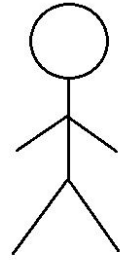
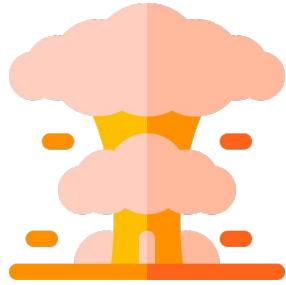
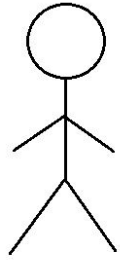


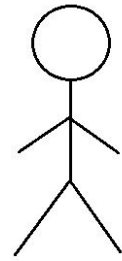
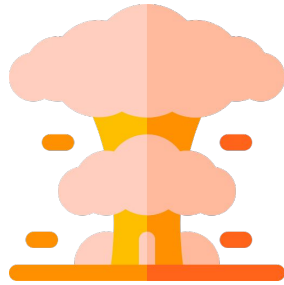
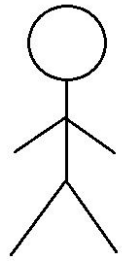
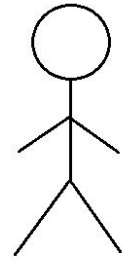
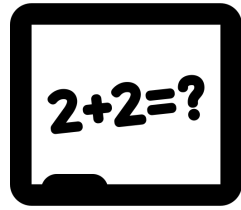
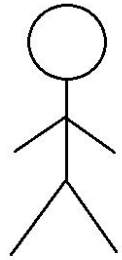
# The Secret Battle of Encryption Algorithms

by @amandasopkin



**LIBRE  
PLANET  
2019**





# Disclaimer

@amandasopkin

**Where are we headed?**

@amandasopkin

# Cryptography (bad) :

"The art of writing or solving codes."


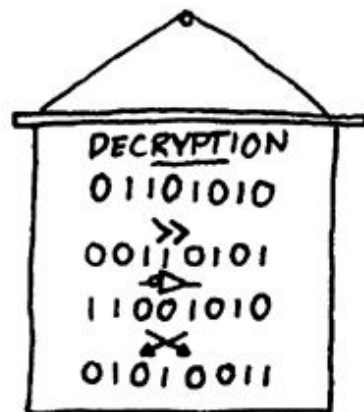
@amandasopkin

# Cryptography (better) :

"method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it."

-IEEE

MY CRYPTOSYSTEM IS LIKE  
ANY FEISTEL CIPHER, EXCEPT  
IN THE S-BOXES WE SIMPLY  
TAKE THE BITSTRING DOWN,  
FLIP IT, AND REVERSE IT.



I'VE BEEN BARRED FROM SPEAKING AT ANY MAJOR  
CRYPTOGRAPHY CONFERENCES EVER SINCE IT BECAME  
CLEAR THAT ALL MY ALGORITHMS WERE JUST  
THINLY DISGUISED MISSY ELLIOTT SONGS.



# Bread and Butter of encryption

@amandasopkin

# Encryption:

encoding using a key and an  
encryption algorithm

@amandasopkin

Key derivation:

process for creating suitable  
keys for use in encryption

@amandasopkin

## Plain text:

input in its natural form

Can be stream of bits, text  
file, bitmap, etc.

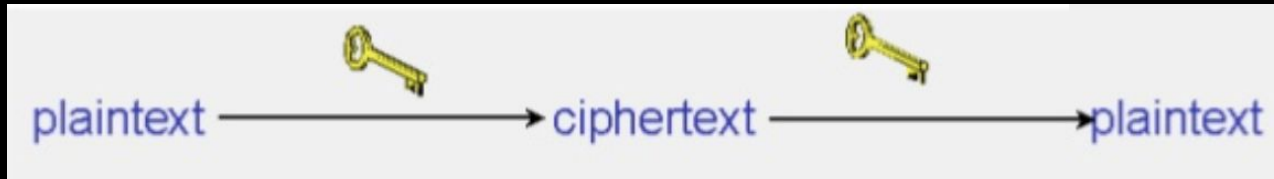
@amandasopkin

Cipher text:

input that has been encrypted

@amandasopkin

# Basic process:



Ciphers:

Method for disguising text

@amandasopkin

# History



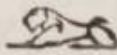



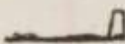


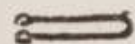



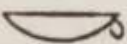
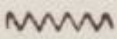
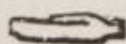
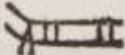
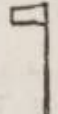


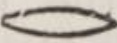

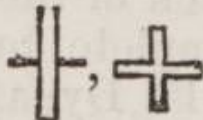

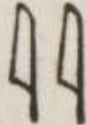
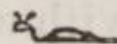



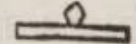






@amandasopkin



1900 BC: Cryptographic  
hieroglyphics

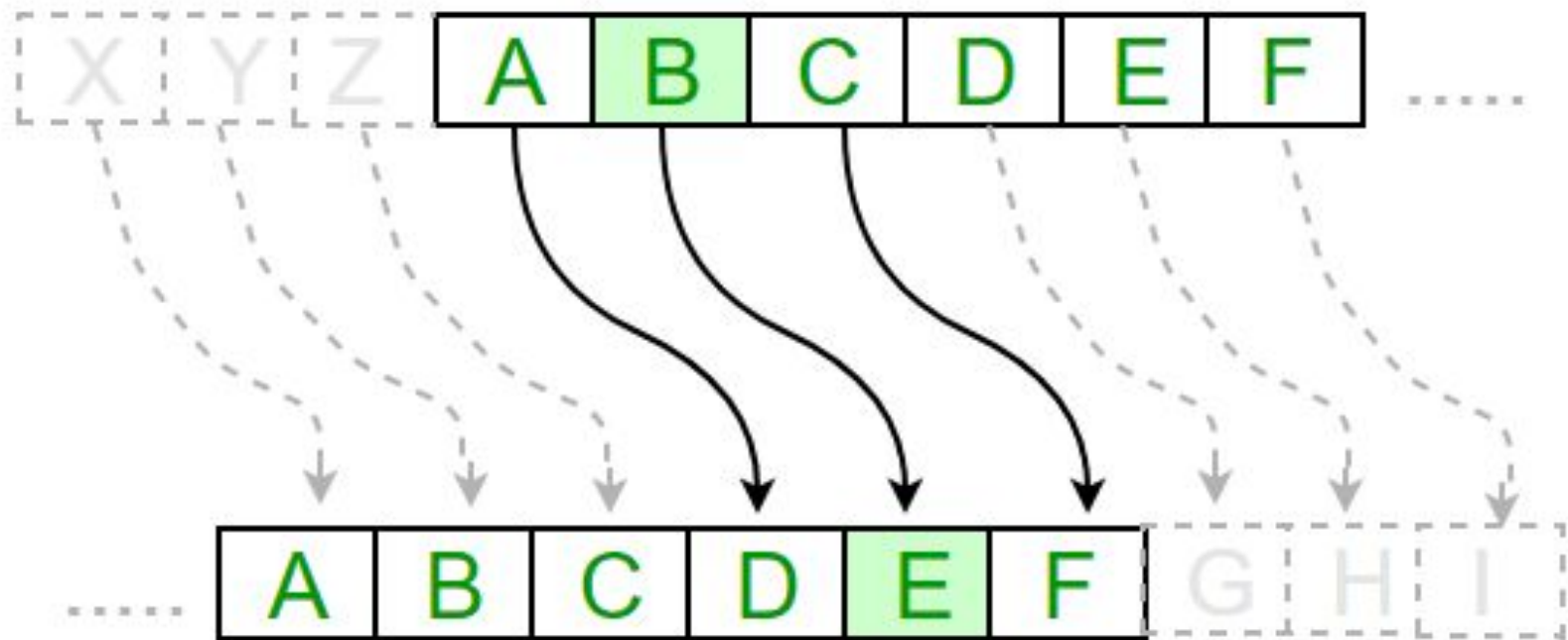
@amandasopkin

## List of the more common Hieroglyphic forms.

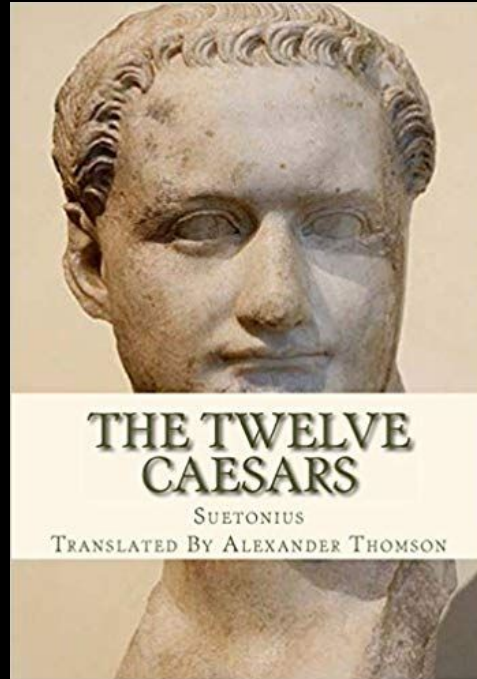
	a.		p.		l.		t.		ka.		sen.
	ā.		k.		m.		th.		mer.		us or os
	a.		k.		n.		t or d.		tum.		neter.
	i.		k.		r.		z.		am.		kheper.
	ī.		f.		s.		kha.		tat.		hotep.
	oo.		h.		s.		her.		nefer.		nen.

100 BC: Julius Caesar

@amandasopkin



# Documentation of Caesar Cipher:



Did Caesar design more  
complicated systems as well?

How effective was the Caesar  
Cipher?

How effective was the Caesar  
Cipher?





# Effectiveness of Caesar Cipher:



Many of Caesar's enemies were illiterate



Others assumed that encoded letters were in another language

9th century Al Kindi  
(mathematician):  
Earliest surviving frequency  
analysis records



# Letter frequencies

Can be used to break a cipher

# Letter frequencies

“

GFS WMY OG LGDVS MF SFNKYHOSU ESLLMRS, PC WS BFGW POL DMFRQMRS, PL OG CPFU M UPCCSKSFO HDMPFOSXO GC OIS LMES DMFRQMRS DGFR SFGQRI OG CPDD GFS LISSO

GK LG, MFU OISF WS NGQFO OIS GNNQKKSFNLS GC SMNI DSOOSK. WS NMDD OIS EGLO CKSJQSFODY GNNQKKPFR DSOOSK OIS 'CPKLO'; OIS FSXO EGLO GNNQKKPFR DSOOSK OIS

'LSNGFU' OIS CGDDGWPFR EGLO GNNQKKPFR DSOOSK OIS 'OIPKU'; MFU LG GF, QFOPD WS MNNGQFO CGK MDD OIS UPCCSKSFO DSOOSKL PF OIS HDMPFOSXO LMEHDS. OISF WS

DGGB MO OIS NPHISK OSXO WS WMFO OG LGDVS MFU WS MDLG NDMLLPCY POL LYEAGDL. WS CPFU OIS EGLO GNNQKKPFR LYEAGD MFU NIMFRS PO OG OIS CGKE GC OIS 'CPKLO'

DSOOSK GC OIS HDMPFOSXO LMEHDS, OIS FSXO EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'LSNGFU' DSOOSK, MFU OIS CGDDGWPFR EGLO NGEEGF LYEAGD PL

NIMFRSU OG OIS CGKE GC OIS 'OIPKU' DSOOSK, MFU LG GF, QFOPD WS MNNGQFO CGK MDD LYEAGDL GC OIS NKYHOGRKME WS WMFO OG LGDVS.

# Letter frequencies

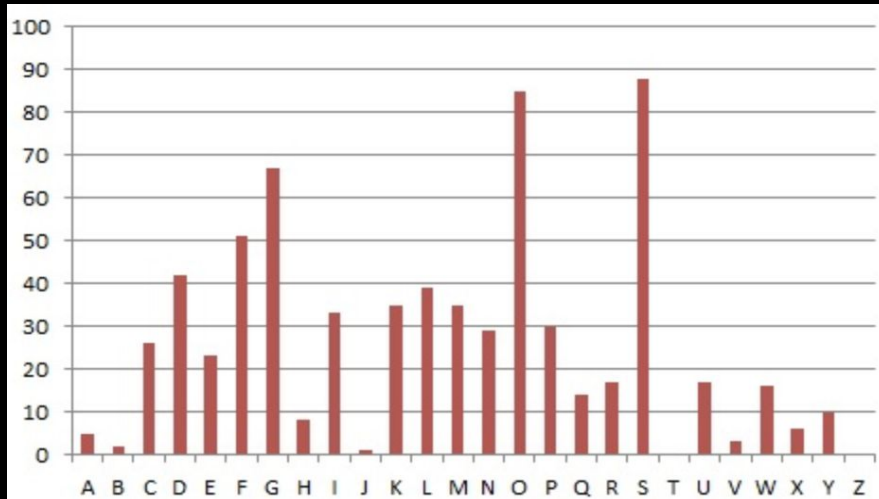
Ciphertext Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	5	2	26	42	23	51	67	8	33	1	35	39	35	29	85	30	14	17	88	0	17	3	16	6	10	0

Frequency of each letter in cipher

Ciphertext Letter	S	O	G	F	D	L	K	M	I	P	N	C	E	R	U	W	Q	Y	H	X	A	V	B	J	T	Z
Frequency	88	85	67	51	42	39	35	35	33	30	29	26	23	17	17	16	14	10	8	6	5	3	2	1	0	0

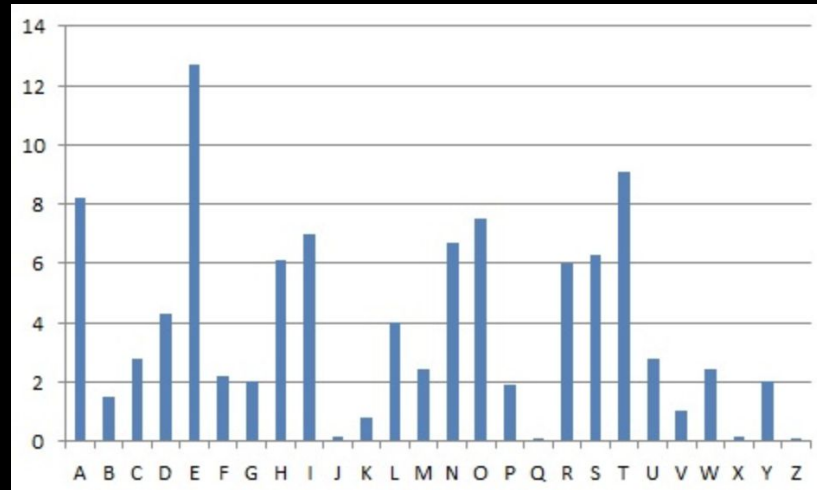
Sorted from most common to least

# Letter frequencies



Frequencies of letters in cipher

# Letter frequencies

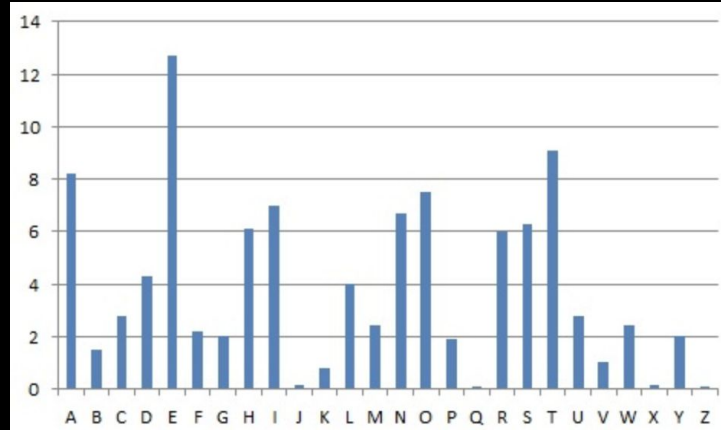


Standard english letter frequencies

# Letter frequencies

Ciphertext Letter	S	O	G	F	D	L	K	M	I	P	N	C	E	R	U	W	Q	Y	H	X	A	V	B	J	T	Z
Frequency	88	85	67	51	42	39	35	35	33	30	29	26	23	17	17	16	14	10	8	6	5	3	2	1	0	0

Most frequent letters in cipher are S and O





# Substitute E and T for S and O

“

GFS WMY OG LGDVS MF SFNKYHOSU ESLLMRS, PC WS BFGW POL DMFRQMRS, PL OG CPFU M UPCCSKSFO HDMPFOSXO GC OIS LMES DMFRQMRS DGFR SFGQRI OG CPDD GFS LISSO  
GK LG, MFU OISF WS NGQFO OIS GNNQKKSFNLS GC SMNI DSOOSK. WS NMDD OIS EGLO CKSJQSFDY GNNQKKPFR DSOOSK OIS 'CPKLO'; OIS FSXO EGLO GNNQKKPFR DSOOSK OIS  
'LSNGFU' OIS CGDDGWPFER EGLO GNNQKKPFR DSOOSK OIS 'OIPKU'; MFU LG GF, QFOPD WS MNNGQFO CGK MDD OIS UPCCSKSFO DSOOSKL PF OIS HDMPFOSXO LMEHDS. OISF WS  
DGGB MO OIS NPHISK OSXO WS WMFO OG LGDVS MFU WS MDLG NDMLLPCY POL LYEAGDL. WS CPFU OIS EGLO GNNQKKPFR LYEAGD MFU NIMFRS PO OG OIS CGKE GC OIS 'CPKLO'  
DSOOSK GC OIS HDMPFOSXO LMEHDS, OIS FSXO EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'LSNGFU' DSOOSK, MFU OIS CGDDGWPFER EGLO NGEEGF LYEAGD PL  
NIMFRSU OG OIS CGKE GC OIS 'OIPKU' DSOOSK, MFU LG GF, QFOPD WS MNNGQFO CGK MDD LYEAGDL GC OIS NKYHOGRKME WS WMFO OG LGDVS.

# Spot instances of "tle"

“  
GFe WMY tG LGDVe MF eFNKYHteU EeLLMRe, PC We BFGW PtL DMFRQMRRe, PL tG CPFU M UPCCeKeFt HDMPFteXt GC tle LMEe  
DMFRQMRRe DGFR eFGORI tG CPDD GFe Lleet GK LG, MFU tleF We NGQFt tle GNNQKKeFNeL GC eMNI DetteK. We NMDD tle EGLt  
CKeJQeFtDY GNNQKKPFR DetteK tle 'CPKlt, tle FeXt EGLt GNNQKKPFR DetteK tle 'LeNGFU' tle CGDDGWPFER EGLt GNNQKKPFR DetteK  
tle 'tIPKU', MFU LG GF, QFtPD We MNNGQFt CGK MDD tle UPCCeKeFt DetteKL PF tle HDMPFteXt LMEHDe. tle' We DGGB Mt tle NPHleK  
teXt We WMFt tG LGDVe MFU We MDLG NDMLLPCY PtL LYEAGDL. We CPFU tle EGLt GNNQKKPFR LYEAGD MFU NIMFRe Pt tG tle CGKE  
GC tle 'CPKlt' DetteK GC tle HDMPFteXt LMEHDe, tle FeXt EGLt NGEEGF LYEAGD PL NIMFReU tG tle CGKE GC tle 'LeNGFU' DetteK, MFU  
tle CGDDGWPFER EGLt NGEEGF LYEAGD PL NIMFReU tG tle CGKE GC tle 'tIPKU' DetteK, MFU LG GF, QFtPD We MNNGQFt CGK MDD  
LYEAGDL GC tle NKYHtGRKME We WMFt tG LGDVe.

Most common letter is now G,  
which must be a, i, or o

“  
GF<sup>e</sup> WMY tG LGDVe MF eFNKYHteU EeLLMR<sup>e</sup>, PC We BFGW PtL DMFRQMR<sup>e</sup>, PL tG CPFU M UPCCeKeFt HDMPFteXt GC tle LME<sup>e</sup>  
DMFRQMR<sup>e</sup> DGFR eFGQRI tG CPDD GF<sup>e</sup> Lleet GK LG, MFU tleF We NGQFt tle GNNQKKeFNeL GC eMNI DetteK. We NMDD tle EGLt  
CKeJQeFtDY GNNQKKPFR DetteK tle 'CPKlt', tle FeXt EGLt GNNQKKPFR DetteK tle 'LeNGFU' tle CGDDGWPFR EGLt GNNQKKPFR DetteK  
tle 'tIPKU', MFU LG GF, QFtPD We MNNGQFt CGK MDD tle UPCCeKeFt DetteKL PF tle HDMPFteXt LMEHDe. tleF We DGGB Mt tle NPHleK  
teXt We WMFt tG LGDVe MFU We MDLG NDMLLPCY PtL LYEAGDL. We CPFU tle EGLt GNNQKKPFR LYEAGD MFU NIMFR<sup>e</sup> Pt tG tle CGKE  
GC tle 'CPKlt' DetteK GC tle HDMPFteXt LMEHDe, tle FeXt EGLt NGEEGF LYEAGD PL NIMFR<sup>e</sup>U tG tle CGKE GC tle 'LeNGFU' DetteK, MFU  
tle CGDDGWPFR EGLt NGEEGF LYEAGD PL NIMFR<sup>e</sup>U tG tle CGKE GC tle 'tIPKU' DetteK, MFU LG GF, QFtPD We MNNGQFt CGK MDD  
LYEAGDL GC tle NKYHtGRKME We WMFt tG LGDVe.

# Substitute e and t for s and o and o for g

“  
oFe WMY to LoDVe MF eFNKYHteU EeLLMRe, PC We BFoW PtL DMFRQMRe, PL to CPFU M UPCCeKeFt HDMPFteXt oC the LMEe  
DMFRQMRe DoFR eFoQRh to CPDD oFe Lheet oK Lo, MFU theF We NoQFt the oNNQKKeFNeL oC eMNH DetteK. We NMDD the EoLt  
CKeJQeFtDY oNNQKKPFR DetteK the 'CPKlt', the FeXt EoLt oNNQKKPFR DetteK the 'LeNoFU' the CoDDoWPFR EoLt oNNQKKPFR DetteK  
the 'thPKU', MFU Lo oF, QFtPD We MNNNoQFt CoK MDD the UPCCeKeFt DetteKL PF the HDMPFteXt LMEHDe. theF We DooB Mt the  
NPHheK teXt We WMFt to LoDVe MFU We MDLo NDMLLPCY PtL LYEAoDL. We CPFU the EoLt oNNQKKPFR LYEAoD MFU NhMFRRe Pt to  
the CoKE oC the 'CPKlt' DetteK oC the HDMPFteXt LMEHDe, the FeXt EoLt NoEEoF LYEAoD PL NhMFRReU to the CoKE oC the 'LeNoFU'  
DetteK, MFU the CoDDoWPFR EoLt NoEEoF LYEAoD PL NhMFRReU to the CoKE oC the 'thPKU' DetteK, MFU Lo oF, QFtPD We MNNNoQFt  
CoK MDD LYEAoDL oC the NKYHtoRKME We WMFt to LoDVe.

# Spot oFe and theF and then Lheet

oFe WMY to LoDVe MF eFNKYHteU EeLLMRe, PC We BFoW PtL DMFRQMRe, PL to CPFU M UPCCeKeFt HDMPFteXt oC the LMEe DMFRQMRe DoFR eFoQRh to CPDD oFe Lheet oK Lo, MFU theF We NoQFt the oNNQKKeFNeL oC eMnh DetteK. We NMDD the EoLt CKeJQeFtDY oNNQKKPFR DetteK the 'CPKlt', the FeXt EoLt oNNQKKPFR DetteK the 'LeNoFU' the CoDDoWPFR EoLt oNNQKKPFR DetteK the 'thPKU', MFU Lo oF, QFtPD We MNNNoQFt CoK MDD the UPCCeKeFt DetteKL PF the HDMPFteXt LMEHDe. theF We DooB Mt the NPHheK teXt We WMFt to LoDVe MFU We MDLo NDMLLPCY PtL LYEAoDL. We CPFU the EoLt oNNQKKPFR LYEAoD MFU NhMFRe Pt to the CoKE oC the 'CPKlt' DetteK oC the HDMPFteXt LMEHDe, the FeXt EoLt NoEEoF LYEAoD PL NhMFReU to the CoKE oC the 'LeNoFU' DetteK, MFU the CoDDoWPFR EoLt NoEEoF LYEAoD PL NhMFReU to the CoKE oC the 'thPKU' DetteK, MFU Lo oF, QFtPD We MNNNoQFt CoK MDD LYEAoDL oC the NKYHtoRKME We WMFt to LoDVe.

# Spot sODVe and OK

“one WMY to soDVe Mn enNKYHteU EessMRe, PC We BnoW Pts DMnRQMRe, Ps to CPnU M UPCCeKent HDMPnteXt oC the sMEe DMnRQMRe DonR enoQRh to CPDD one sheet oK so, MnU then We NoQnt the oNNQKKenNes oC eMNH DetteK. We NMDD the East CKeJqentDY oNNQKKPnR DetteK the 'CPKst', the neXt East oNNQKKPnR DetteK the 'seNonU' the CoDDoWPnR East oNNQKKPnR DetteK the 'thPKU'; MnU so on, QntPD We MNNoQnt CoK MDD the UPCCeKent DetteKs Pn the HDMPnteXt sMEHDe. then We DooB Mt the NPHheK teXt We WMnt to soDVe MnU We MDso NDMssPCY Pts sYEAoDs. We CPnU the East oNNQKKPnR sYEAoD MnU NhMnRe Pt to the CoKE oC the 'CPKst' DetteK oC the HDMPnteXt sMEHDe, the neXt East NoEEon sYEAoD Ps NhMnReU to the CoKE oC the 'seNonU' DetteK, MnU the CoDDoWPnR East NoEEon sYEAoD Ps NhMnReU to the CoKE oC the 'thPKU' DetteK, MnU so on, QntPD We MNNoQnt CoK MDD sYEAoDs oC the NKYHtoRKME We WMnt to soDVe.

# Sub 1 for D, v for V, R for K

“one WMY to solve Mn enNrYHteU EessMRe, PC We BnoW Pts IMnRQMRe, Ps to CPnU M UPCCerent HIMPnteXt oC the sMEe IMnRQMRe lonR enoQRh to CPll one sheet or so, MnU then We NoQnt the oNNQrrrenNes oC eMnh letter. We NMll the East CrejQentlY oNNQrrPnR letter the 'CPrst', the neXt East oNNQrrPnR letter the 'seNonU' the ColloWPnR East oNNQrrPnR letter the 'thPrU', MnU so on, QntPl We MNNoQnt Cor Mll the UPCCerent letters Pn the HIMPnteXt sMEHle. then We looB Mt the NPHher teXt We WMnt to solve MnU We Mlso NIMssPCY Pts sYEAols. We CPnU the East oNNQrrPnR sYEAol MnU NhMnRe Pt to the CorE oC the 'CPrst' letter oC the HIMPnteXt sMEHle, the neXt East NoEEon sYEAol Ps NhMnReU to the CorE oC the 'seNonU' letter, MnU the ColloWPnR East NoEEon sYEAol Ps NhMnReU to the CorE oC the 'thPrU' letter, MnU so on, QntPl We MNNoQnt Cor Mll sYEAols oC the NrYHtoRrME We WMnt to solve.

# Spot enoQRh

“one WMY to solve Mn enNrYHteU EessMRe, PC We BnoW Pts IMnRQMRe, Ps to CPnU M UPCCerent HIMPnteXt oC the sMEe IMnRQMRe lonR enoQRh to CPll one sheet or so, MnU then We NoQnt the oNNQrrrenNes oC eMnh letter. We NMll the East CrejQentlY oNNQrrPnR letter the 'CPrst', the neXt East oNNQrrPnR letter the 'seNonU' the ColloWPnR East oNNQrrPnR letter the 'thPrU', MnU so on, QntPl We MNNoQnt Cor Mll the UPCCerent letters Pn the HIMPnteXt sMEHle. then We looB Mt the NPHher teXt We WMnt to solve MnU We Mlso NIMssPCY Pts sYEAols. We CPnU the East oNNQrrPnR sYEAol MnU NhMnRe Pt to the CorE oC the 'CPrst' letter oC the HIMPnteXt sMEHle, the neXt East NoEEon sYEAol Ps NhMnReU to the CorE oC the 'seNonU' letter, MnU the ColloWPnR East NoEEon sYEAol Ps NhMnReU to the CorE oC the 'thPrU' letter, MnU so on, QntPl We MNNoQnt Cor Mll sYEAols oC the NrYHtoRrME We WMnt to solve.



# Spot EesMge and Nount

“  
one WMY to solve Mn enNrYHteU **EessMge**, PC We BnoW Pts IMnguMge, Ps to CPnU M UPCCerent HIMPnteXt oC the sMEe IMnguMge long  
enough to CPll one sheet or so, MnU then We **Nount** the oNNurrenNes oC eMnh letter. We NMll the East Crejuently oNNurrPng letter the  
'CPrst', the neXt East oNNurrPng letter the 'seNonU' the ColloWPng East oNNurrPng letter the 'thPrU', MnU so on, untPl We MNNount Cor  
Mll the UPCCerent letters Pn the HIMPnteXt sMEHle. then We looB Mt the NPHher teXt We WMnt to solve MnU We Mlso NIMssPCY Pts  
sYEAols. We CPnU the East oNNurrPng sYEAol MnU NhMnge Pt to the CorE oC the 'CPrst' letter oC the HIMPnteXt sMEHle, the neXt East  
NoEEon sYEAol Ps NhMngeU to the CorE oC the 'seNonU' letter, MnU the ColloWPng East NoEEon sYEAol Ps NhMngeU to the CorE oC the  
'thPrU' letter, MnU so on, untPl We MNNount Cor Mll sYEAols oC the NrYHtogrME We WMnt to solve.

Few more steps...

# Solved!

“  
one way to solve an encrypted message, if we know its language, is to find a different plaintext of the same language long enough to fill one sheet or so, and then we count the occurrences of each letter. we call the most frequently occurring letter the 'first', the next most occurring letter the 'second' the following most occurring letter the 'third', and so on, until we account for all the different letters in the plaintext sample. then we look at the cipher text we want to solve and we also classify its symbols. we find the most occurring symbol and change it to the form of the 'first' letter of the plaintext sample, the next most common symbol is changed to the form of the 'second' letter, and the following most common symbol is changed to the form of the 'third' letter, and so on, until we account for all symbols of the cryptogram we want to solve.

1500s: Vignere's system

@amandasopkin

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Key = "sup"

here is a super secure message  
sups up s upsup supsup supsups

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

Key = "sup"

here is a super secure message  
sups up s upsup supsup supsups  
z . . . . .



How effective was the Vignere  
system?

How effective was the Vignere system?



"le chiffre indéchiffrable"  
until 1863  
(but broken as early as the 16th  
century)

How was it broken?

## The Kasiski examination:

takes advantage of the fact that repeated words are, by chance, sometimes encrypted using the same key letters, leading to repeated groups in the ciphertext.

# The Kasiski examination:

Key: ABCDABCDABCDABCDABCDABCDABCDABCD

Plaintext: **CRYPTO**ISSHORTFOR**CRYPTO**GRAPHY

Ciphertext: **CSASTP**KVSIQUTGQU**CSASTP**IUAQJB

# The Kasiski examination:

Key: ABCDABCDABCDABCDABCDABCDABCDABCD

Plaintext: **CRYPTO**ISSHORTFOR**CRYPTO**GRAPHY

Ciphertext: **CSASTP**KVSIQUTGQU**CSASTP**IUAQJB

Using the distance between repeated subsequences, the length of the key can be found.

# The Kasiski examination:

Key: ABCDABCDABCDABCDABCDABCDABCDABCD

Plaintext: **CRYPTO**ISSHORTFOR**CRYPTO**GRAPHY

Ciphertext: **CSASTP**KVSIQUTGQU**CSASTP**IUAQJB

Once length is known, if a key is N letters long then every Nth letter must have been encoded using same letter of the text



# Vignere System and The Civil War

Confederate soldiers had messages frequently cracked because they relied on the phrases "Complete Victory," "Manchester Bluff" and "Come Retribution."

**Pro Tip:** Don't Use Easy  
to Guess Phrases!



Kerchhoff's Principle:  
secrecy of key

@amandasopkin

Let's get electric!

@amandasopkin

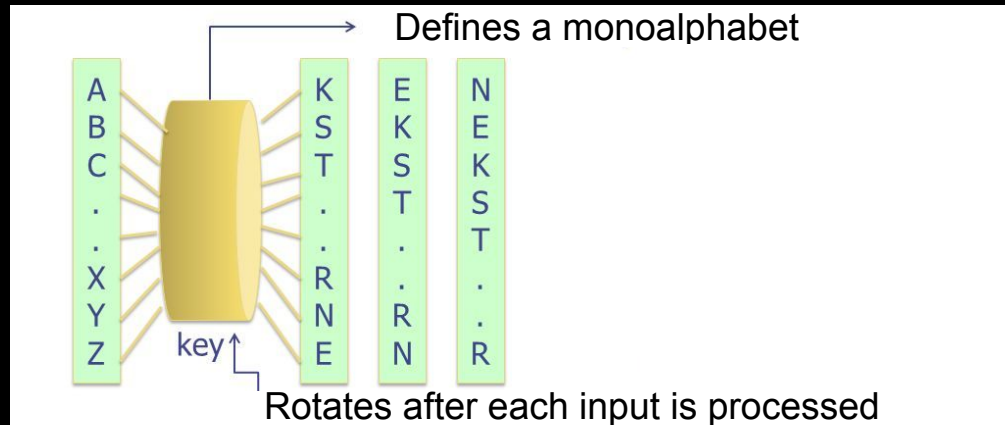
1800s: Hebern's system

@amandasopkin

# 1800s: Hebern's system



# 1800s: Hebern's system





William Friedman

vs.



Hebern System



# Breaking Hebern's system

# Breaking Hebern's system

With each rotor, one step = one keypress

Fastest rotor always at either end of rotor series

Statistical method called kappa test applied



William Friedman: 1

vs.



Hebern System: 0

How effective was  
Hebern's system?

How effective was  
Hebern's system?



# WW1/WW2 : Engima Machine

@amandasopkin



Rotors

Lampboard

Keyboard

Plugboard

# WW1: Engima Machine

Breakthroughs by Polish  
Mathematicians





Marian Rejewski



Marian Rejewski

vs.



Enigma Machine

# Key Insights into Enigma

1. Single initial 6 letter setting for all messages each day
2. Chosen message key repeated in this initial setting

Indicator or Grundstellung =  
initial rotor setting

# Indicator or Grundstellung = initial rotor setting

Initial setting	RAO
3 letter message key	IHL
Resulting indicator from setting rotors to RAO and encoding IHL twice	DQYQQT

Indicator: DQYQQT

Indicator: DQYQQT

D and Q represent the  
same letter

By collecting enough messages  
enciphered with same indicator,  
a table could be produced:

<b>First letter</b>	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>Fourth letter</b>	N	S	Y	Q	T	I	C	H	A	F	E	X	J	P	U	L	W	R	Z	K	G	O	V	M	D	B



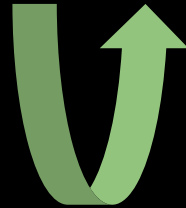
Path from first letter to fourth then  
from that letter to its fourth and so  
on leads to cycle group

<b>First letter</b>	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>Fourth letter</b>	N	S	Y	Q	T	I	C	H	A	F	E	X	J	P	U	L	W	R	Z	K	G	O	V	M	D	B



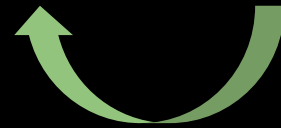
Path from first letter to fourth then  
from that letter to its fourth and so  
on leads to cycle group

<b>First letter</b>	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>Fourth letter</b>	N	S	Y	Q	T	I	C	H	A	F	E	X	J	P	U	L	W	R	Z	K	G	O	V	M	D	B



Path from first letter to fourth then  
from that letter to its fourth and so  
on leads to cycle group

<b>First letter</b>	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>Fourth letter</b>	N	S	Y	Q	T	I	C	H	A	F	E	X	J	P	U	L	W	R	Z	K	G	O	V	M	D	B



Path from first letter to fourth then  
from that letter to its fourth and so  
on leads to cycle group

<b>First letter</b>	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>Fourth letter</b>	N	S	Y	Q	T	I	C	H	A	F	E	X	J	P	U	L	W	R	Z	K	G	O	V	M	D	B



Cycle group starting at A 9	(A, N, P, L, X, M, J, F, I, A)
Cycle group starting at B 3	(B, S, Z, B)
Cycle group starting at C 9	(C, Y, D, Q, W, V, O, U, G, C)
Cycle group starting at E 3	(E, T, K, E)
Cycle group starting at H 1	(H, H)
Cycle group starting at R 1	(R, R)

Cycle group starting at A	(A, N, P, L, X, M, J, F, I, A)
Cycle group starting at B	(B, S, Z, B)
Cycle group starting at C	(C, Y, D, Q, W, V, O, U, G, C)
Cycle group starting at E	(E, T, K, E)
Cycle group starting at H	(H, H)
Cycle group starting at R	(R, R)

$1 * 3 * 9 = 27$  possibilities for ciphers at 1 and 4

# Key Insights into Enigma

Another weak link

=

Lazy cipher clerks!

# Key Insights into Enigma

Lazy cipher clerks often  
used same starting  
position i.e.

"AAA"



Given a day's traffic...

Solve for indicator/day key =>

Factor out board permutation =>

Commercial Enigma wiring =>

Rightmost rotor wiring

Given a day's traffic...

Solve for indicator/day key => 

Factor out board permutation => 

Commercial Enigma wiring => 

Rightmost rotor wiring 



Given a day's traffic...

Solve for indicator/day key => 

Factor out board permutation => 

Commercial Enigma wiring => 

Rightmost rotor wiring 



vs.

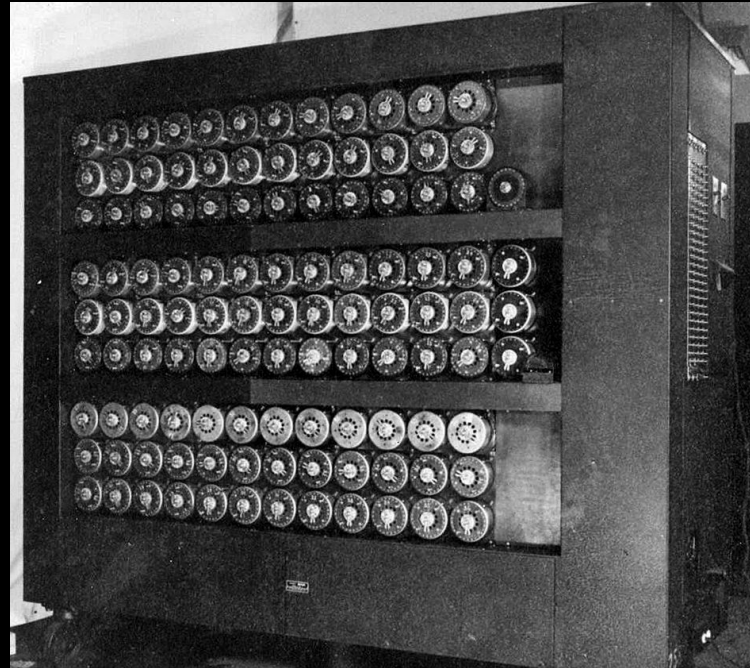


Marian Rejewski: 1

Enigma Machine: 0

Alan Turing  
and  
British efforts to  
crack the "Engima"

# Using findings of Rejewski and others:



One Bombe = 36 Enigmas!



97,000 parts

7 feet wide

One Bombe = 36 Enigmas!

2,000 pounds

£4,000,000

12 miles  
of wiring

Bombe provided several  
possible answers,  
Codebreakers narrowed  
it down

At peak,  
200+ Bombe machines  
cracking 3,000 messages  
each day!

Shortened the war by an  
estimated  
2 years!

How effective was  
The Engima machine?

How effective was  
The Engima machine?



**Pro Tip:** Establish a  
process and eliminate  
possible human error!



Let's get some standards!

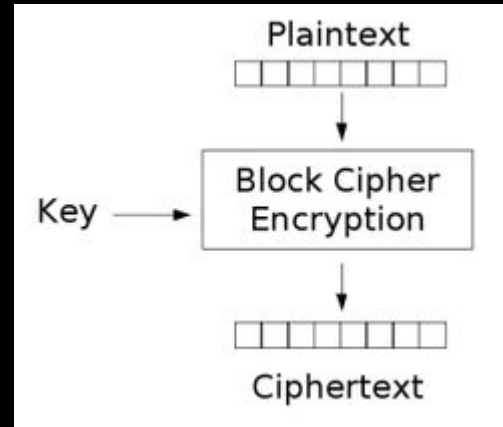


1973: IBM's Luther

@amandasopkin

# Note on block cipher encryption

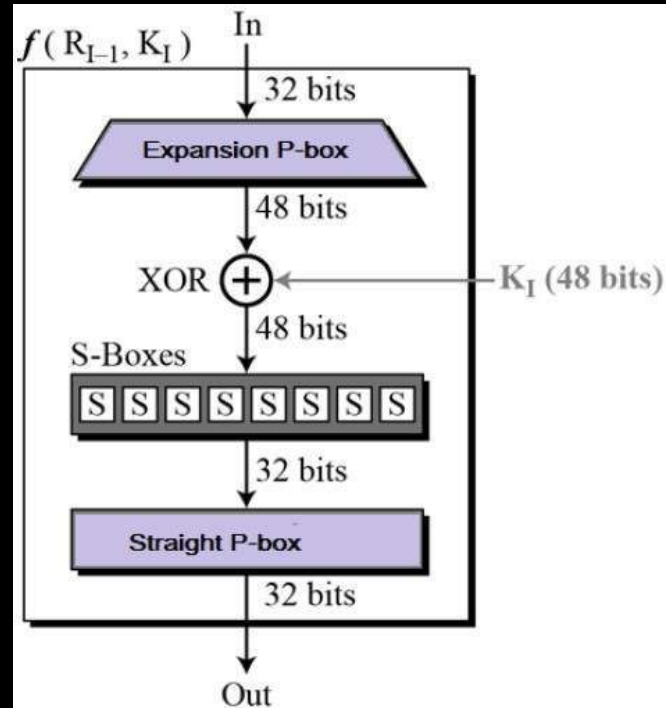
@amandasopkin



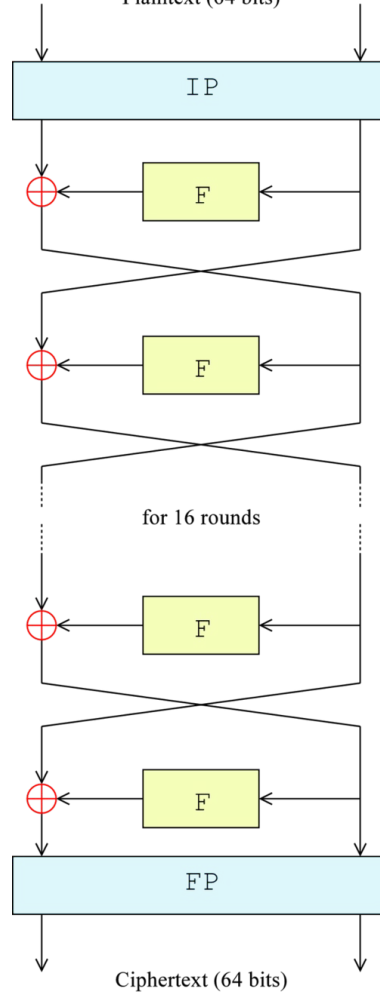
# DES

@amandasopkin

# DES



Plaintext (64 bits)



Ciphertext (64 bits)

# DES Criticism

- Shortened key length (56 bits)
- S-box structure

@amandasopkin

# DES Criticism

"NSA worked closely with IBM to strengthen the algorithm against all except brute-force attacks and to strengthen substitution tables, called S-boxes. Conversely, NSA tried to convince IBM to reduce the length of the key from 64 to 48 bits. Ultimately they compromised on a 56-bit key."

-American Cryptology During the Cold War



# DES Criticism

"We sent the S-boxes off to Washington.  
They came back and were all different."

-Alan Konheim

(one of the designers of DES)

20 years later...

"It took the academic  
community two decades to  
figure out that the NSA  
'tweaks' actually improved the  
security of DES."

-Bruce Schneier

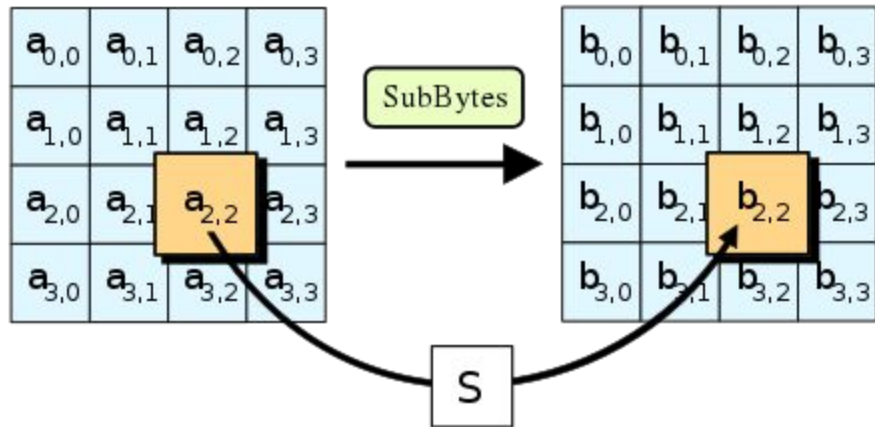
How effective was  
DES?

How effective was  
DES?



# 2000: Advanced Encryption Standard (Rijndael)

@amandasopkin



**AES = 128 bits!**

@amandasopkin



# Attacks on AES

@amandasopkin

# Attacks on AES

=> so far not practical

@amandasopkin

# Attacks on AES

=>

so far not practical

@amandasopkin

Attacks on [insert  
algorithm with  $x \geq 256$   
bit key strength here]  
=> so far not practical

@amandasopkin

How effective is  
AES?

How effective is  
AES?



# Crypto Wars

@amandasopkin

# WARNING

This shirt is classified as a munition and  
may not be exported from the United  
States, or shown to a foreign nation

## RSA

encryption in perl

```
#!/usr/bin/perl -w
use Crypt::RSA;
my $key = Crypt::RSA->new(1024);
my $text = "This is a test message";
my $cipher = $key->encrypt($text);
print $cipher;

```

Machine readable version of program: CO<sup>2</sup> Barcode





# Key size restrictions

@amandasopkin

1991: Sen. Biden introduced a bill requiring providers of electronic communication to provide voice, data, and other content to the government when authorized by law

1991: PGP  
(Pretty Good Privacy)

@amandasopkin

PGP: relies on math  
that is difficult to  
reverse

@amandasopkin

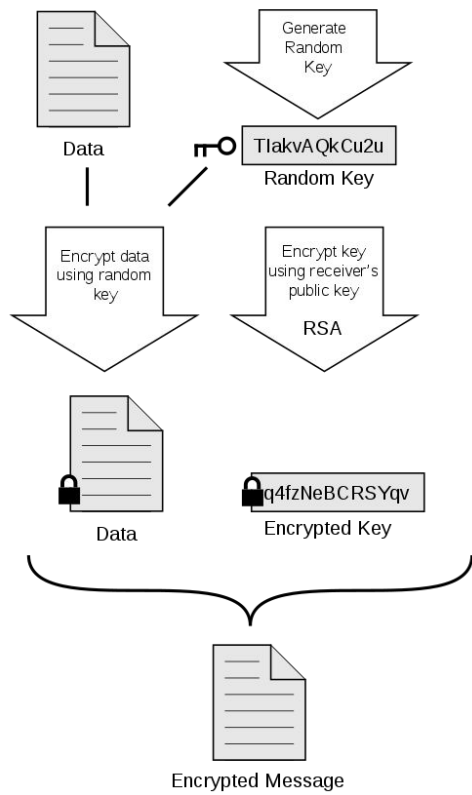
PGP = 3 keys

1. Public key

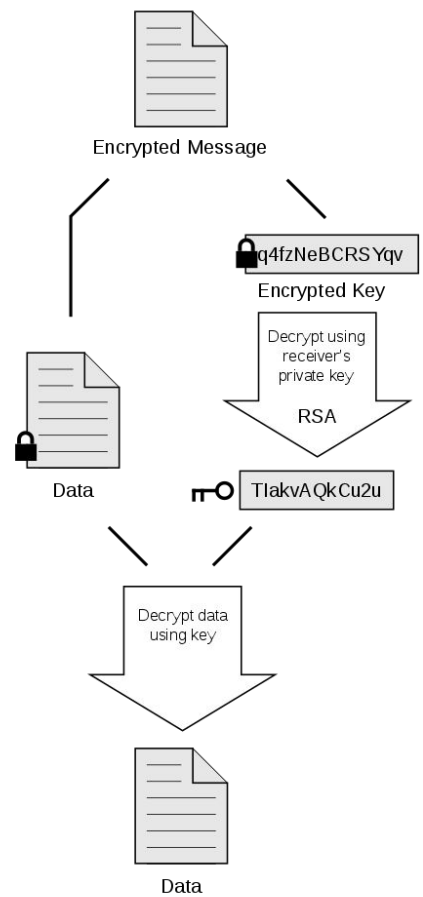
2. Private key

3. Encrypted key that  
gets sent

# Encrypt



# Decrypt



1. You generate a random key.
2. You use that key to encrypt your data.
3. I send you my public key.
4. My public key is used to encrypt your random key.
5. You send both the encrypted data and the encrypted random key to me.
6. I use my private key to decrypt your random key.
7. I use your random key to decrypt the data.



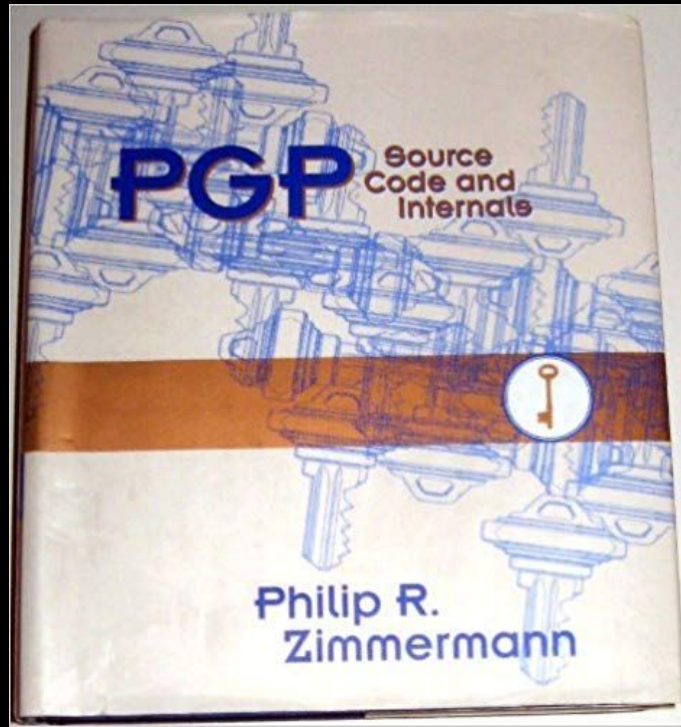
vs.



Phil Zimmerman/PGP

Criminal Investigation





Published by MIT press to allow export  
under 1st amendment



vs.



Phil Zimmerman/PGP: 1

Criminal Investigation: 0

# The end of crypto wars

@amandasopkin

# Randomness & Encryption

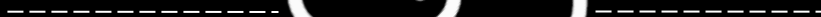
@amandasopkin

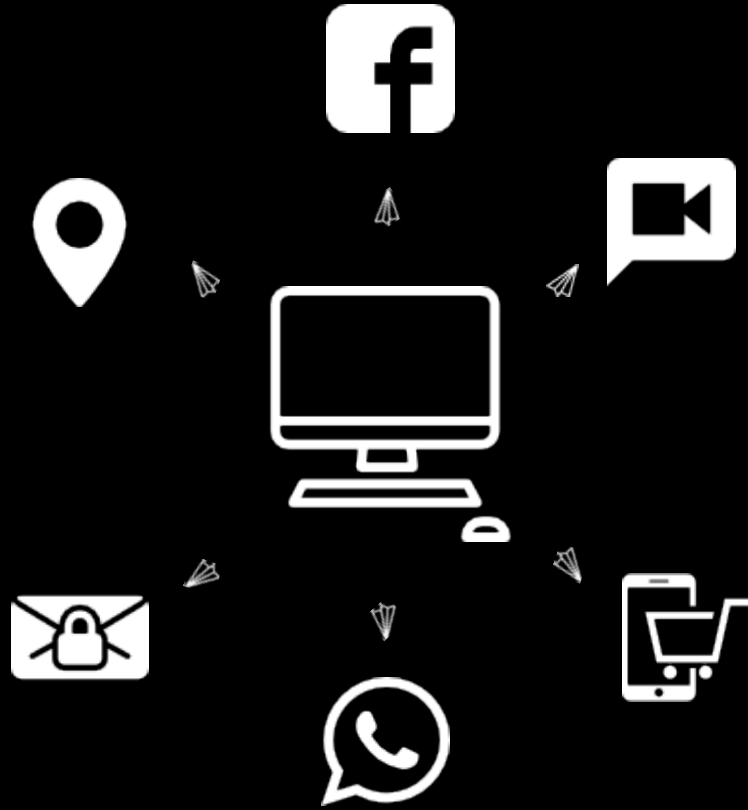
4oio342ip4o24p32o



4fdslf95454









# DUAL\_EC\_DRBG Controversy

- 2004: Dual EC PRNG introduced

800-90 and Dual EC DRBG

John Kelsey, NIST

# DUAL\_EC\_DRBG Controversy

- 08/2007: Shumow and Ferguson present Dual\_EC\_DRBG flaw at cryptography conference

On the Possibility of a Back Door  
in the NIST SP800-90 Dual Ec  
Prng

Dan Shumow  
Niels Ferguson  
Microsoft

# DUAL\_EC\_DRBG Controversy

- 11/2007: Schneier bases article in Wired on their findings

## Did NSA Put a Secret Backdoor in New Encryption Standard?

Bruce Schneier

*Wired*

November 15, 2007

## DUAL\_EC\_DRBG Controversy

“...would allow NSA to determine the state of the random number generator, and thereby eventually be able to read all data sent over the SSL connection.”

# The Washington Post

Printed on 100% recycled paper with soy-based inks.



Thunderstorm 6/20 • Tomorrow: Thunderstorm 6/20 • BEKANA, B4

MONDAY, JUNE 16, 2013

washingtonpost.com • B1, B5

## Man who leaked NSA secrets steps forward

A REPORTER'S ACCOUNT

To leaker, personal risks were clear

BY BARTON GELLMAN

He called me BRASSKANNER, a code name in the double-barreled style of the National Security Agency, where he worked in the signals intelligence directorate.

Vexx was the name he chose for himself, "truth teller" in Latin. I asked him early on, without reply, whether he intended to hint at the alternative fates that lay before him.

Two British dissenters had used the pseudonym. Clement Walker, a 17th-century detractor of Parliament, died in the brutal confines of the Tower of London. Two centuries later, social critic Henry Dunckley adopted "Vexx" as his byline over weekly columns in the Manchester Examiner. He was showered with testimonials

and an honorary degree.

Edward Joseph Snowden, 29, knew full well the risks he had undertaken and the awesome powers that would soon be arrayed to hunt for him. Pseudonyms were the least of his precautions as we corresponded from afar. Snowden was spilling some of the most sensitive secrets of a surveillance apparatus he had grown to detest. By late last month, he believed he was already "on the X" — exposure imminent.

"I understand that I will be made to suffer for my actions, and that the return of this information to the public marks my end," he wrote in early May, before we had our first direct contact. He warned that even journalists who

SNOWDEN CONTINUED ON A5



Before the world knew his name, tech specialist Edward Snowden, 29, now in Hong Kong, drafted a note of explanation. STORY, A1

### Risks of outsourcing

Government reliance on private spying contractors comes with costs as well as benefits. A2

### A historic leak

Edward Snowden receives praise and criticism as his name joins that of Daniel Ellsberg. A4

### EDWARD SNOWDEN: 'I'M NOT GOING TO HIDE'

Booz Allen consultant could face prosecution

BY BARTON GELLMAN,  
AARON BLAKE  
AND GREG MILLER

A 29-year-old man who says he is a former undercover CIA employee said Sunday that he was the principal source of recent disclosures about top secret National Security Agency programs, exposing himself to possible prosecution in an acknowledgment that had little if any precedent in the long history of U.S. intelligence leaks.

Edward Snowden, a tech specialist who has contracted for the NSA and works for the consulting firm Booz Allen Hamilton, unmasked himself as a source after a string of stories in The Washington Post and the Guardian that detailed previously unknown U.S.

surveillance programs. He said he disclosed secret documents in response to what he described as the systematic surveillance of innocent citizens.

In an interview Sunday, Snowden said he is willing to face the consequences of exposure.

"I'm not going to hide," Snowden told The Post from Hong Kong, where he has been staying. "Allowing the U.S. government to intimidate its people with threats of retaliation for revealing wrongdoing is contrary to the public interest."

Asked whether he believes that his disclosures will change anything, he said: "I think they already have. Everyone everywhere now understands how bad things

SURVEILLANCE CONTINUED ON A5

# DUAL\_EC\_DRBG Controversy

- 09/2013: One of the purposes of Bullrun is described as being "to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world."

## *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*

By NICOLE PERLROTH, JEFF LARSON and SCOTT SHANE SEPT. 5, 2013

# DUAL\_EC\_DRBG Controversy

- NIST recommends removal of the algorithm as a standard

NEWS

**NIST Removes Cryptography Algorithm from Random Number Generator Recommendations**

# DUAL\_EC\_DRBG Controversy

- 2004: Dual EC PRNG introduced
- 08/2007: Shumow and Ferguson present Dual\_EC\_DRBG flaw at cryptography conference
- 11/2007: Schneier bases article in Wired on their findings



# DUAL\_EC\_DRBG Controversy

- 09/2013: One of the purposes of Bullrun is described as being "to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world."
- 12/2013: Presidential advisory examines encryption standards
- 2014: Standard is removed

Years until standard removed...

10!

Who did this impact?

Microsoft, Google, Apple, McAfee,  
Docker, IBM, Oracle, Cisco, VMWare,  
Juniper, HP, Red Hat, Samsung,  
Toshiba, DELL, Ruckus, F5 Networks,  
Lenovo, Nokia, the RSA BSAFE  
libraries for Java and C++ and  
[more](#)....

Pro Tip:

Don't assume  
standardized = good



Modern Encryption...

Where are we now?

# Modern Encryption...



# Modern Encryption...



Pro Tip:

Often good security is  
not flashy

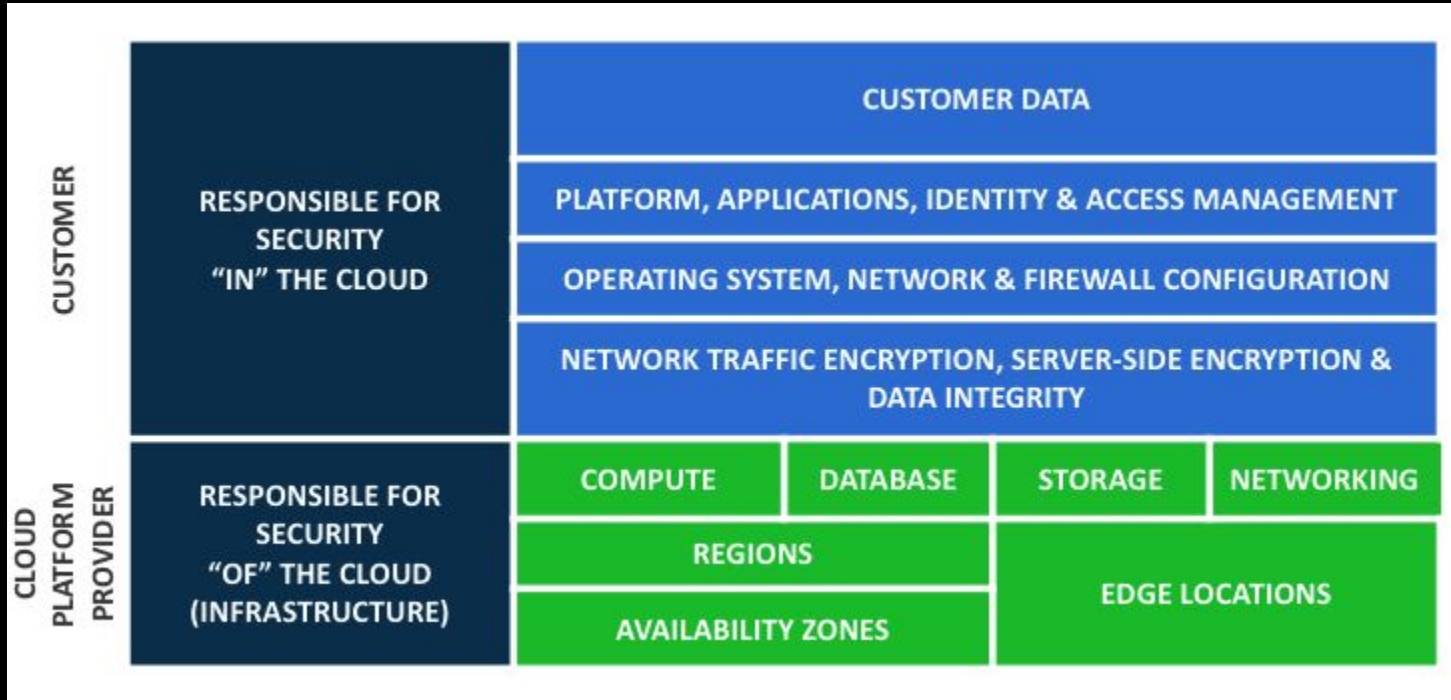




# Common breach causes

- ★ Not encrypting all the things
- ★ Using cloud storage without pre-encrypting
- ★ Using a poor random number generator

# Cloud encryption



Let's wrap up...



@amandasopkin

# Historical Encryption Lessons

Security != obscurity

Process is ESSENTIAL

Trust no one (kidding)

@amandasopkin

Something to say?

Amanda Sopkin

@amandasopkin



Thank you!



@amandasopkin

**THE END**

@amandasopkin

## Sources:

- Icons taken from flaticon.com
- <https://crypto.stackexchange.com/questions/51232/using-32-hexadecimal-digits-vs-ascii-equivalent-16-character-password>
- <https://dev.to/walker/pseudo-random-numbers-in-python-from-arithmetic-to-probability-distributions>
- Wired Magazine
- The Washington Post
- NYT
- <http://home.bt.com/tech-gadgets/cracking-the-enigma-code-how-turings-bombe-turned-the-tide-of-wwii-11363990654704>
- Geeks for Geeks
- Crypto Corner