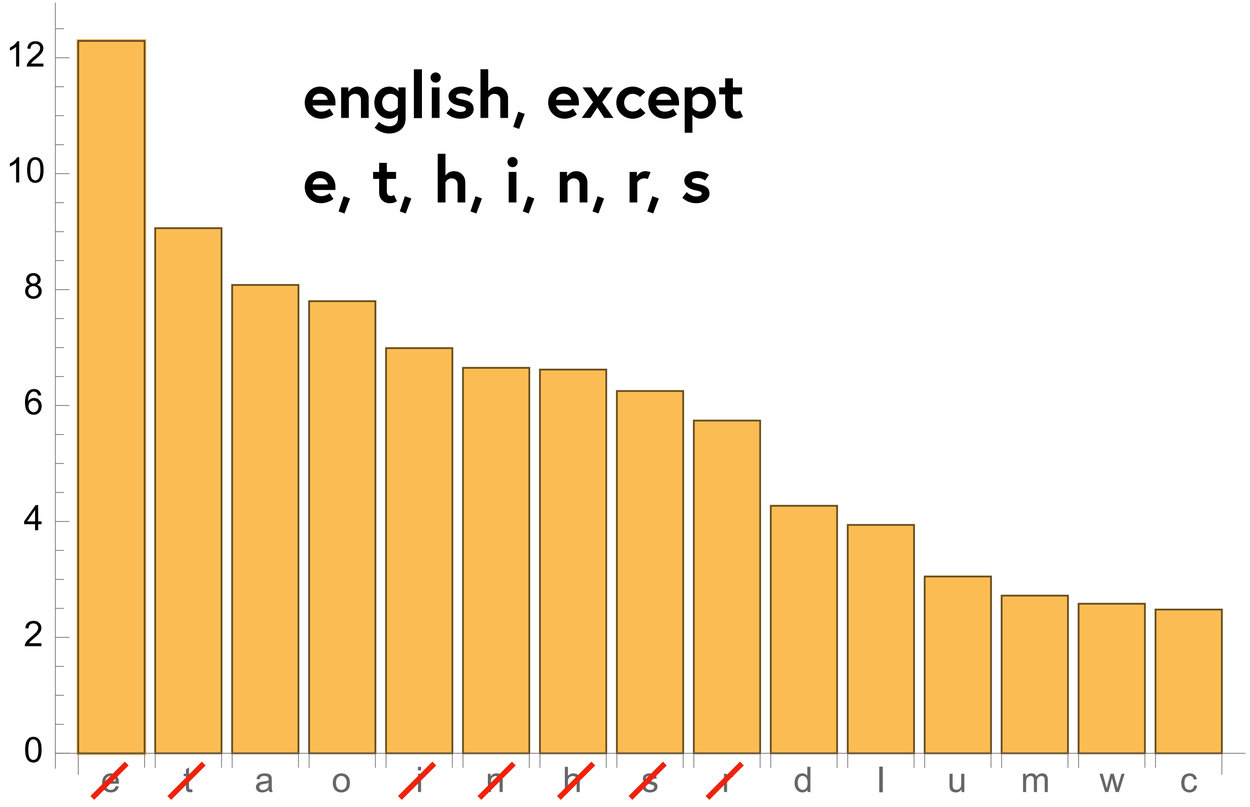
T~e, Z~t, I~h, I~h, O~i, F~n

Hypothesis 4:
K~r, L~s

thisEGXrseQiDstGintrGRXEeNGXtGtheHrinEiHSesQnRteEhniJXesGYseEXrinUEGDHXtersQnREGD
HXternetVGrAsVithYGEXsGninternetseEXritNtheEGXrseiseYYeEtiCeSNsHSitintGtVGHQrtsYi
rstintrGRXEinUthethеGrNGYErNHtGUrQHhNinESXRinUhGVDQnNESQssiEQSQnRHGHXSQrQSUGrithD
sVGrAeUResrsQRiUitQSsiUnQtXresQnRseEGnRHrGCiRinURetQiSsGYreQSinternetseEXritNHrGt
GEGSsQSUGrithDsQnRthreQtseUiHseECirXsesYireVQSSshenEeNGXViSSSeQrnWGththeGretiEQSQ
sHeEtsGYEGDHXterQnRnetVGrAseEXritNQsVeSSQshGVthQttheGrNisQHHSieRintheinternetthis
AnGVSeRUeViSSheSHNGXinResiUninUQnRReCeSGHinUseEXreQHHSiEQtiGnsQnRnetVGrAHrGtGEGSs
QsVeSSQsWXiSRinUseEXrenetVGrAs

Come back to most frequent letters, except T, Z, I, O, F, K, L...

Come back to most frequent letters



Hypothesis 5: G~a or G~o.

Hypothesis 5.1: G~a

thisEaXrseQiDstaintraRXEeNaXtatheHrinEiHSesQnRteEhniJXesaYseEXrinUEaDHXtersQnREaD
HXternetVarAsVithYaEXsaninternetseEXritNtheEaXrseiseYYeEtiCeSNsHSitintatVaHQrtsYi
rstintraRXEinUthethearNaYErNHtaUrQHhNinESXRinUhaVDQnNESQssiEQSQnRHaHXSQrQSUarithD
sVarAeUResrsQRiUitQSsiUnQtXresQnRseEanRHraCiRinURetQiSsaYreQSinternetseEXritNHrat
aEaSsQSUarithDsQnRthreQtseUiHseECirXsesYireVQSSshenEeNaXViSSSeQrnWaththeareti EQSQ
sHeEtsaYEaDHXterQnRnetVarAseEXritNQsVeSSQshaVthQtthearNisQHHSieRintheinternetthis
AnaVSeRUeViSSheSHNaXinResiUninUQnRReCeSaHinUseEXreQHHSiEQtiansQnRnetVarAHrataEaSs
QsVeSSQsWXiSRinUseEXrenetVarAs

Hypothesis 5.2: G~o

thisEoXrseQiDstointroRXEeNoXtotheHrinEiHSesQnRteEhniJXesoYseEXrinUEoDHXtersQnREoD
HXternetVorAsVithYoEXsoninternetseEXritNtheEoXrseiseYYeEtiCeSNsHSitintotVoHQrtsYi
rstintroRXEinUthetheorNoYErNHtoUrQHhNinESXRinUhoVDQnNESQssiEQSQnRHoHXSQrQSUorithD
sVorAeUResrsQRiUitQSsiUnQtXresQnRseEonRHroCiRinURetQiSsoYreQSinternetseEXritNHrot
oEoSsQSUorithDsQnRthreQtseUiHseECirXsesYireVQSSshenEeNoXViSSSeQrnWoth theoreti EQSQ
sHeEtsoYEoDHXterQnRnetVorAseEXritNQsVeSSQshoVthQttheorNisQHHSieRintheinternetthis
AnoVSeRUeViSSheSHNoXinResiUninUQnRReCeSoHinUseEXreQHHSiEQtionsQnRnetVorAHrotoEoSs
QsVeSSQsWXiSRinUseEXrenetVorAs

thisEoXrseQiDstointroRXEeNoXtotheHrinEiHSesQnRteEhniJXesoYseEXrinUEoDHXtersQnREoD
HXternetVorAsVithYoEXsoninternetseEXritNtheEoXrseiseYYeEtiCeSNsHSitintotVoHQrtsYi
rstintroRXEinUthetheorNoYErNHtoUrQHhNinESXRinUhoVDQnNESQssiEQSQnRHoHXSQrQSUorithD
sVorAeUResrsQRiUitQSsiUnQtXresQnRseEonRHroCiRinURetQiSsoYreQSinternetseEXritNHrot
oEoSsQSUorithDsQnRthreQtseUiHseECirXsesYireVQSSshenEeNoXViSSSeQrnWoththeoretiEQSQ
sHeEtsoYEoDHXterQnRnetVorAseEXritNQsVeSSQshoVthQttheorNisQHHSieRintheinternetthis
AnoVSeRUeViSSheSHNoXinResiUninUQnRReCeSoHinUseEXreQHHSiEQtionsQnRnetVorAHrotoEoSs
QsVeSSQsWXiSRinUseEXrenetVorAs

Hypothesis 6:
R~d, X~u, E~c

thiscourseQiDstointroduceNoutotheHrinciHSesQndtechniJuesoYsecurinUcoDHutersQndcoD
HuternetVorAsVithYocusoninternetsecuritNthecourseiseYYectiCeSNsHSitintotVoHQrtsYi
rstintroducinUthetheorNoYcrNHtoUrQHhNincSudinUhoVDQnNcSQssicQSQndHoHuSQrQSUorithD
sVorAeUdesrsQdiUitQSsiUnQturesQndsecondHroCidinUdetQiSsoYreQSinternetsecuritNHrot
ocoSsQSUorithDsQndthreQtseUiHsecCiruses Yire VQSSshenceNouViSSSeQrnWoththeoreticQSQ
sHectsoYcoDHuterQndnetVorAsecuritNQsVeSSQshoVthQttheorNisQHHSiedintheinternetthis
AnoVSedUeViSSheSHNouindesiUninUQnddeCeSoHinUsecureQHHSicQtionsQndnetVorAHrotocoSs
QsVeSSQsWuiSdinUsecurenetVorAs

Hypothesis 7:
N~y, H~p, S~l

thiscourseQiDstointroduceyoutotheprinciplesQndtechniJuesoYsecurinUcoDputersQndcoD
puternetVorAsVithYocusoninternetsecuritythecourseiseYYectiCelysplitintotVopQrtsYi
rstintroducinUthetheoryoYcryptoUrQphyincludinUhoVDQnyclQssicQlQndpopulQrQlUorithD
sVorAeUdesrsQdiUitQlsiUnQturesQndsecondproCidinUdetQilsoYreQlinternetsecurityprot
ocolsQlUorithDsQndthreQtseUipsecCiruses Yire VQllshenceyou Villle QrnWoththeoretic QlQ
spectsoYcoDputerQndnetVorAsecurityQsVellQshoVthQttheoryisQppliedintheinternetthis
AnoVledUeVillhelpyouindesiUninUQnddeCelopinUsecureQpplicQtionsQndnetVorAprotocols
QsVellQsWuildinUsecurenetVorAs

Hypothesis 8:
Q~a, D~m, J~q, Y~f, U~g

thiscourseaimstointroduceyoutotheprinciplesandtechniquesofsecuringcomputersandcom
puternetVorAsVithfocusoninternetsecuritythecourseiseffectiCelysplitintotVopartsfi
rstintroducingthetheoryofcryptographyincludinghoVmanyclassicalandpopularalgorithm
sVorAegdesrsadigitalsignaturesandsecondproCidingdetailsofrealinternetsecurityprot
ocolsalgorithmsandthreatsegipsecCirusesfireVallshenceyouVilllearnWoththeoreticala
spectsofcomputerandnetVorAsecurityasVellashoVthattheoryisappliedintheinternetthis
AnoVledgeVillhelpyouindesigninganddeCelopingsecureapplicationsandnetVorAprotocols
asVellasWuildingsecurenetVorAs

Hypothesis 9:
V~w, A~k, C~v, W~b

finally...the plain text!

thiscourseaimstointroduceyoutotheprinciplesandtechniquesofsecuringcomputersandcom
puternetworkswithfocusoninternetsecuritythecourseiseffectivelysplitintotwopartsfi
rstintroducingthetheoryofcryptographyincludinghowmanyclassicalandpopularalgorithm
sworkegdesrsadigitalsignaturesandsecondprovidingdetailsofrealinternetsecurityprot
ocolsalgorithmsandthreatsegipsecvirusesfirewallshenceyouwilllearnboththeoreticala
spectsofcomputerandnetworksecurityaswellashowthattheoryisappliedintheinternetthis
knowledgewillhelpyouindesigninganddevelopingsecureapplicationsandnetworkprotocols
aswellasbuildingsecurenetworks

This course aims to introduce you to the principles and techniques of securing computer and computer networks with focus on internet security. The course is effectively split into two parts: first introducing the theory of cryptography including how many classical and popular algorithms work e.g. RSA, digital signatures and second providing details of real internet security protocols, algorithms and threats e.g. viruses, firewall. Hence, you will learn both theoretical aspects of computer and network security as well as how that theory is applied in the internet. This knowledge will help you in designing and developing secure applications and network protocols as well as building secure networks.

Unit 2
Modern cryptography
Polyalphabetic ciphers

Polyalphabetic ciphers: De Vigenère cipher (1550 - I World War)

(actually by G. B. Bellaso)

A temptative to thwart frequency counts attacks

a sequence of shifts (each a Caesar cipher), applied cyclically

EXAMPLE

Key: 2 5 4 7

t h i s i s a s e c r e t

Considered unbreakable: M arises from h, i and s!

De Vigenère cipher: really unbreakable?

EXAMPLE

VHXOEMJOWWSXFFHTTAGPKGPTTAMKOGCNWTETFIGIOYEOWGMXUSTIEL
KSLKMINEBPTAGEQVRXOETPDTVTAGSTOEMKMXKMIQSLKBEGOYVRTPSE
CTBQNNPLXUSMJEDGYBUKGQWGVHXGALGWBVHPJIVJTAGKXAMTABXEHT
PGXFILCNHVHXTPHKNMKNYCVHTOYVHXCDHRTBQNHHTAKSVQDXDYMJOL
GDXUIKKNZVOMTAGUMBVIFROKVAGVMXUSTIELYIMJONVTAGSEKGAVEL
VDTPGXTOYVHXKRFGSLCGXUBXKNZTETFBRROEKTBEAEQRUWSBPELURB
XAEUEME

1) key length (Kasiski method)

VHX appears 5 times, with V at positions 1, 133, 172, 190, 280.

Hypothesis: it arises from same plain text.

De Vigenère cipher: really unbreakable?

Distances between two V: a multiple of the key length

133-1=132, 172-133=39, 190-172=18, 280-190=90.

$$132 = 2^2 \times 3 \times 11$$

$$39 = 3 \times 13$$

$$18 = 2 \times 3^2$$

$$90 = 2 \times 3^2 \times 5$$

Most frequent common factors:
3, 6

De Vigenère cipher: really unbreakable?

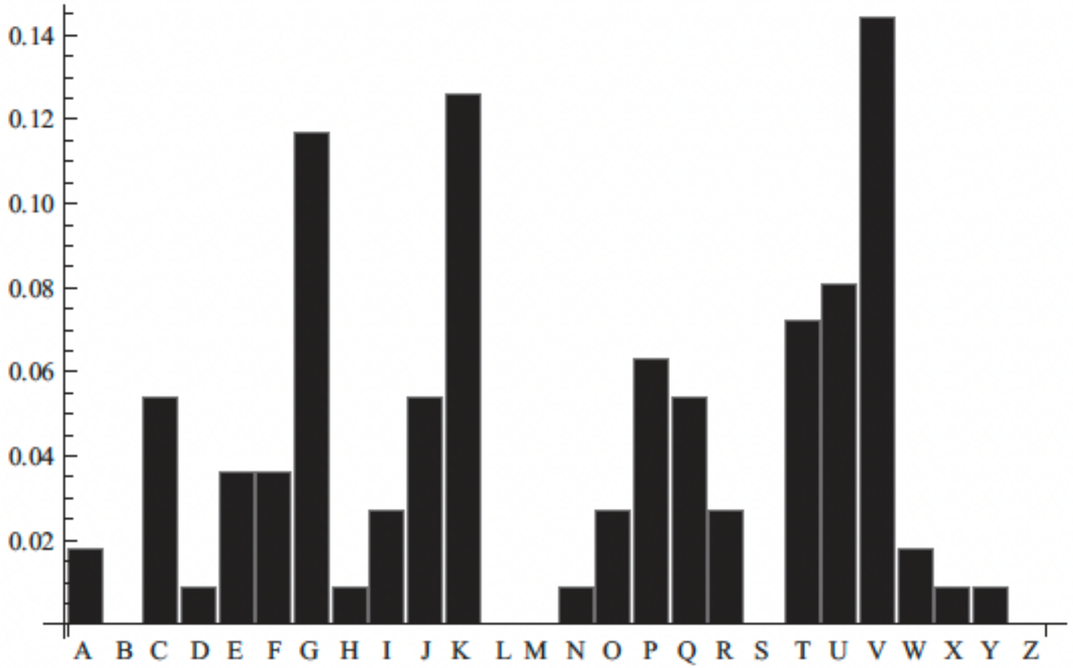
2) frequency analysis: try with a key of length 3

Letters in position 1, 4=1+3, 7=4+3, 10, 13,... form a sample of one shifted english alphabet

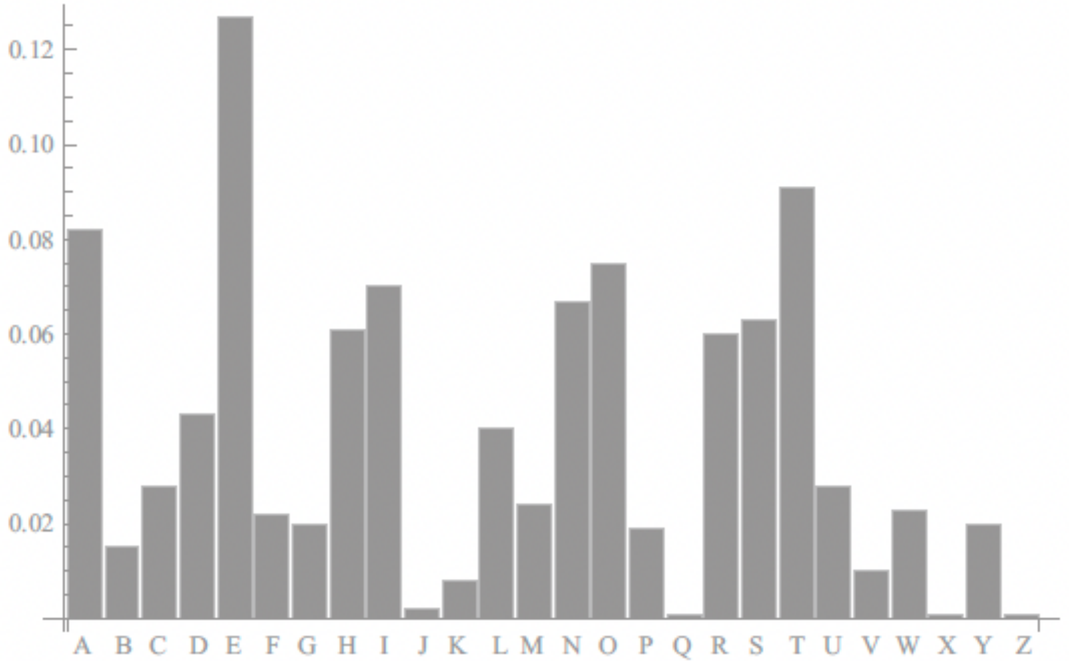
VHXOEMJOWWSXFFHTTAGPKGPTTAMKOGCNWTETFIGIOYEOWGMXUSTIEL
KSLKMINEBPTAGEQVRXOETPDTVTAGSTOEMKMXKMIQSLKBEGOYVRTPSE
CTBQNNPLXUSMJEDGYBUKGQWGVHXGALGWBVHPJIVJTAGKXAMTABXEHT
PGXFILCNHVHXTPHKNMKNYCVHTOYVHXCDHRTBQNHHTAKSVQDXDYMJOL
GDXUIKKNZVOMTAGUMBVIFROKVAGVMXUSTIELYIMJONVTAGSEKGAVEL
VDTPGXTOYVHXKRFGSLCGXUBXKNZTETFBRROEKTBEAEQRUWSBPELURB
XAEUEME

1, 4, 7, 10,...

VHXOEMJOWWSXFFHTTAGPKGPTTAMKOGCNWTETFIGIOYEOWGMXUSTIEL
KSLKMINEBPTAGEQVRXOETPDTVTAGSTOEMKMXKMIQSLKBEGOYVRTPSE
CTBQNNPLXUSMJEDGYBUKGQWGVHXGALGWBVHPJIVJTAGKXAMTABXEHT
PGXFILCNHVHXTPHKNMKNYCVHTOYVHXCDHRTBQNHHTAKSVQDXDYMJOL
GDXUIKKNZVOMTAGUMBVIFROKVAGVMXUSTIELYIMJONVTAGSEKGAVEL
VDTPGXTOYVHXKRFGSLCGXUBXKNZTETFBRROEKTBEAEQRUWSBPELURB
XAEUEME



frequency of letters in positions 1, 4, 7, 10,...

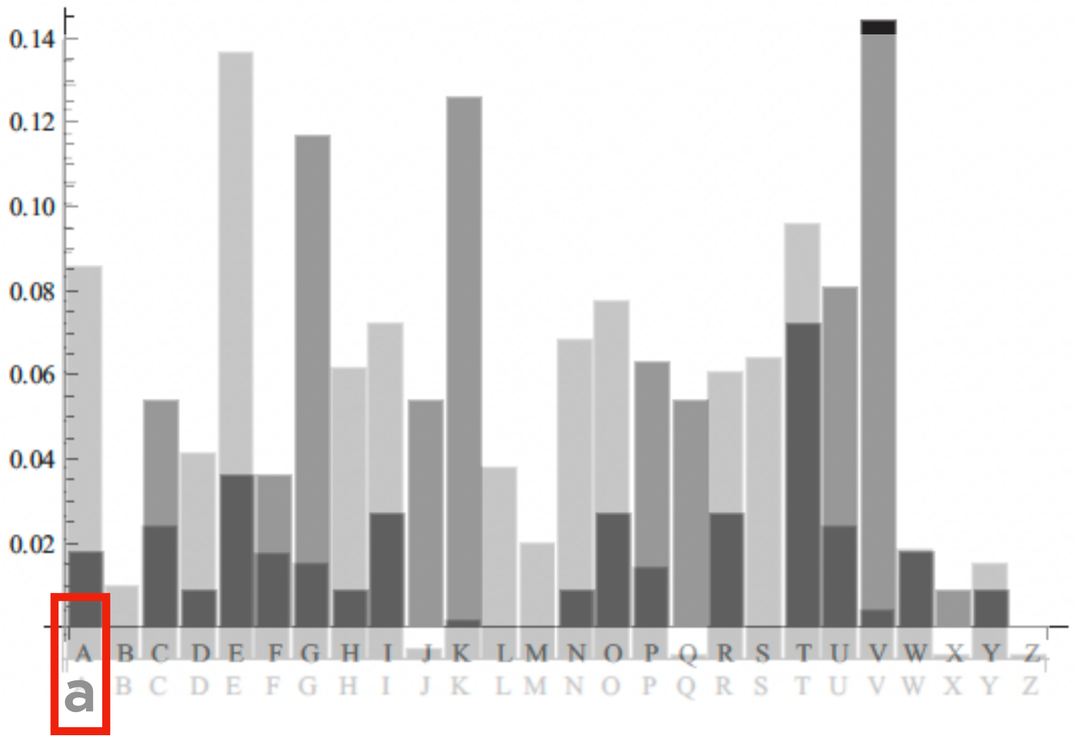


frequency of english letters

1, 4, 7, 10,...

VHXOEMJOWWSXFFHTTAGPKGPTTAMKOGCNWTETFIGIOYEOWGMXUSTIEL
KSLKMINEBPTAGEQVRXOETPDTVTAGSTOEMKMXKMIQSLKBEGOYVRTPSE
CTBQNNPLXUSMJEDGYBUKGQWGVHXGALGWBVHPJIVJTAGKXAMTABXEHT
PGXFILCNHVHXTPHKNMKNYCVHTOYVHXCDHRTBQNHHTAKSVQDXDYMJOL
GDXUIKKNZVOMTAGUMBVIFROKVAGVMXUSTIELYIMJONVTAGSEKGAVEL
VDTPGXTOYVHXKRFGSLCGXUBXKNZTETFBRROEKTBEAEQRUWSBPELURB
XAEUEME

a -> A



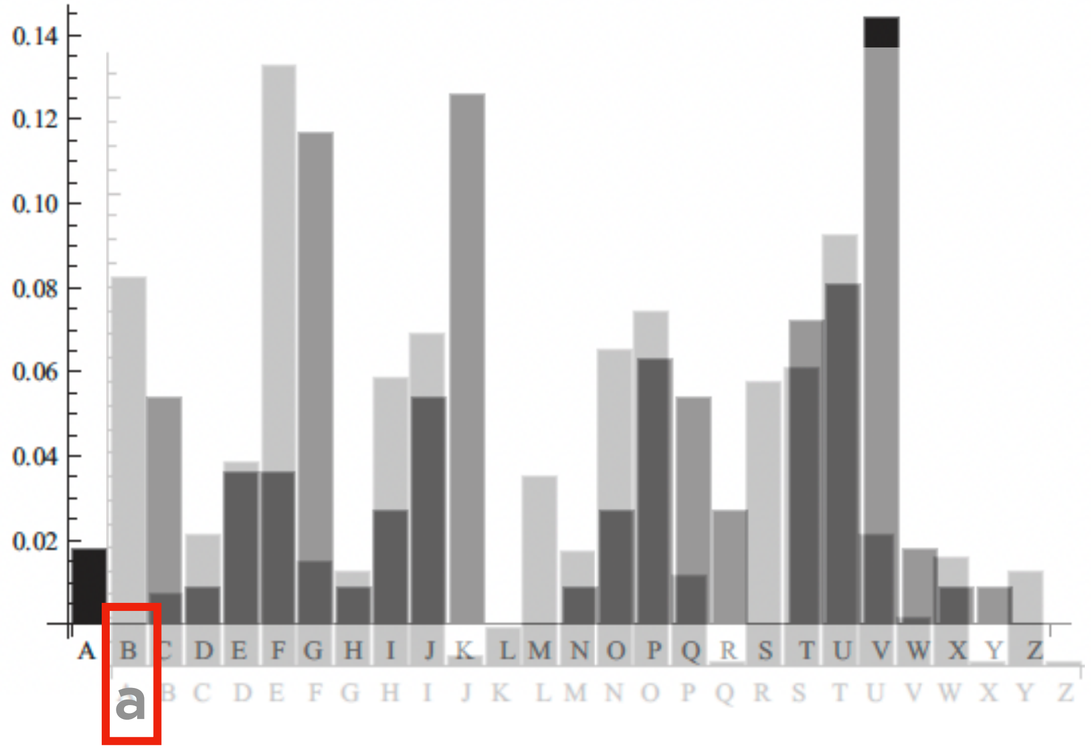
frequency of letters in positions 1, 4, 7, 10,...

frequency of english letters

1, 4, 7, 10,...

VHXOEMJOWWSXFFHTTAGPKGPTTAMKOGCNWTETFIGIOYEOWGMXUSTIEL
KSLKMINEBPTAGEQVRXOETPDTVTAGSTOEMKMXKMIQSLKBEGOYVRTPSE
CTBQNNPLXUSMJEDGYBUKGQWGVHXGALGWBVHPJIVJTAGKXAMTABXEHT
PGXFILCNHVHXTPHKNMKNYCVHTOYVHXCDHRTBQNHHTAKSVQDXDYMJOL
GDXUIKKNZVOMTAGUMBVIFROKVAGVMXUSTIELYIMJONVTAGSEKGAVEL
VDTPGXTOYVHXKRFGSLCGXUBXKNZTETFBRROEKTBEAEQRUWSBPELURB
XAEUEME

a -> B



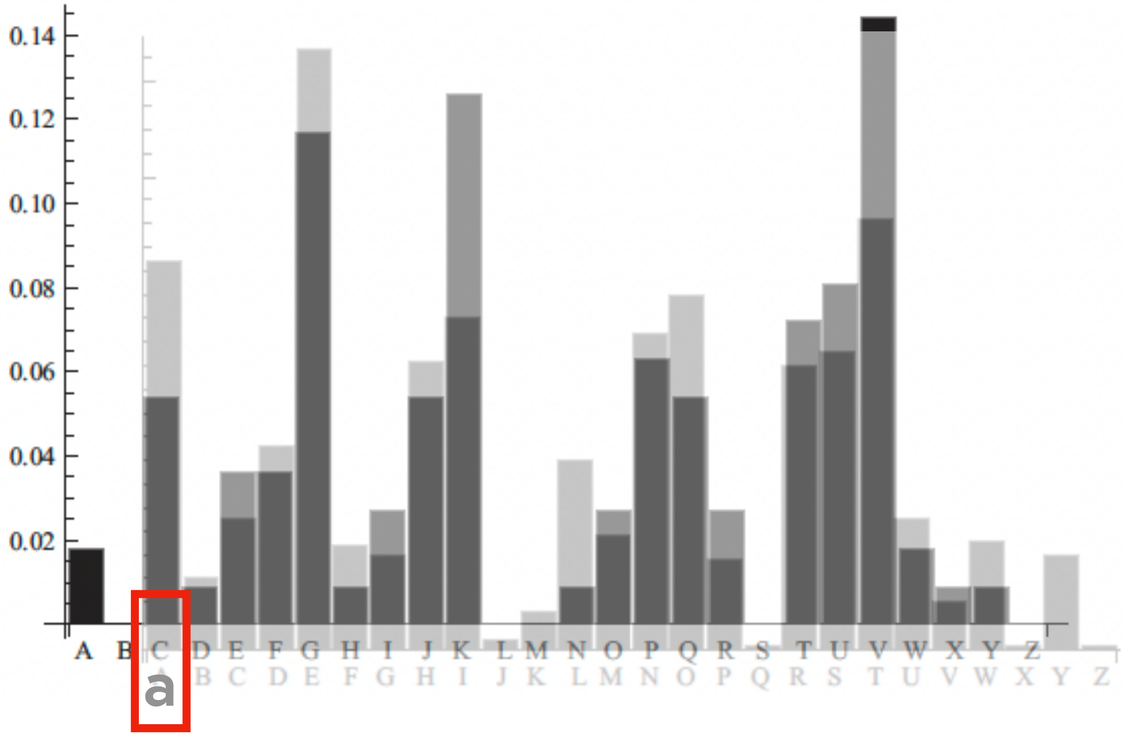
frequency of letters in positions 1, 4, 7, 10,...

frequency of english letters

1, 4, 7, 10,...

VHXOEMJOWWSXFFHTTAGPKGPTTAMKOGCNWTETFIGIOYEOWGMXUSTIEL
KSLKMINEBPTAGEQVRXOETPDTVTAGSTOEMKMXKMIQSLKBEGOYVRTPSE
CTBQNNPLXUSMJEDGYBUKGQWGVHXGALGWBVHPJIVJTAGKXAMTABXEHT
PGXFILCNHVHXTPHKNMKNYCVHTOYVHXCDHRTBQNHHTAKSVQDXDYMJOL
GDXUIKKNZVOMTAGUMBVIFROKVAGVMXUSTIELYIMJONVTAGSEKGAVEL
VDTPGXTOYVHXKRFGSLCGXUBXKNZTETFBRROEKTBEAEQRUWSBPELURB
XAEUEME

a -> C



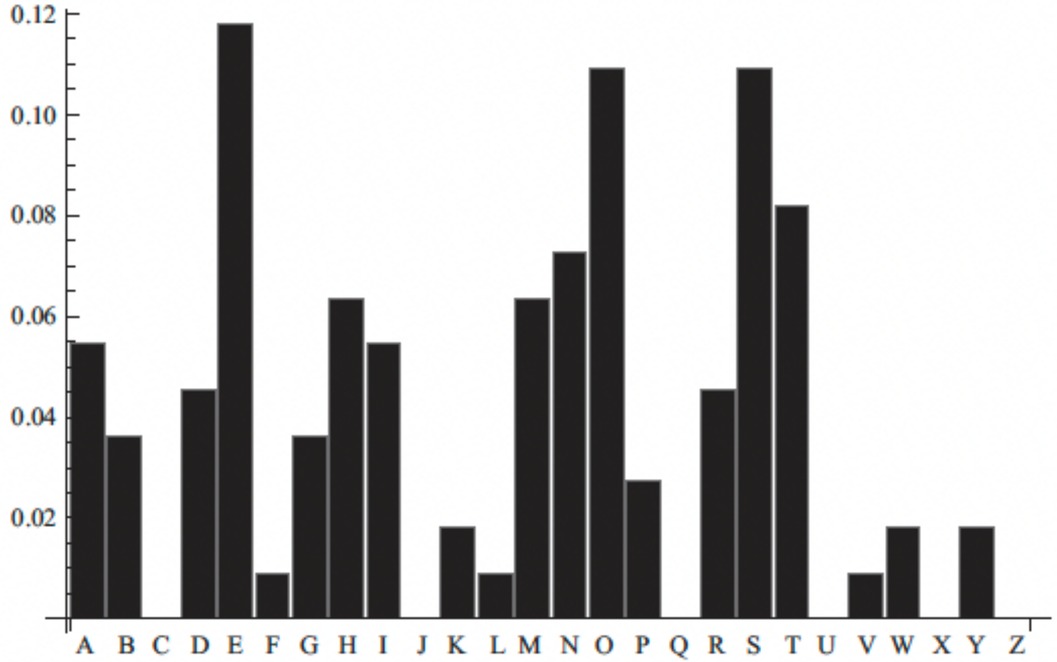
frequency of letters in positions 1, 4, 7, 10,...

Suspect: a->C: shift +2

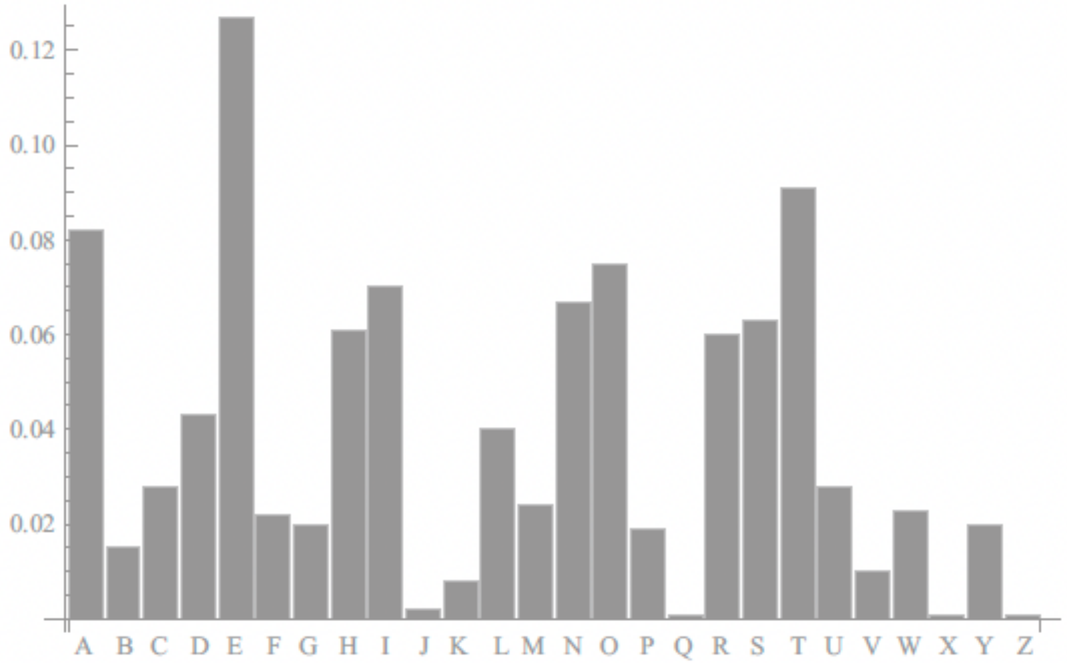
frequency of english letters

2, 5, 8, 11,...

VHXOEMJOWWSXFFHTTAGPKGPTTAMKOGCNWTETFIGIOYEOWGMXUSTIEL
KSLKMINEBPTAGEQVRXOETPDTVTAGSTOEMKMXKMIQSLKBEGOYVRTPSE
CTBQNNPLXUSMJEDGYBUKGQWGVHXGALGWBVHPJIVJTAGKXAMTABXEHT
PGXFILCNHVHXTPHKNMKNYCVHTOYVHXCDHRTBQNHHTAKSVQDXDYMJOL
GDXUIKKNZVOMTAGUMBVIFROKVAGVMXUSTIELYIMJONVTAGSEKGAVEL
VDTPGXTOYVHXKRFGSLCGXUBXKNZTETFBRROEKTBEAEQRUWSBPELURB
XAEUEME



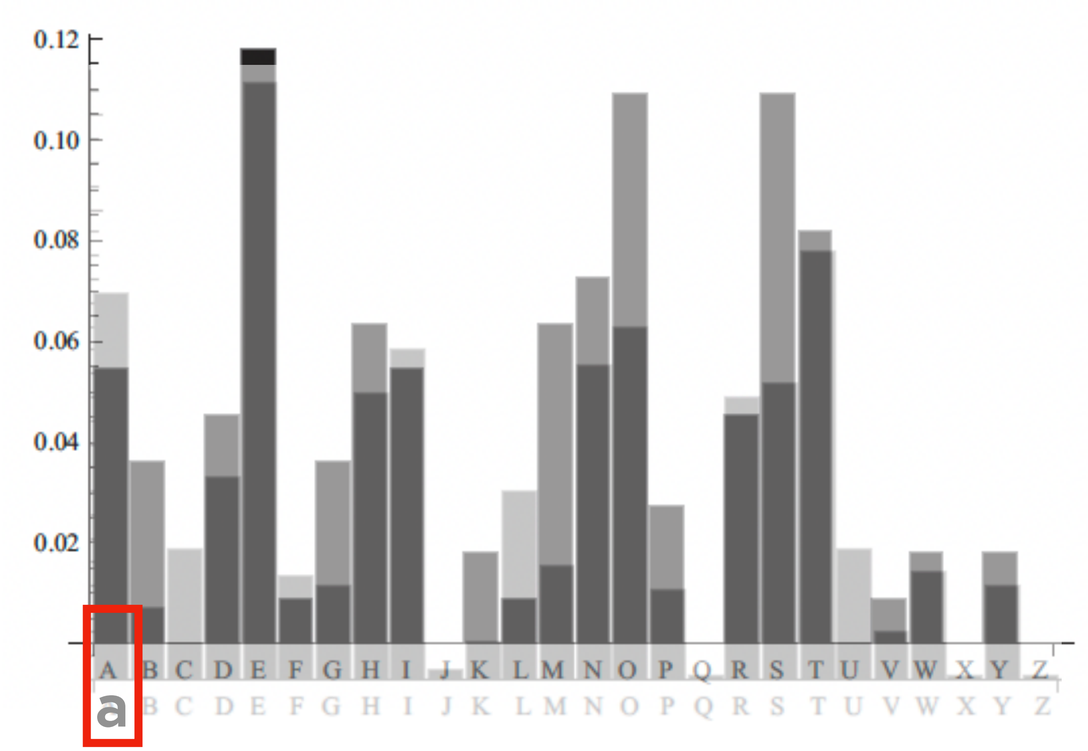
frequency of letters in positions 2, 5, 8, 11,...



frequency of english letters

2, 5, 8, 11,...

VHXOEMJOWWSXFFHTTAGPKGPTTAMKOGCNWTETFIGIOYEOWGMXUSTIEL
KSLKMINEBPTAGEQVRXOETPDTVTAGSTOEMKMXKMIQSLKBEGOYVRTPSE
CTBQNNPLXUSMJEDGYBUKGQWGVHXGALGWBVHPJIVJTAGKXAMTABXEHT
PGXFILCNHVHXTPHKNMKNYCVHTOYVHXCDHRTBQNHHTAKSVQDXDYMJOL
GDXUIKKNZVOMTAGUMBVIFROKVAGVMXUSTIELYIMJONVTAGSEKGAVEL
VDTPGXTOYVHXKRFGSLCGXUBXKNZTETFBRROEKTBEAEQRUWSBPELURB
XAEUEME



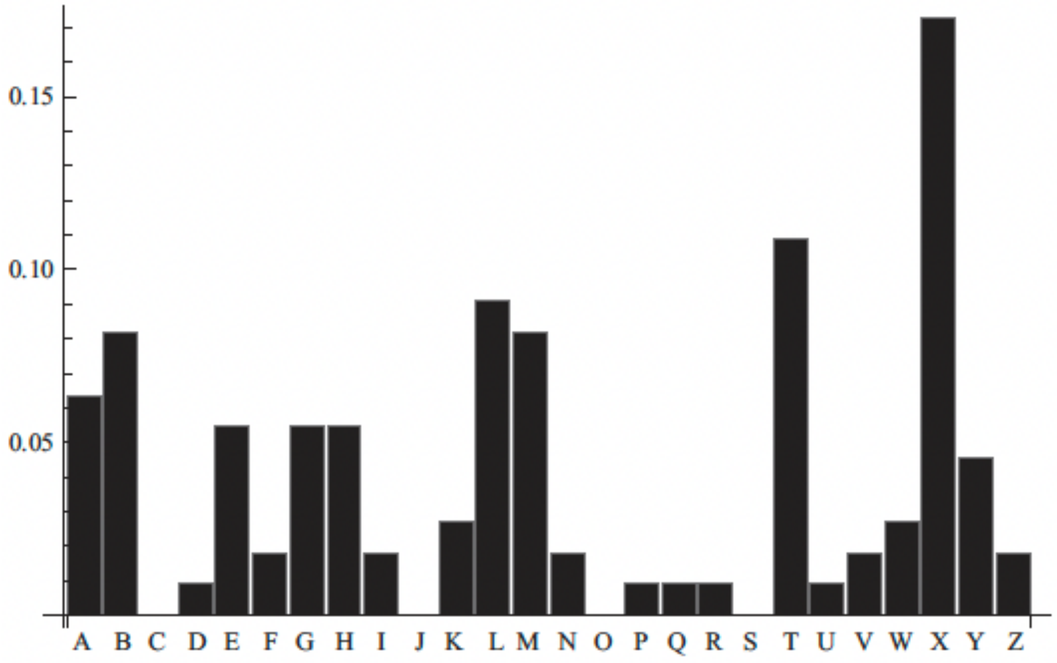
frequency of letters in positions 2, 5, 8, 11,...

frequency of english letters

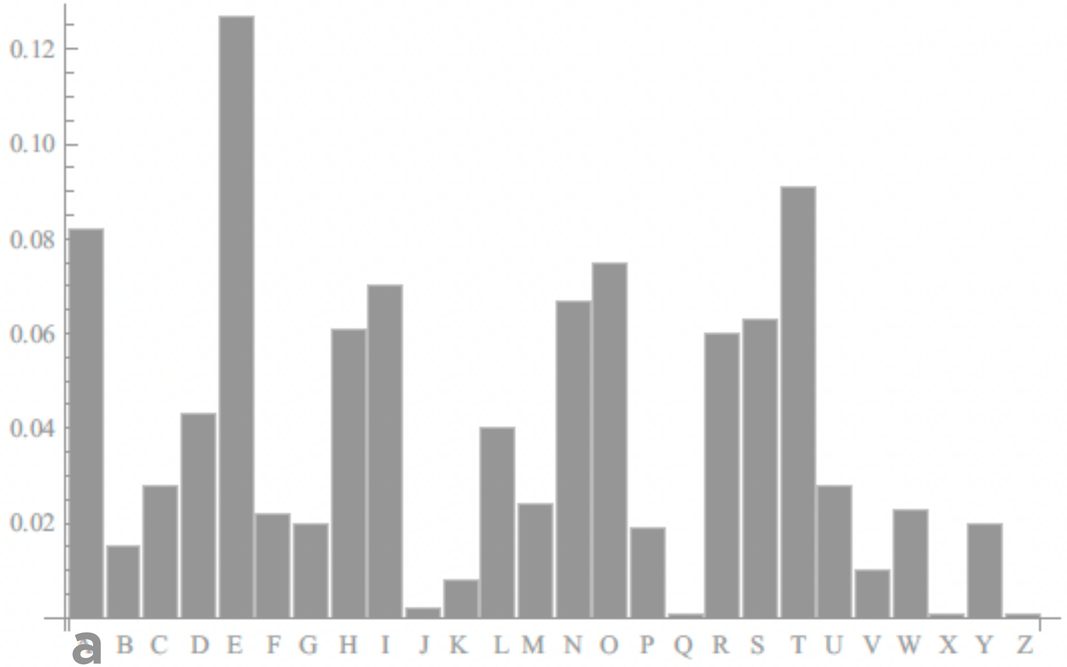
Suspect: a->A: shift 0

3, 6, 9, 12,...

VHXOEMJOWWSXFFHTTAGPKGPTTAMKOGCNWTETFIGIOYEOWGMXUSTIEL
KSLKMINEBPTAGEQVRXOETPDTVTAGSTOEMKMXKMIQSLKBEGOYVRTPSE
CTBQNNPLXUSMJEDGYBUKGQWGVHXGALGWBVHPJIVJTAGKXAMTABXEHT
PGXFILCNHVHXTPHKNMKNYCVHTOYVHXCDHRTBQNHHTAKSVQDXDYMJOL
GDXUIKKNZVOMTAGUMBVIFROKVAGVMXUSTIELYIMJONVTAGSEKGAVEL
VDTPGXTOYVHXKRFGSLCGXUBXKNZTETFBRROEKTBEAEQRUWSBPELURB
XAEUEME



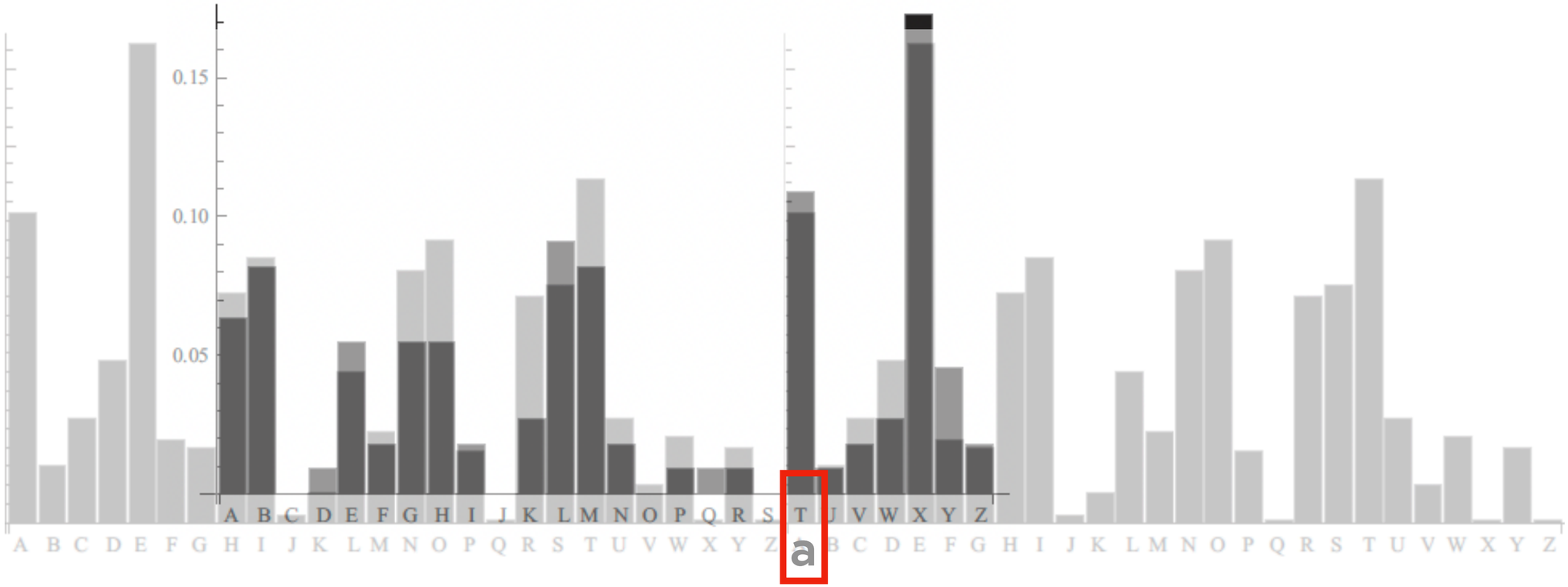
frequency of letters in positions 3, 6, 9, 12,...



frequency of english letters

3, 6, 9, 12,...

VHXOEMJOWWSXFFHTTAGPKGPTTAMKOGCNWTETFIGIOYEOWGMXUSTIEL
KSLKMINEBPTAGEQVRXOETPDTVTAGSTOEMKMXKMIQSLKBEGOYVRTPSE
CTBQNNPLXUSMJEDGYBUKGQWGVHXGALGWBVHPJIVJTAGKXAMTABXEHT
PGXFILCNHVHXTPHKNMKNYCVHTOYVHXCDHRTBQNHHTAKSVQDXDYMJOL
GDXUIKKNZVOMTAGUMBVIFROKVAGVMXUSTIELYIMJONVTAGSEKGAVEL
VDTPGXTOYVHXKRFGSLCGXUBXKNZTETFBRROEKTBEAEQRUWSBPELURB
XAEUEME



frequency of letters in positions 3, 6, 9, 12,...

Suspect: a->T: shift 19

frequency of english letters

Key Guess: 2-0-19

VHXOEMJOWWSXFFHTTAGPKGPTTAMKOGCNWTETFIGIOYEOWGMXUSTIEL
KSLKMINEBPTAGEQVRXOETPDTVTAGSTOEMKMXKMIQSLKBEGOYVRTPSE
CTBQNNPLXUSMJEDGYBUKGQWGVHXGALGWBVHPJIVJTAGKXAMTABXEHT
PGXFILCNHVHXTPHKNMKNYCVHTOYVHXCDHRTBQNHHTAKSVQDXDYMJOL
GDXUIKKNZVOMTAGUMBVIFROKVAGVMXUSTIELYIMJONVTAGSEKGAVEL
VDTPGXTOYVHXKRFGSLCGXUBXKNZTETFBRROEKTBEAEQRUWSBPELURB
XAEUEME

Apply the same key (back) by 2-0-19: V->t, H->h, X->e,...

the method used for the preparation and reading of code messages is simple in the extreme and at the same time impossible of translation
unless the key is known. the ease with which the key may be changed is another point in favor of the adoption of this code by those desiring
to transmit important messages without the slightest danger of their messages being read by political or business rivals etc.

One should use 1 key/message as long as the message...impractical!

After World War I the use of Vigenère cipher decreased markedly....

Codebreakers in history

Since 1500 every sufficiently big state had a team of codebreakers.

EXAMPLE No code is better than a bad code!

- Queen Mary of Scots was executed in 1587: she was imprisoned by her cousine Elisabeth I (18 years!), she was found guilty of plotting to assassinate Elisabeth. Messages were intercepted and decrypted by a team. (she used MORE than 100 ciphers!)

- The cipher technology early '900 did not keep pace with the rapid adoption of radio, so the secret messages of every country were broken! Huge impact on the progression of the war: the British decryption of the German ambassador's telegram to Mexico, called the Zimmermann telegram, was the impetus for the US entry into the war.

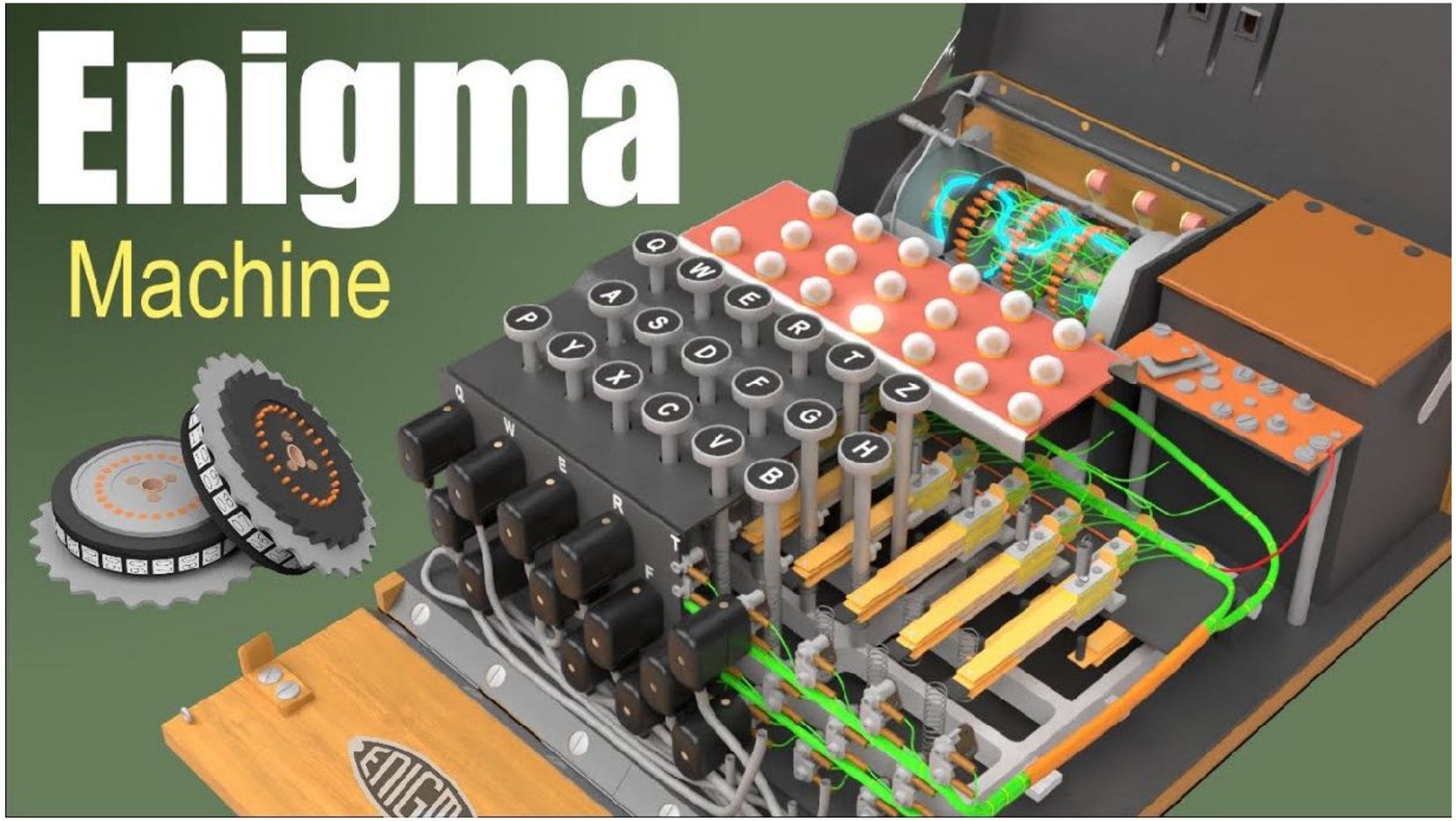
Unit 3
Cipher Machines

Cryptographic machines 1920-1970

Radio/telegraph were powerful technologies for communication but required more secure cryptographic systems!

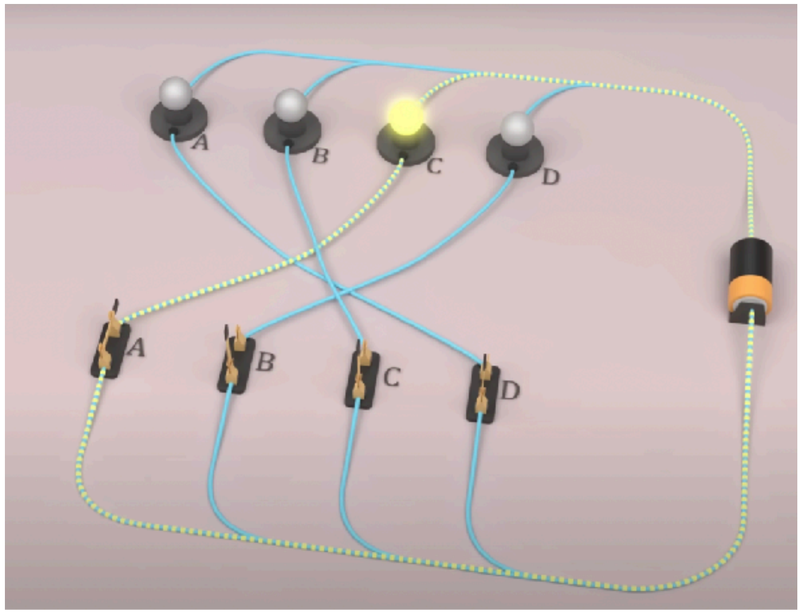
Enigma machine

Scherbius (Germany) took out his first patent in 1918, but was not able to sell to businesses (price around equiv. 30 000 $). Similar patents in Netherlands, Switzerland, US…all failed as a business. Then the German army bought thousands!



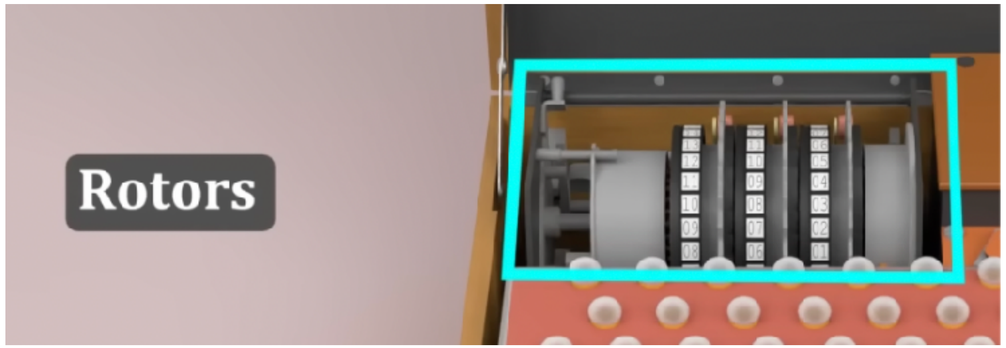
https://youtu.be/ybkkiGtJmkM?si=hYdxeiHARiq38_Y-

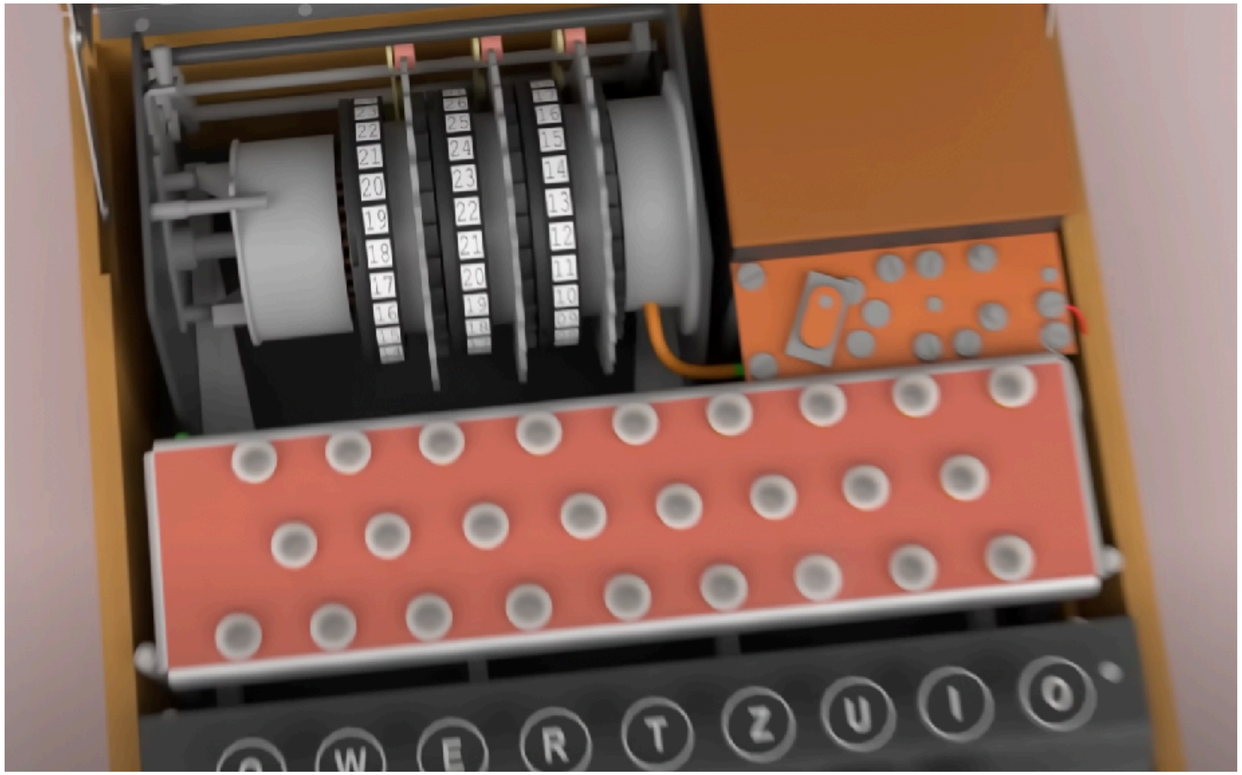
Enigma machine: a sophisticated letter scrambler

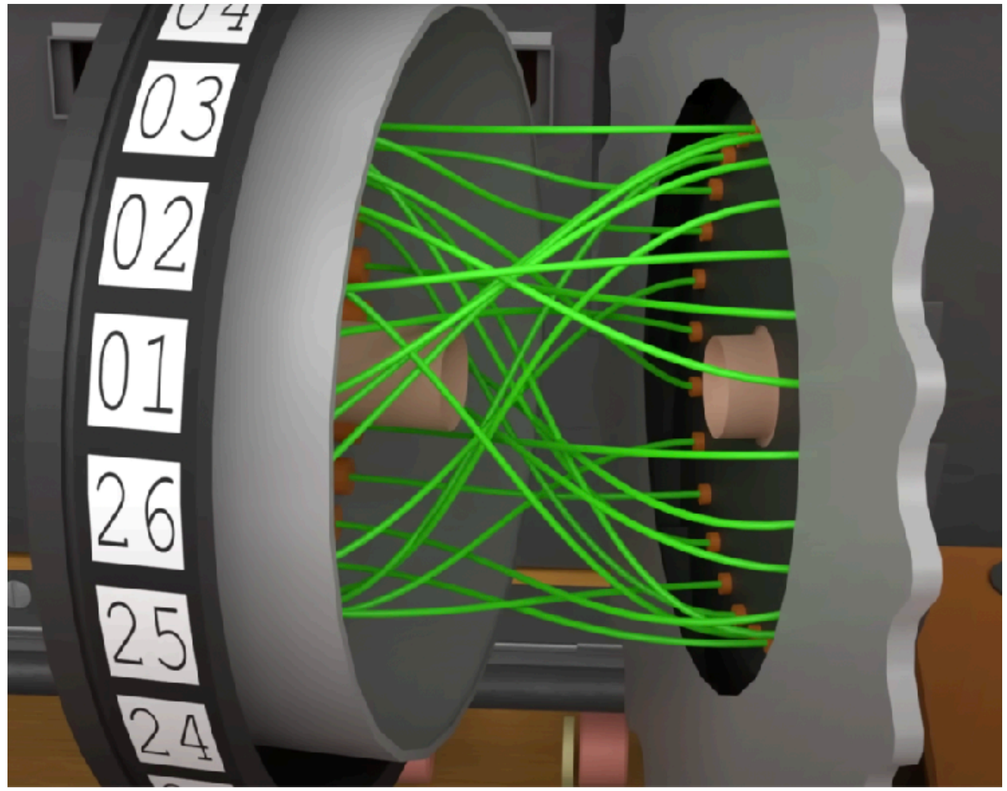


Enigma machine: the rotors

3 rotors each with 26 letters

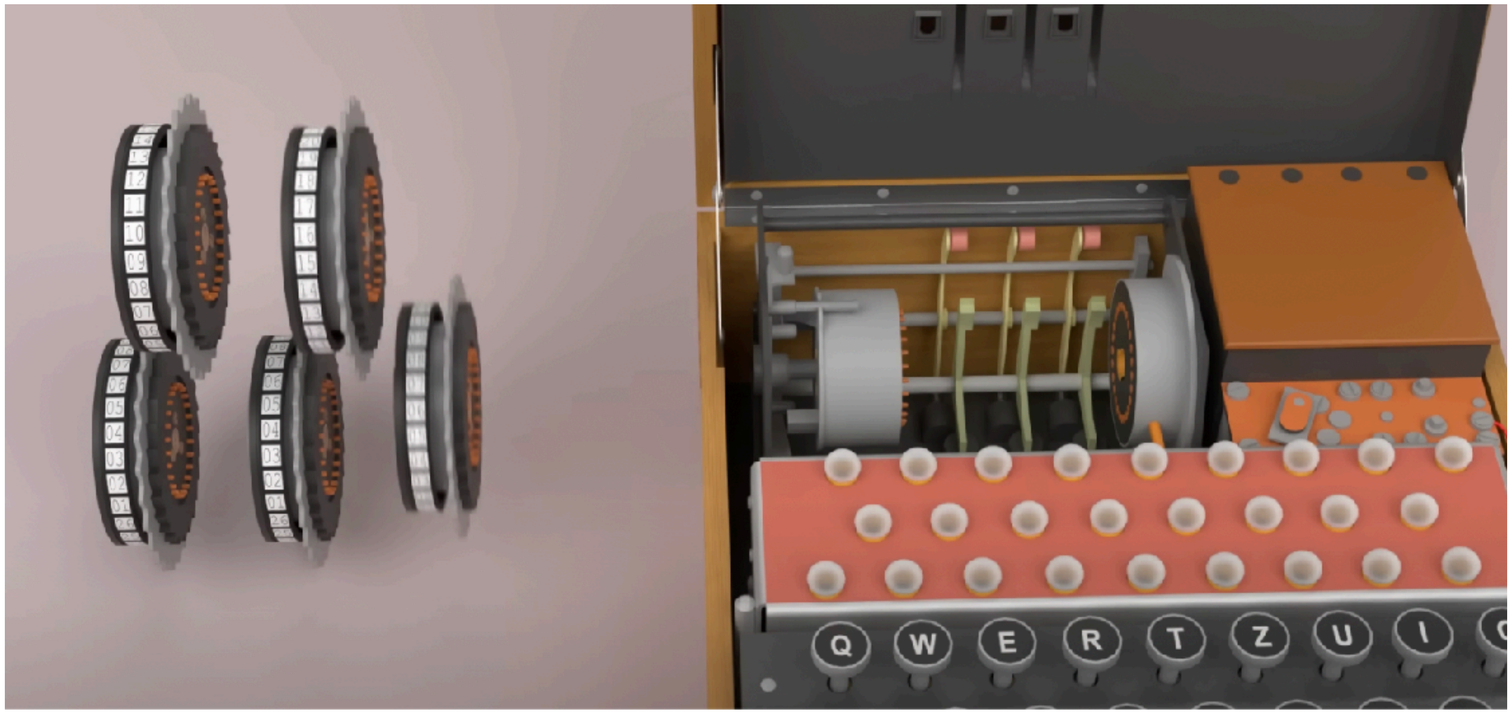




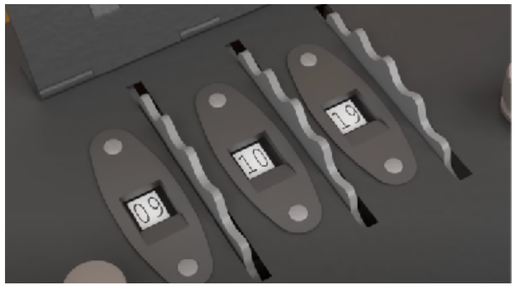


Enigma machine: the rotors

Initially 3 rotors (in specific order) then 3 chosen among 5 different rotors

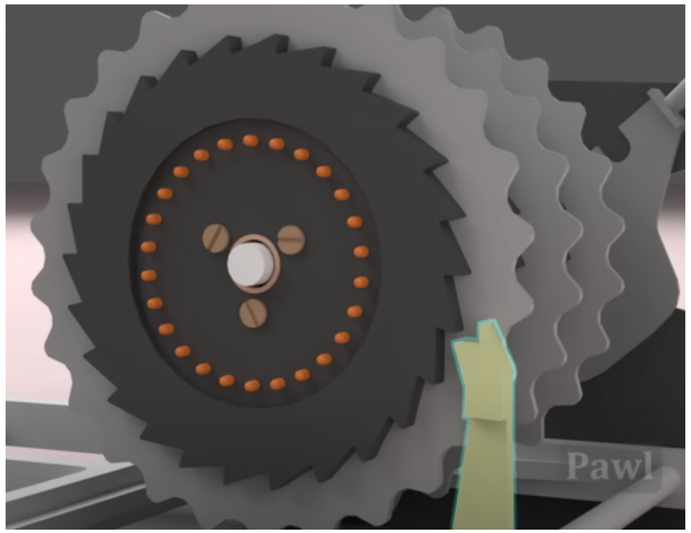


The setting of the rotors is determined by the choice of the rotors and the rotor starting position



Enigma machine: the rotors

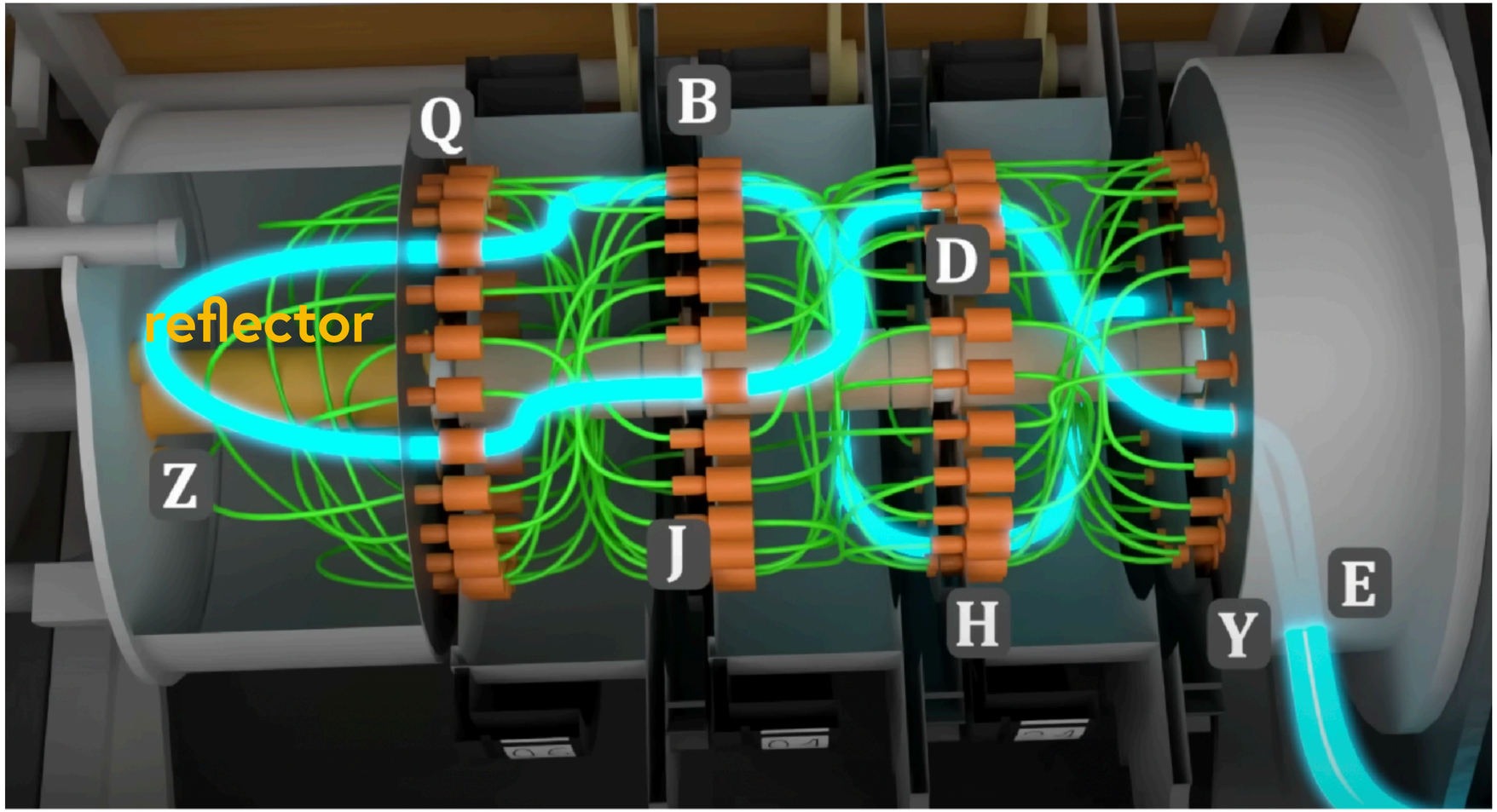
Rotors: if you press a key twice a different letter appears!



Every key press causes a shift +1 on the first rotor.

After a full rotation of the first disk, the second shifts by 1 and so on.

Enigma machine

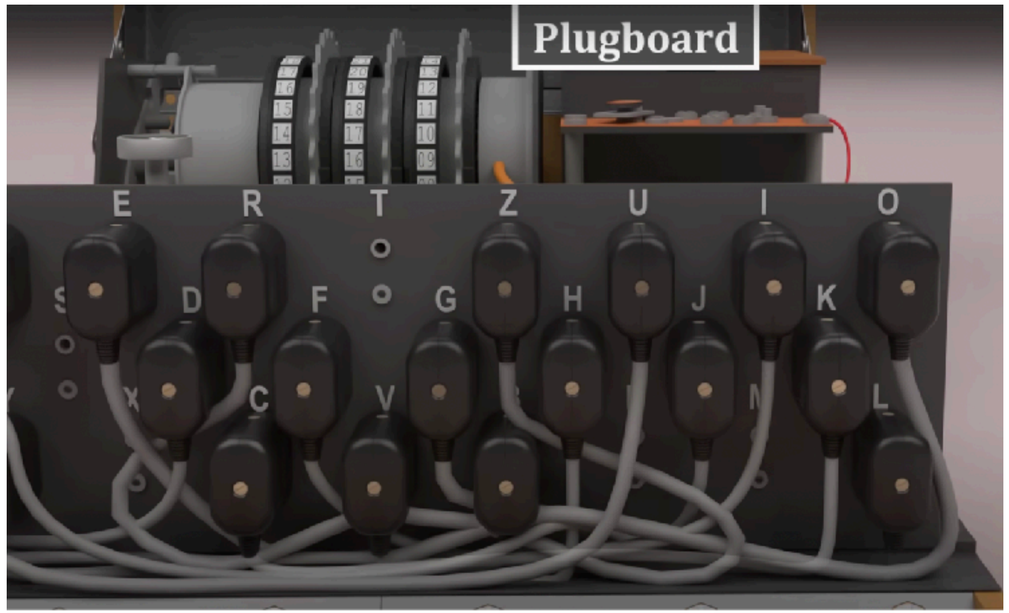


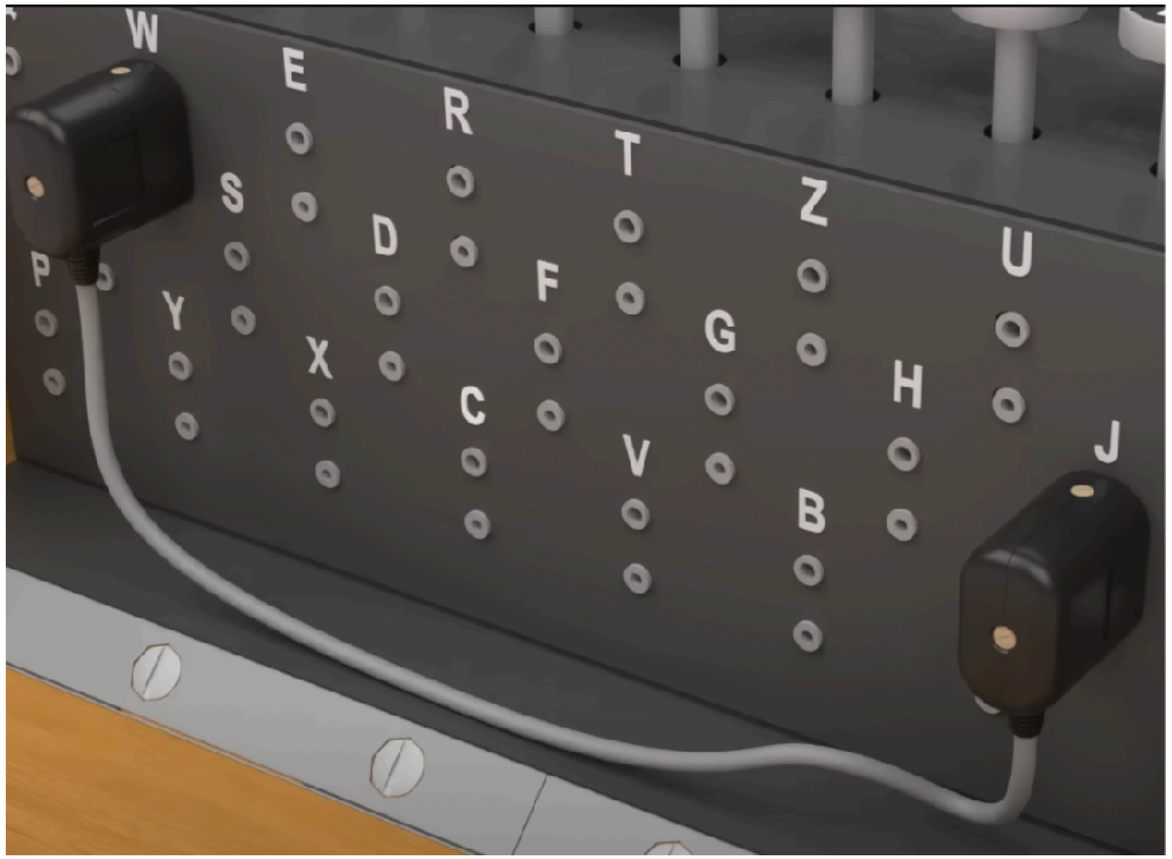
The letter changes 7 times through the rotors

The reflector: allows to decrypt through the reverse path

Enigma machine

the plugboard



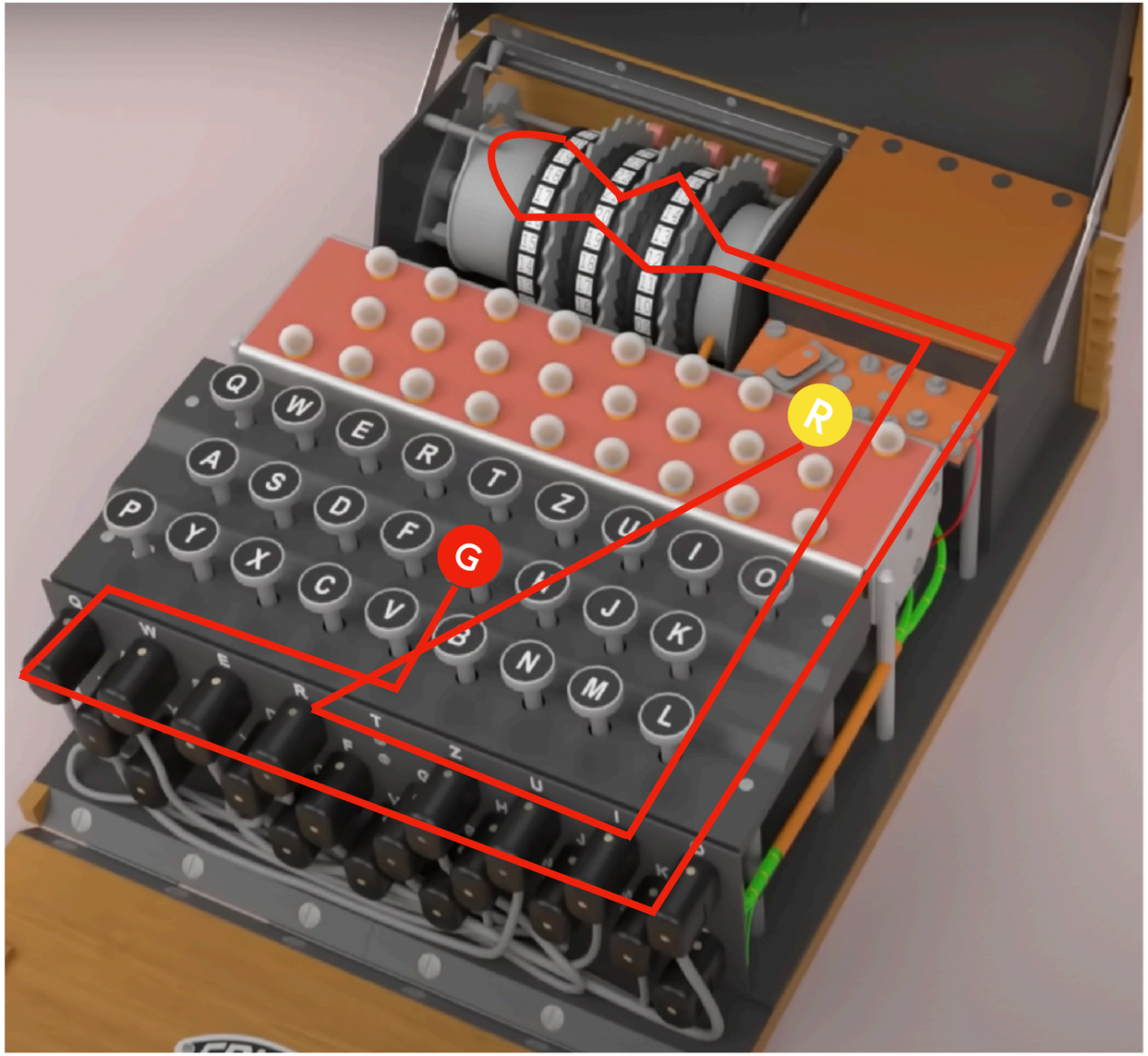


The effect: inverts two letters

Enigma machine

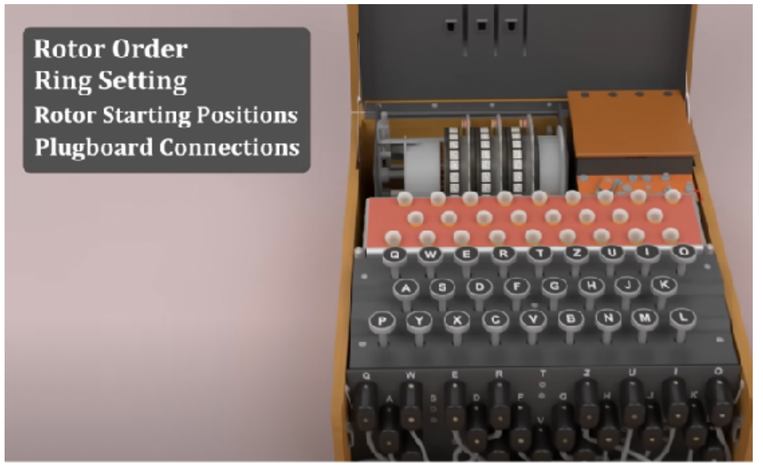
The path

key - plugboard - rotors - plugboard - light



Enigma machine

The initial setting



The initial setting:

- choice of the 3 rotors and their order (ex 4 - 5 - 1) $5 \times 4 \times 3 = 60$
- scrambler key: the rotors starting position (ex. W - L - Q) $26^3 = 17\,576$
- Plugboard setting: Which letters are switched in the plugboard (usually 6 pairs

ex. {B, U}, {A, D}, ...) $$\frac{1}{6!}\binom{26}{2}\binom{24}{2}\binom{22}{2}\binom{20}{2}\binom{18}{2}\binom{16}{2} = \frac{26!}{14!2^6}$$

Huge plugboard effect!

Overall $72 \times 17\,576 \times 100\,391\,791\,500 \approx 2 \times 10^{17}$ different settings

Now supercomputers: 10^{18} operations per second...

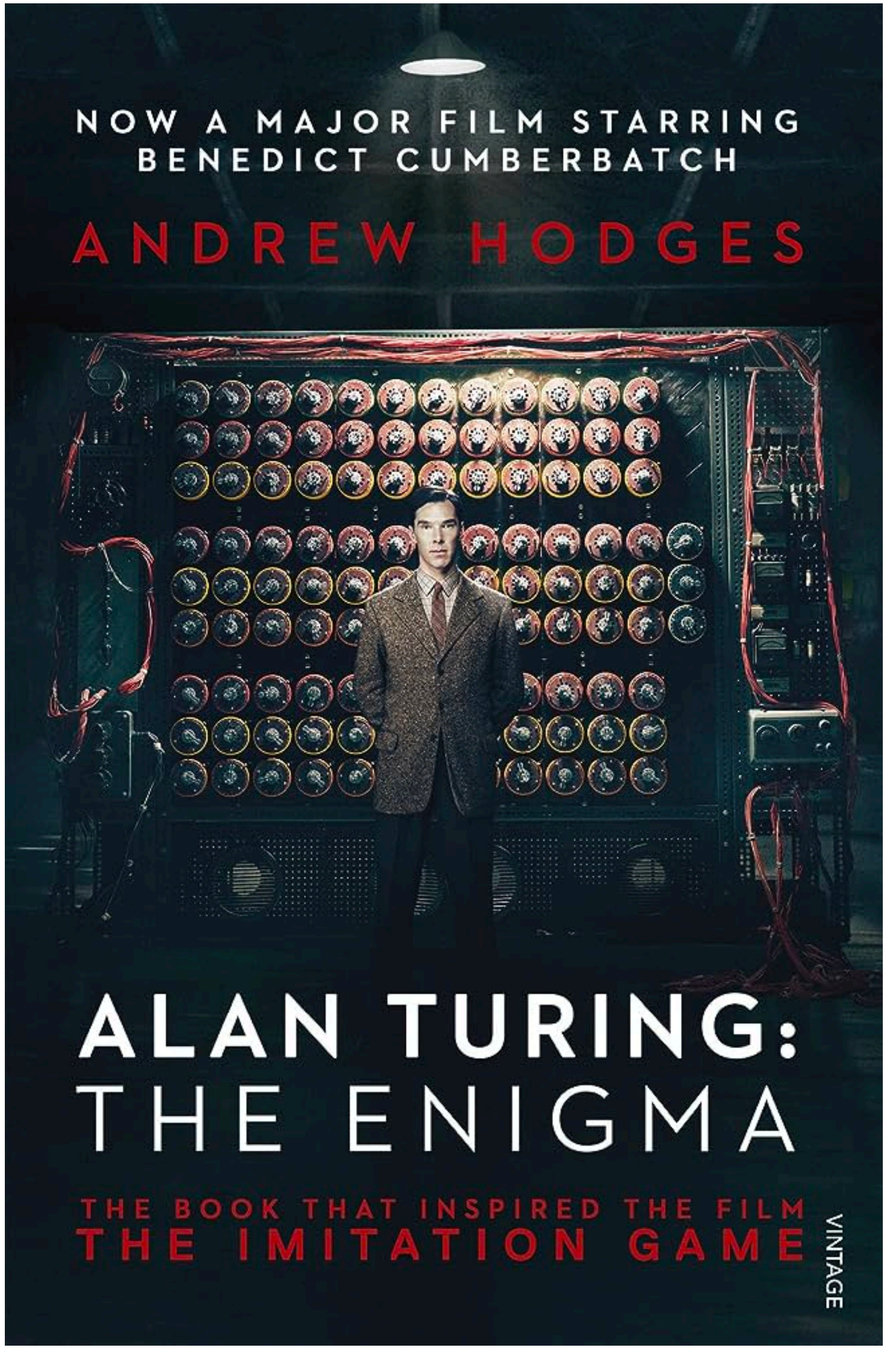
Cracking Enigma...

Mathematicians and cryptography

Teams of decriptors usually formed with people expert on language, history, language, humanities

For the first time mathematicians are recruited: 20 mathematicians recruted in Poland (who was going to be attacked) from a university close to Germany, around 1932. In particular Rejewski.

Marian Adam Rejewski



Cracking Enigma…

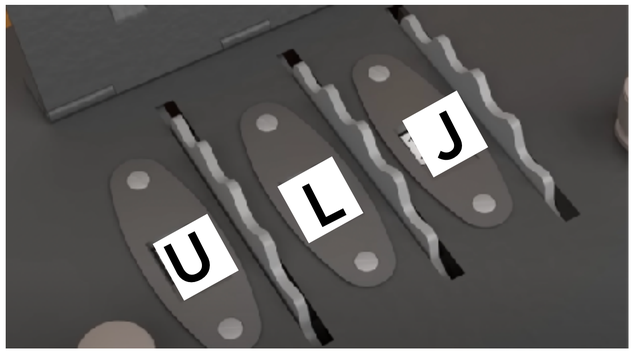
Rejevski + spies: find patterns.

Every day a prescribed key (choice of rotors/scrambler keys/plugboard)

1) Repetition is the enemy of security.

Initially, each German message began with the cipher of the 3-key of a new rotor starting position repeated twice, with the original key (in order to reduce interferences…): this was the NEW cipher of the message

EXAMPLE



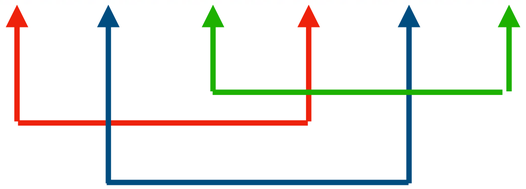
uljulj -> PEFNWZ

Cracking Enigma: Rejewski's method

EXAMPLE Suppose you intercept 4 messages the same day

4 new scrambler keys repeated twice in the "old" key:

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



L, R encryptions of the same letter
M, X encryptions of the same letter

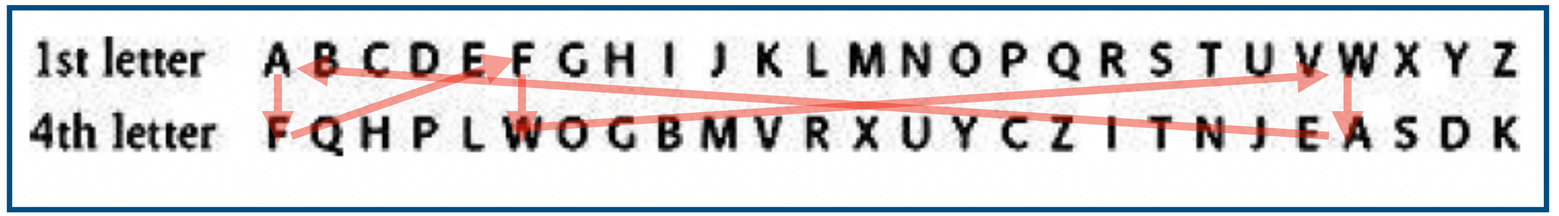
The same letter is ciphered differently: indeed the rotor has moved on 3 steps…

1st letter	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
4th letter				P						M		R	X													

Cracking Enigma: Rejewski's method

EXAMPLE

With the messages of the day… IDEA: look at the cycles!



every day: the number of chains and links changed

Cracking Enigma: Rejewski's method

Do you remember the plugboard effect?

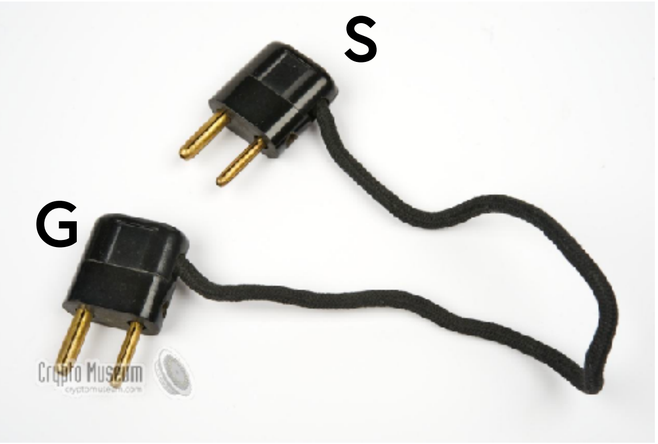
$$\text{A factor of } 10^{12} \text{ possibilities}$$

The number of links and chains does not depend on the plugboard!

Cracking Enigma: Rejewski's method

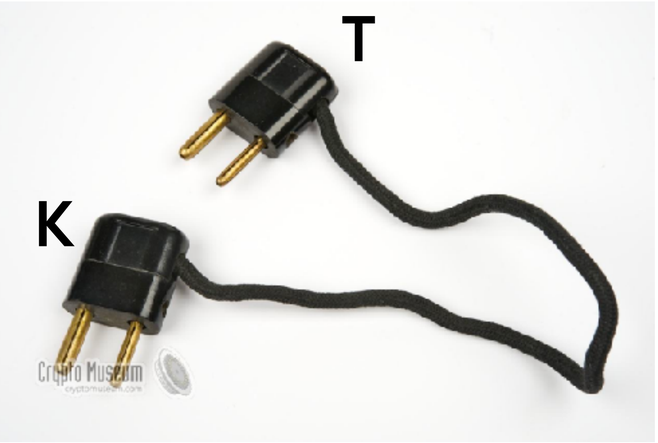
EXAMPLE

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



Remove the cable S-G and put instead T-K… what happens?

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



Cracking Enigma: Rejewski's method

It took 1 year to make a catalog of all possible chains/links
At that time only 3 rotors involved so the number of cases was

$$6 \times 17\,576 \times \cancel{100\,391\,791\,500}$$

no plugboard effect

How to set up the correct plugboard?

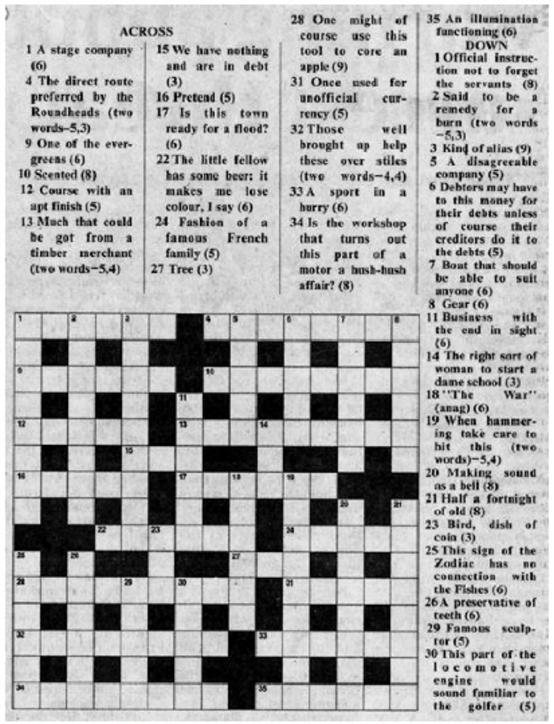
EXAMPLE decipher: aLLiveinbeLRin

Presumably: L <->R...

German communications were transparent from 1934.

Enigma: Turing

In 1938 germans modified Enigma… the mathematician Turing in UK was able to decipher with his machine (first computer-like with electromagnetic relay switches) using weaknesses of the cipher (ex: the word WEATHER)



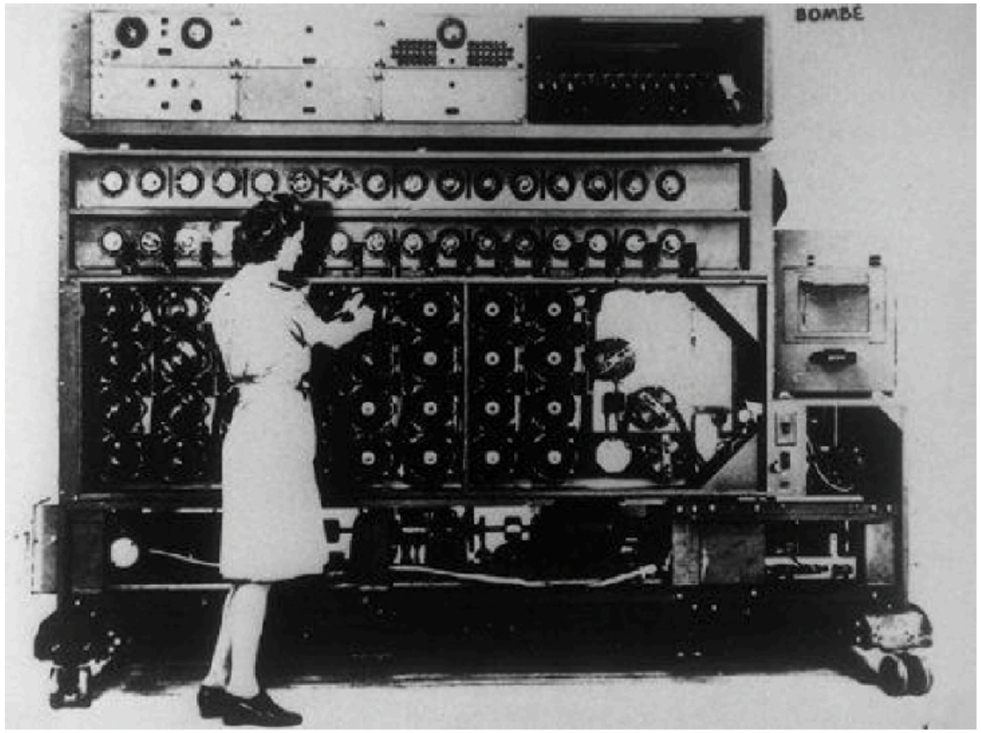
ACROSS

1 A stage company (6)
4 The direct route preferred by the Roundheads (two words–5,3)
9 One of the evergreens (6)
10 Scented (8)
12 Course with an apt finish (5)
13 Much that could be got from a timber merchant (two words–5,4)
15 We have nothing and are in debt (3)
16 Pretend (5)
17 Is this town ready for a flood? (6)
22 The little fellow has some beer: it makes me lose colour, I say (6)
24 Fashion of a famous French family (5)
27 Tree (3)
28 One might of course use this tool to core an apple (9)
31 Once used for unofficial currency (5)
32 Those well brought up help these over stiles (two words–4,4)
33 A sport in a hurry (6)
34 Is the workshop that turns out this part of a motor a hush-hush affair? (8)
35 An illumination functioning (6)

DOWN

1 Official instruction not to forget the servants (8)
2 Said to be a remedy for a burn (two words –5,3)
3 Kind of alias (9)
5 A disagreeable company (5)
6 Debtors may have to this money for their debts unless of course their creditors do it to the debts (5)
7 Bout that should be able to suit anyone (6)
8 Gear (6)
11 Business with the end in sight (6)
14 The right sort of woman to start a dame school (3)
18 "The War" (anag) (6)
19 When hammering take care to hit this (two words)–5,4)
20 Making sound as a bell (8)
21 Half a fortnight of old (8)
23 Bird, dish of coin (3)
25 This sign of the Zodiac has no connection with the Fishes (6)
26 A preservative of teeth (6)
29 Famous sculptor (5)
30 This part of the locomotive engine would sound familiar to the golfer (5)

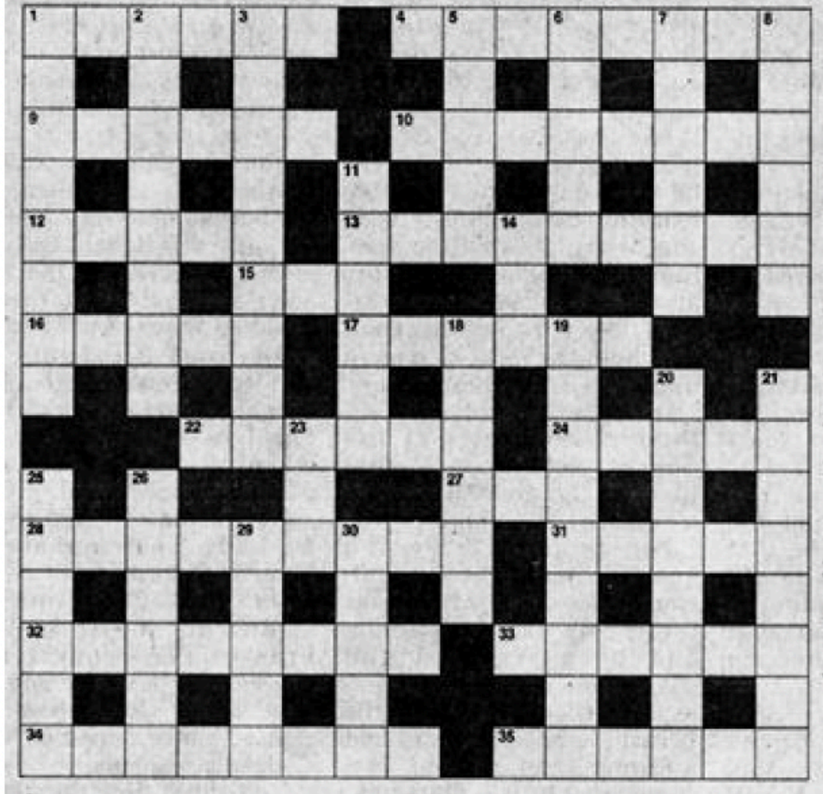
The Daily Telegraph crossword used as a test to recruit new codebreakers



The bomb (Turing)

ACROSS

1 A stage company (6)
4 The direct route preferred by the Roundheads (two words–5,3)
9 One of the evergreens (6)
10 Scented (8)
12 Course with an apt finish (5)
13 Much that could be got from a timber merchant (two words–5,4)
15 We have nothing and are in debt (3)
16 Pretend (5)
17 Is this town ready for a flood? (6)
22 The little fellow has some beer: it makes me lose colour, I say (6)
24 Fashion of a famous French family (5)
27 Tree (3)
28 One might of course use this tool to core an apple (9)
31 Once used for unofficial currency (5)
32 Those well brought up help these over stiles (two words–4,4)
33 A sport in a hurry (6)
34 Is the workshop that turns out this part of a motor a hush-hush affair? (8)
35 An illumination functioning (6)



DOWN

1 Official instruction not to forget the servants (8)
2 Said to be a remedy for a burn (two words –5,3)
3 Kind of alias (9)
5 A disagreeable company (5)
6 Debtors may have to this money for their debts unless of course their creditors do it to the debts (5)
7 Boat that should be able to suit anyone (6)
8 Gear (6)
11 Business with the end in sight (6)
14 The right sort of woman to start a dame school (3)
18 "The War" (anag) (6)
19 When hammering take care to hit this (two words)–5,4)
20 Making sound as a bell (8)
21 Half a fortnight of old (8)
23 Bird, dish of coin (3)
25 This sign of the Zodiac has no connection with the Fishes (6)
26 A preservative of teeth (6)
29 Famous sculptor (5)
30 This part of the locomotive engine would sound familiar to the golfer (5)

The Lorenz cipher

A far more complicated machine "Lorenz SZ40" was used by Hitler to send messages to generals.

A weakness in the way the cipher was used led to break the code. The bomb machines were not flexible enough (just specific tasks at high speed).

Max Newman, a UK mathematician designed a machine - Colossus -capable of adapting itself to different problems (dec 8, 1943): 1500 electronic valves, programmable: the first precursor of digital computer.

REMARK

Secrecy: Colossus was destroyed, UK kept Enigma's decipher techniques secret up to early 70's (and gave Enigma machines to Commonwealth…)

The invention of computer was credited to Eckert-Mauchly in 1945 (18 000 valves)

Unit 4
Modern cryptography

Modern cryptography (1970 -)

Advent of computers: fast decryption of simple ciphers

ASCII: Every letter/symbol is converted to a sequence of bits

ASCII binary numbers for the capital letters.

A	1000001	N	1001110
B	1000010	O	1001111
C	1000011	P	1010000
D	1000100	Q	1010001
E	1000101	R	1010010
F	1000110	S	1010011
G	1000111	T	1010100
H	1001000	U	1010101
I	1001001	V	1010110
J	1001010	W	1010111
K	1001011	X	1011000
L	1001100	Y	1011001
M	1001101	Z	1011010

Modern cryptography (1970 -)

A complicated cipher: Lucifer 1971 (IBM) based on substitution and transposition

A precursor of DES: Data Encryption System, still used nowdays

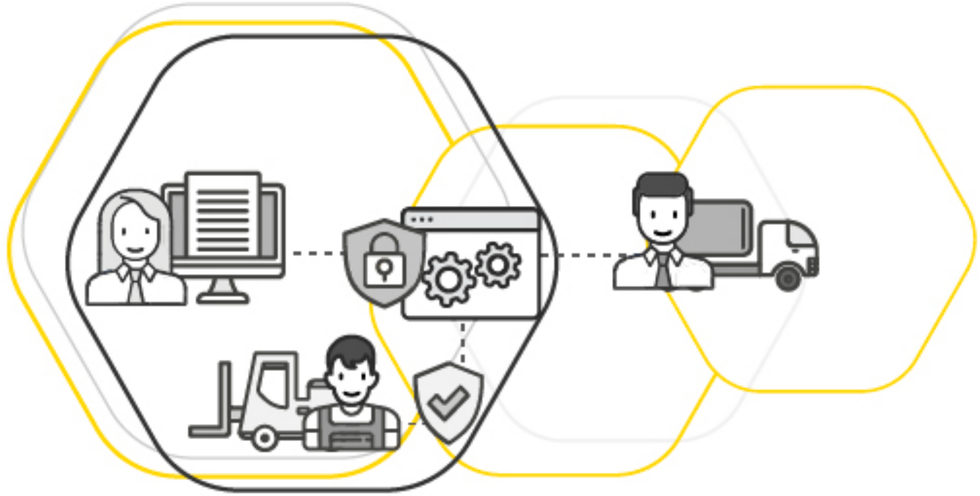
All are symmetric ciphers: a key enables to encrypt, a reverse process based on the same private key enables to decrypt

Private keys

The weakness of all ciphersystems: private keys.

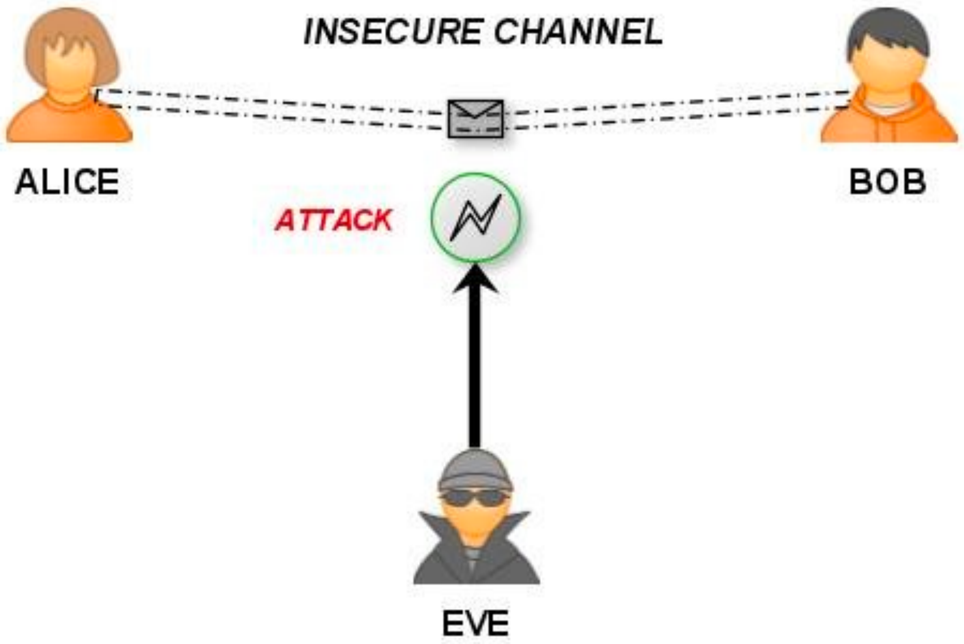
Germany (Enigma): entire books with the keys of all the days of the year delivered

A huge economical problem and weakness of symmetric ciphers: distribution of keys.
Even governments had serious logistic problems in distributing tons of keys.



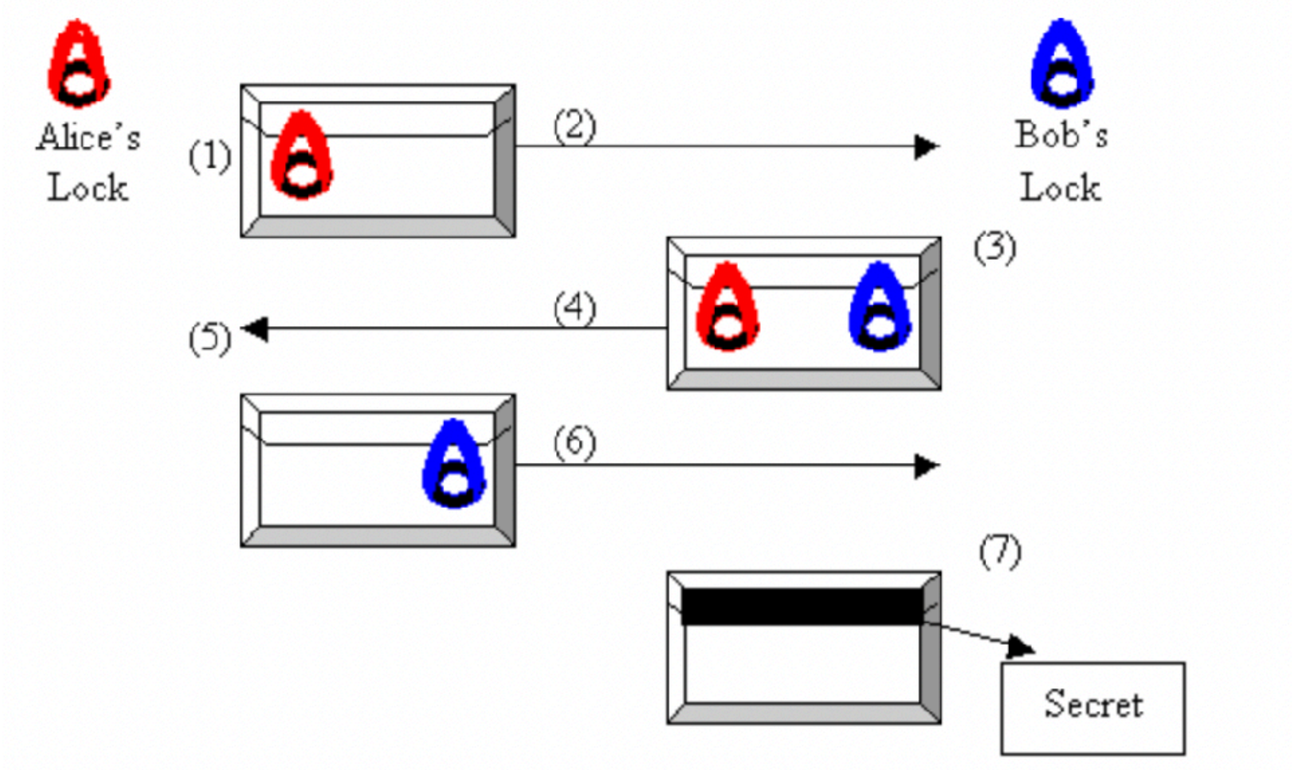
Public keys: Maths come back again

How to share a message between Alice and Bob if an eavesdropper (Eve) may intercept every communication between A and B without the need of exchanging a private key?



an idea: the double private key

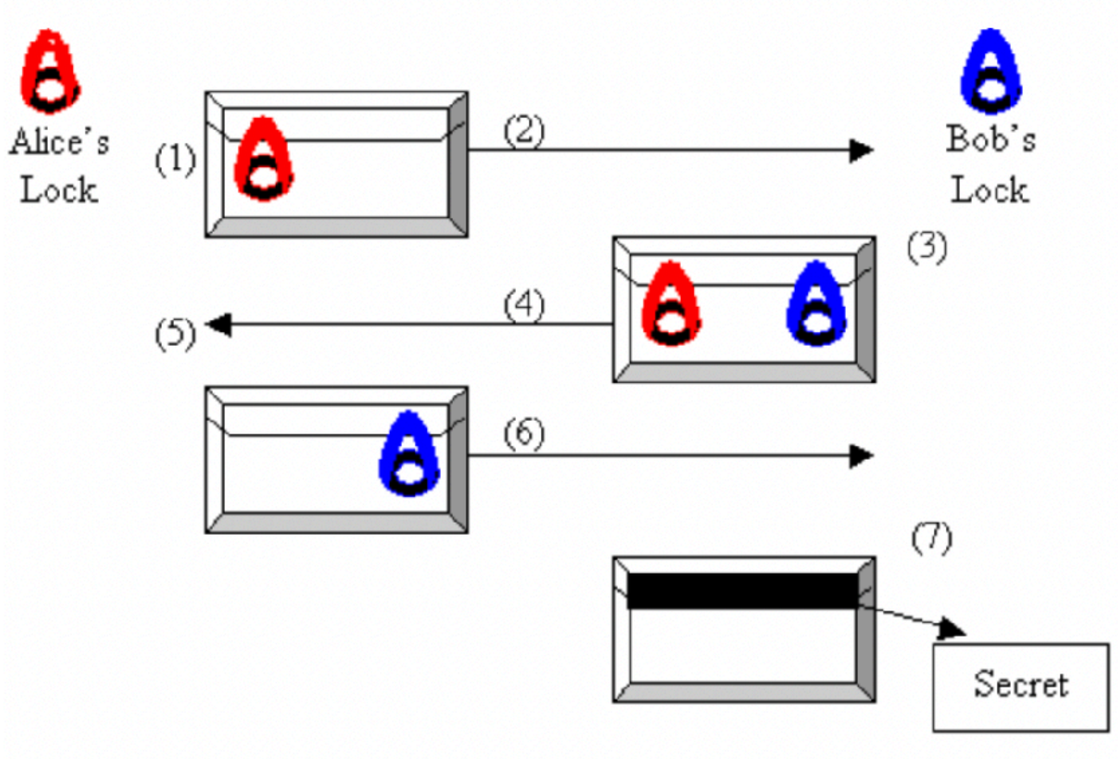
1. Alice puts a secret in a box, which she locks with her own lock. Only Alice has the key to this lock.
2. Alice then ships the box to Bob.
3. Bob adds his own lock to this box in parallel, so that now the box has two locks.
4. Bob then ships the box back to Alice.
5. Alice, knowing that the box is secure with Bob's lock, then takes her own lock off the box (with her key).
6. Alice sends the box back to Bob.
7. Bob then removes his lock and receives the secret (which could have been a new shared key).



2 private keys?

lock ⟷ encrypyt unlock ⟷ decrypyt

1. Alice encrypts
2. Bob encrypts
3. Alice decrypts using Alice's key
4. Bob decrypts using Bob's key



Does it work?

NO: order counts in ciphering

Two private keys?

EXAMPLE

1. Alice encrypts
2. Bob encrypts
3. Alice decrypts using Alice's key
4. Bob decrypts using Bob's key

Alice's key

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

Bob's key

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

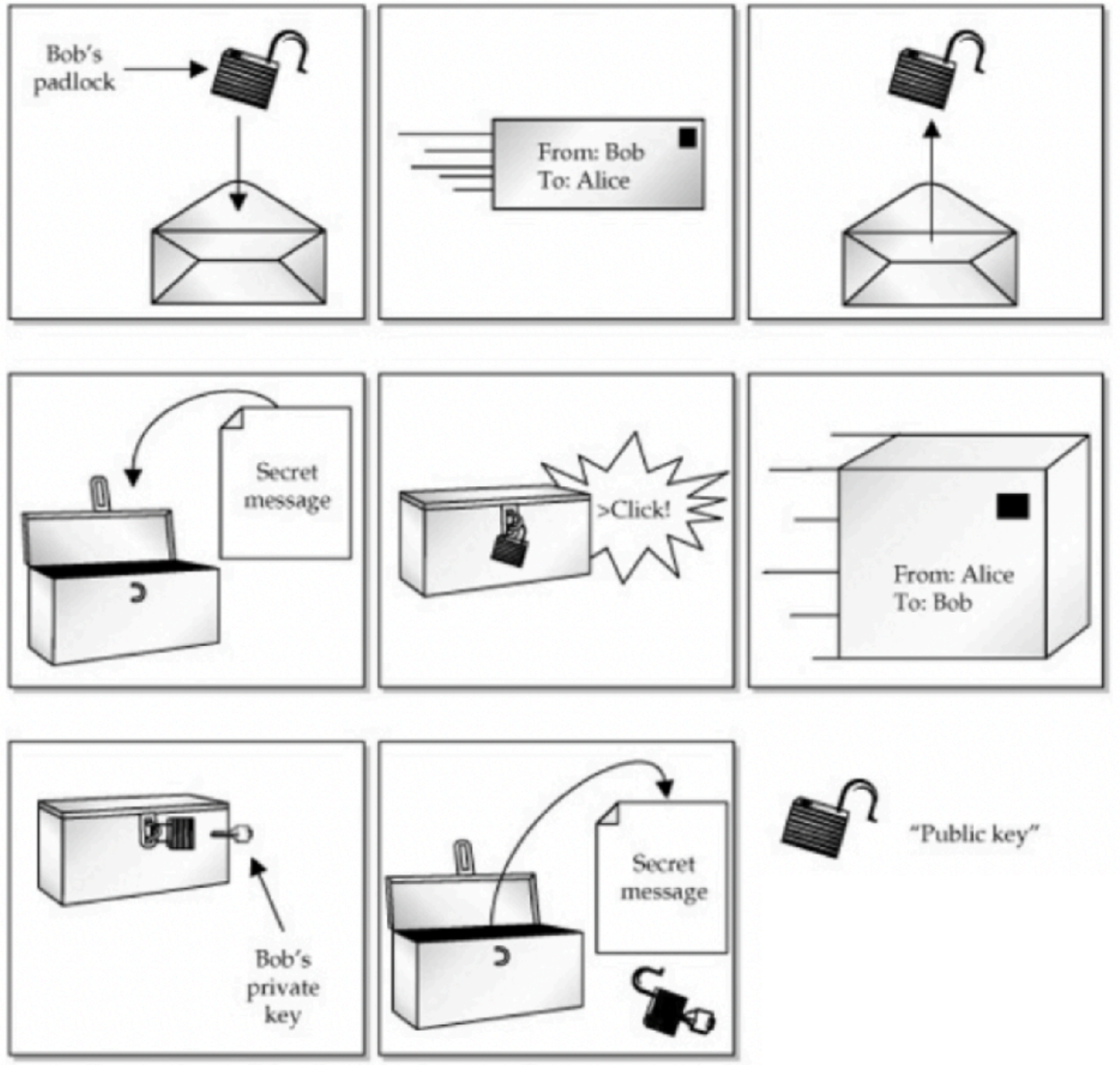
Message	m e e t	m e	a t	n o o n
Encrypted with Alice's key	Y G G C	Y G	H C	J B B J
Encrypted with Bob's key	L N N M	L N	O M	E P P E
Decrypted with Alice's key	Z Q Q X	Z Q	L X	K P P K
Decrypted with Bob's key	w n n t	w n	y t	x b b x

The concept of two keys: one private and one public

Bob shows his public key and gives it to anybody who wants to send him a message

Alice encrypts using Bob's public key

Bob decrypts using Bob's private key



(Ed Burns blog)

Was conceived by Duffie-Helmann who were not able to find how to implement it

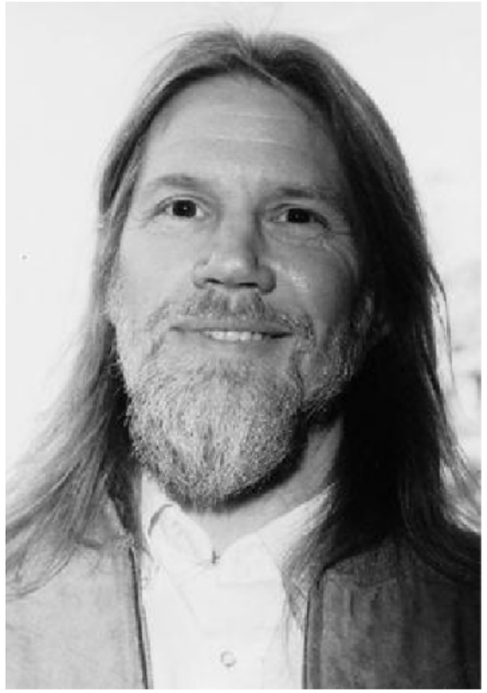
How to share a random key

Diffie - Hellmann - (Merkle) key exchange

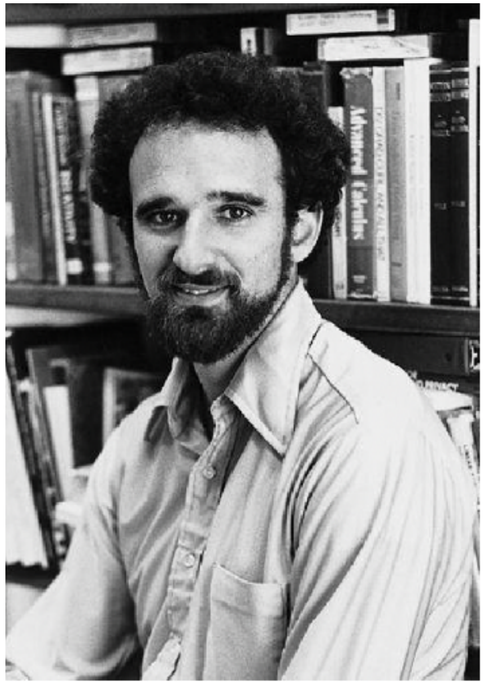
A solution based on mathematics (modular algebra) **Course topic**

Diffie, Whitfield; Hellman, Martin E. (November 1976). "New Directions in Cryptography" (PDF). *IEEE Transactions on Information Theory*. **22** (6): 644–654.

The idea came out after years of trials and thinkings: modular algebra



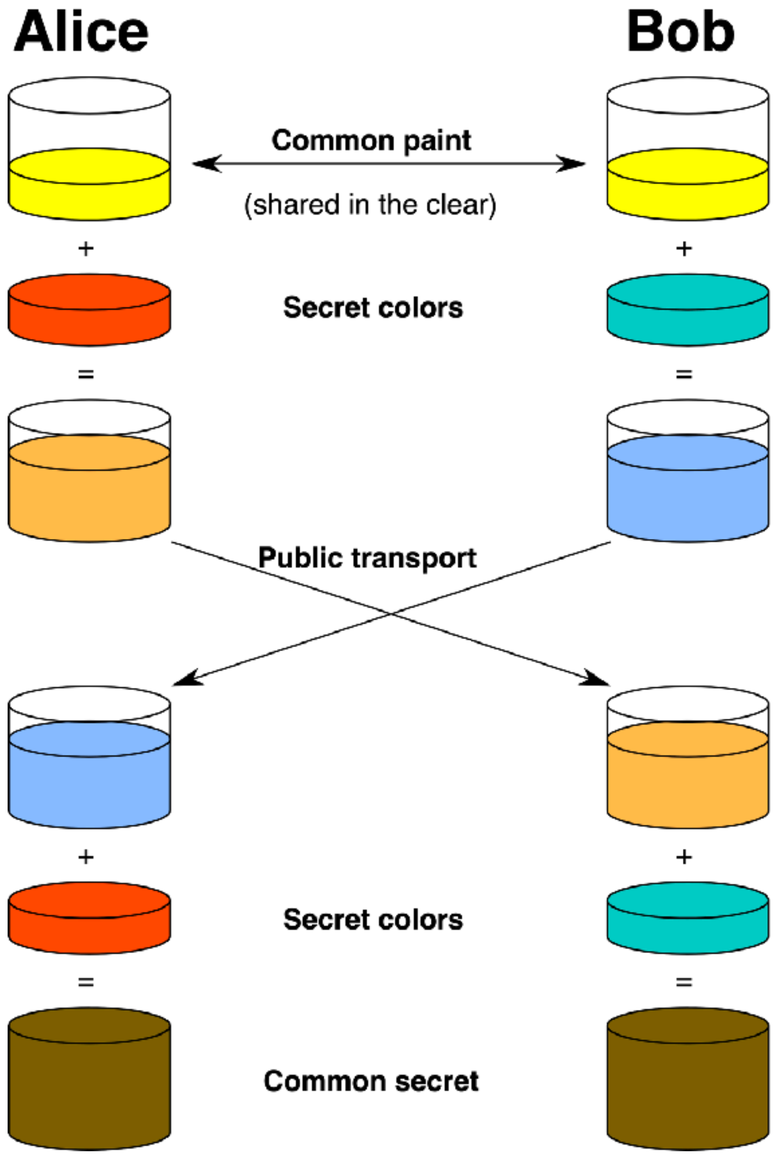
W. Diffie
(Sun microsystems - Stanford)



M. Hellmann (Stanford)

Diffie - Hellmann - (Merkle) key exchange concept

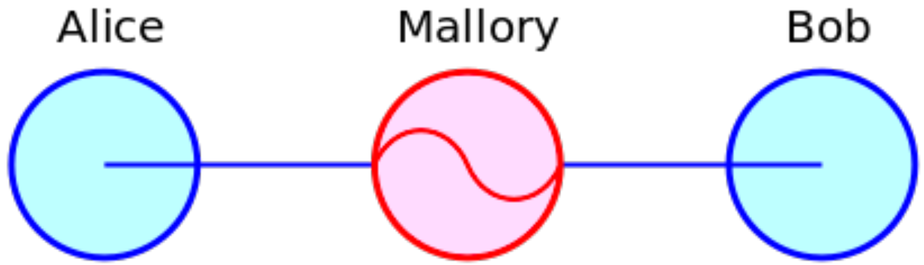
Sharing a random message - paint analogy



Digital signature

PROBLEM

In Diffie - Hellman key exchange how can Alice be sure that Bob is him and Alice is her? (MITM Attack: Man In The Middle Attack)



The concept of Digital Signature was defined by Diffie - Hellman who did not find how to implement it...

Course topic

Digital Signature: mathematical scheme for verifying the authenticity of digital messages or documents

Public key cryptography: the solution

Rivest, Shamir, Adleman (MIT)

Actually a similar system was invented by C. Cocks UK mathematician in 1973, but it was too early for low computer performance. Declassified in 1997!

1978: RSA cryptosystem

Course topic

Rivest, R.; Shamir, A.; Adleman, L. (February 1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" (PDF). *Communications of the ACM*. **21** (2): 120–126

RSA solved also digital signature

Ronald Rivest, Adi Shamir and Leonard Adleman.

based on the difficulty of factoring large numbers as product of prime numbers

MATHEMATICIAN

Factor a number as a product of two primes

RSA-232 [edit]

RSA-232 has 232 decimal digits (768 bits), and was factored on February 17, 2020, by N. L. Zamarashkin, D. A. Zheltkov and S. A. Matveev.[36]

```
RSA-232 = 1009881397871923546909564894309468582818233821955573955141120516205831021338
          5285453743661097571543636649133800849170651699217015247332943892702802343809
          6090980497644054071120196541074755382494867277137407501157718230539834060616
          2079
```

```
RSA-232 = 2966909333208360660361779924242630634742946262521852394401857157419437019472
          3262390744910112571804274494074452751891
        × 3403816175197563438006609498491521420547121760734723172735163413276050706174
          8526506443144325148088881115083863017669
```

Factor a number as a product of two primes

RSA-1024 [edit]

RSA-1024 has 309 decimal digits (1,024 bits), and has not been factored so far. $100,000 was previously offered for factorization.

```
RSA-1024 = 135066410865995223349603216278805969938881475605667027524485143851526510604
           859533833940287150571909441798207282164471551373680419703964191743046496589
           274256239341020864383202110372958725762358509643110564073501508187510676594
           629205563685529475213500852879416377328533906109750544334999811150056977236
           890927563
```

END of
LESSON 1
History and why MATHS came in Cryptography