

Week 1: Introduction to Cryptography

Jay Daigle

Occidental College

August 31, 2017

Three ways to hide messages

Three ways to hide messages

- Steganography

Three ways to hide messages

- Steganography
- Codes

Three ways to hide messages

- Steganography
- Codes
- Ciphers

I am resigning from my position as Science Envoy for the Department of State of the United States. Since 1996, I have served the Departments of Energy, the US Environmental Protection Agency, and the State Department in a number of roles. Working closely with the talented teams at State Department Headquarters and at U. S. embassies abroad, we have built significant partnerships in North and East Africa, and in the Middle East, around shared visions of national security, job creation in the U. S. and sustainable energy.

My decision to resign is in response to your attacks on core values of the United States. Your failure to condemn white supremacists and neo-Nazis has domestic and international ramifications. On this issue, I stand with the unequivocal and authoritative statements of Charlottesville Mayor Mike Signer, Virginia Governor Terry McAuliffe, Ohio Governor John Kasich, Senator John McCain, Congresswoman Ileana Ros-Lehtinen, Governor Arnold Schwarzenegger, Presidents George H. W. Bush and George W. Bush, Dr. Cornel West, Linda Sarsour, the Palestinian-American activist and one of the organizers of the Women's March, and many others.

Particularly troubling to me is how your response to Charlottesville is consistent with a broader pattern of behavior that enables sexism and racism, and disregards the welfare of all Americans, the global community and the planet.

Examples of this destructive pattern have consequences on my duties as Science Envoy. Your decision to abdicate the leadership opportunities and the job creation benefits of the Paris Climate Accord, and to undermine energy and environmental research are not acceptable to me.

Acts and words matter. To continue in my role under your administration would be inconsistent with the principles of the United States Oath of Allegiance to which I adhere.

Character is vital in leadership. I find particularly wise the admonition of President Dwight D. Eisenhower, who cautioned that, "A people [or person] that values its privileges above principles soon loses both."

Herein, with regret, I resign. I deeply respect and value the work of the many fine people I have encountered in our federal agencies and will miss the opportunity to work with and support them. Your actions to date have, sadly, harmed the quality of life in the United States, our standing abroad, and the sustainability of the planet.

Dan Kammen's resignation letter

I am resigning from my position as Science Envoy for the Department of State of the United States. Since 1996, I have served the Departments of Energy, the US Environmental Protection Agency, and the State Department in a number of roles. Working closely with the talented teams at State Department Headquarters and at U. S. embassies abroad, we have built significant partnerships in North and East Africa, and in the Middle East, around shared visions of national security, job creation in the U. S. and sustainable energy.

My decision to resign is in response to your attacks on core values of the United States. Your failure to condemn white supremacists and neo-Nazis has domestic and international ramifications. On this issue, I stand with the unequivocal and authoritative statements of Charlottesville Mayor Mike Signer, Virginia Governor Terry McAuliffe, Ohio Governor John Kasich, Senator John McCain, Congresswoman Ileana Ros-Lehtinen, Governor Arnold Schwarzenegger, Presidents George H. W. Bush and George W. Bush, Dr. Cornel West, Linda Sarsour, the Palestinian-American activist and one of the organizers of the Women's March, and many others.

Particularly troubling to me is how your response to Charlottesville is consistent with a broader pattern of behavior that enables sexism and racism, and disregards the welfare of all Americans, the global community and the planet.

Examples of this destructive pattern have consequences on my duties as Science Envoy. Your decision to abdicate the leadership opportunities and the job creation benefits of the Paris Climate Accord, and to undermine energy and environmental research are not acceptable to me.


Acts and words matter. To continue in my role under your administration would be inconsistent with the principles of the United States Oath of Allegiance to which I adhere.

Character is vital in leadership. I find particularly wise the admonition of President Dwight D. Eisenhower, who cautioned that, "A people [or person] that values its privileges above principles soon loses both."

Herein, with regret, I resign. I deeply respect and value the work of the many fine people I have encountered in our federal agencies and will miss the opportunity to work with and support them. Your actions to date have, sadly, harmed the quality of life in the United States, our standing abroad, and the sustainability of the planet.

Dan Kammen's resignation letter with a hidden message



 britneyspears [Follow](#)

421,451 likes 4w

britneyspears Such a great shoot with @david_roemer

[view all 6,742 comments](#)

[pacheco8380](#) Flakita hermosa 🥰🥰

[lerka24](#) 🥰🥰🥰

[gabbyhyman](#) @ndeblasio

[olya_1296](#) БайКрасотка)

[victoriamiller_official](#) 🥰🥰🥰

[andreehelena](#) @azumpano she looks like old Brit!!! 🥰

[asmith2155](#) #2hot make loved to her, uupss #Hot #X

[meela_universe](#) Still hot!

[lilyabraun](#) 🥰🥰🥰

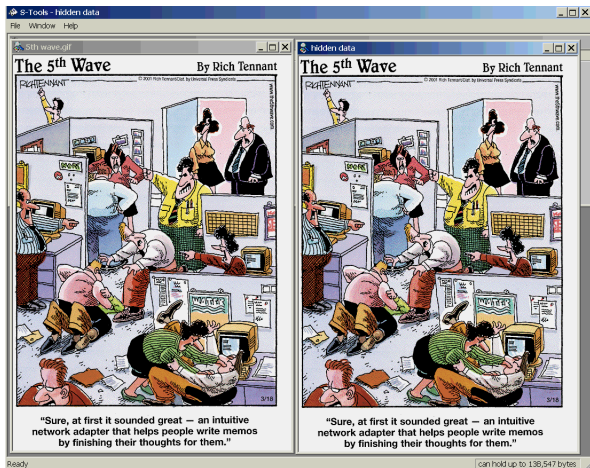
[limonnn.c](#) Saatlerce sikmek isterdim

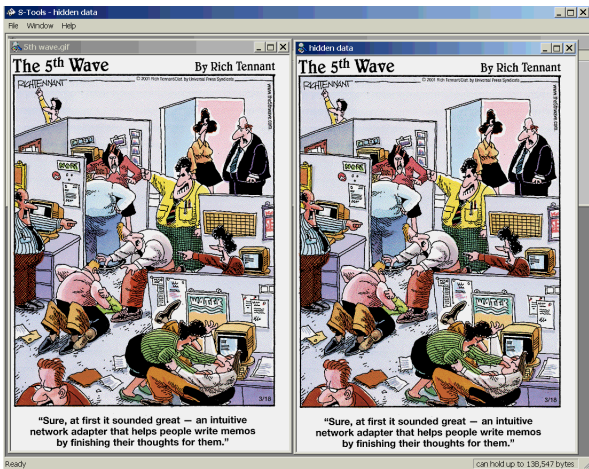
[thenotoriouscma](#) Iconic @cheriemadelein

[shylasvsyoga](#) @carlos_misan_tropo

[Log in](#) to like or comment. ⋮

Russian hackers controlling their botnets
Screenshot by ESET





The picture on the right contains 14 kb of hidden text content.
<http://www.garykessler.net/library/steganography.html>



MY HOBBY: FOLLOWING FIELD BIOLOGISTS AROUND AND INTERPRETING EVERYTHING THEY SAY AS CODE PHRASES.

<https://xkcd.com/733/>



Japanese code book from 1941
Bletchley Park

31788	此ノ外	32427	之ニ反以
95184	此ノ附近	49515	之ニ異計
18598	此ノ限ニ在ラス[イム]	85233	之ニ重計
74445	此ノ件	38258	之ニ對計
88597	此ノ期間	24135	之ニ要計
98211	此ノ機	87389	之ヲ
55683	此ノ機會	60688	之ヲ單送
85638	此ノ儀	12219	之ヲ單應
61137	此ノ旨	81024	之ヲ次單

Each five-digit string corresponds to a word, but there is no pattern.

Alice wants to communicate securely with Bob.

Alice wants to communicate securely with Bob.
Eve wants to eavesdrop.

Alice wants to communicate securely with Bob.

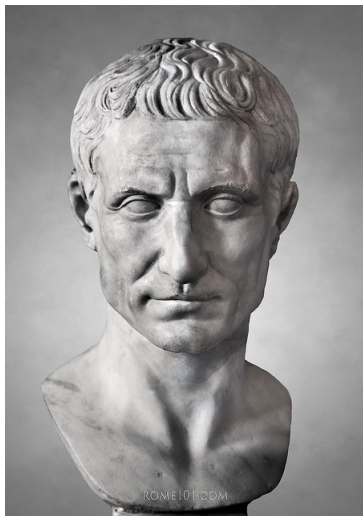
Eve wants to eavesdrop.

Without the key, Eve can't get the plaintext from intercepting the ciphertext.

Alice wants to communicate securely with Bob.

Eve wants to eavesdrop.

Without the key, Eve can't get the plaintext from intercepting the ciphertext. But Bob has the key, so he can!



A Caesar Cipher Example

Plaintext		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
Ciphertext		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

A Caesar Cipher Example

Plaintext	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
Ciphertext	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

QEFP JBPPXDB EXP YBBK BKZFMEOBA YV X ZXBPXO ZFMEBO

TFQE X PEFCQ LC QEOBB

A Caesar Cipher Example

Plaintext	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
Ciphertext	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

QEFP JBPPXDB EXP YBBK BKZFMEBOBA YV X ZXPXO ZFMEBO
 THIS MESSAGE HAS BEEN ENCIPHERED BY A CAESAR CIPHER

TFQE X PEFCQ LC QEOBB
 WITH A SHIFT OF THREE

Breaking the Cipher

Breaking the Cipher

IWXH RXEWTG XH HWXUITS QN TATKTC

Breaking the Cipher

IWXH RXEWTG XH HWXUITS QN TATKTC

Breaking the Cipher

IWXH RXEWTG XH HWXUITS QN TATKTC

0	IWXH	7	PDEO	14	WKLV	21	DRSC
1	JXYI	8	QEFP	15	XLMW	22	ESTD
2	KYZJ	9	RFGQ	16	YMNX	23	FTUE
3	LZAK	10	SGHR	17	ZNOY	24	GUVF
4	MABL	11	THIS	18	AOPZ	25	HVWG
5	NBCM	12	UIJT	19	BPQA		
6	OCDN	13	VJKU	20	CQRB		

Breaking the Cipher

IWXH RXEWTG XH HWXUITS QN TATKTC

0	IWXH	7	PDEO	14	WKLV	21	DRSC
1	JXYI	8	QEFP	15	XLMW	22	ESTD
2	KYZJ	9	RFGQ	16	YMNX	23	FTUE
3	LZAK	10	SGHR	17	ZNOY	24	GUVF
4	MABL	11	THIS	18	AOPZ	25	HVWG
5	NBCM	12	UIJT	19	BPQA		
6	OCDN	13	VJKU	20	CQRB		

Breaking the Cipher

IWXH RXEWTG XH HWXUITS QN TATKTC
 THIS CIPHER IS SHIFTED BY ELEVEN

0	IWXH	7	PDEO	14	WKLV	21	DRSC
1	JXYI	8	QEFP	15	XLMW	22	ESTD
2	KYZJ	9	RFGQ	16	YMNX	23	FTUE
3	LZAK	10	SGHR	17	ZNOY	24	GUVF
4	MABL	11	THIS	18	AOPZ	25	HVWG
5	NBCM	12	UIJT	19	BPQA		
6	OCDN	13	VJKU	20	CQRB		

CWU HLY UXN BCM WUH SIO

CWU HLY UXN BCM WUH SIO

CWU HLY UXN BCM WUH SIO

0	CWU	7	JDB	14	QKI	21	XRP
1	DXV	8	KEC	15	RLJ	22	YSQ
2	EYW	9	LFD	16	SMK	23	ZTR
3	FZX	10	MGE	17	TNL	24	AUS
4	GAY	11	NHF	18	UOM	25	BVT
5	HBZ	12	OIG	19	VPN		
6	ICA	13	PJH	20	WQO		

CWU HLY UXN BCM WUH SIO

0	CWU	7	JDB	14	QKI	21	XRP
1	DXV	8	KEC	15	RLJ	22	YSQ
2	EYW	9	LFD	16	SMK	23	ZTR
3	FZX	10	MGE	17	TNL	24	AUS
4	GAY	11	NHF	18	UOM	25	BVT
5	HBZ	12	OIG	19	VPN		
6	ICA	13	PJH	20	WQO		

4, 6, 12, 24

CWU HLY UXN BCM WUH SIO

CWU HLY UXN BCM WUH SIO

0	CWUHL Y	7	JDBOSF	14	QKIVZM	21	XRPCGT
1	DXVIMZ	8	KECPTG	15	RLJWAN	22	YSQDHU
2	EYWJNA	9	LFDQUH	16	SMKXBO	23	ZTREIV
3	FZXKOB	10	MGERVI	17	TNLYCP	24	AUSFJW
4	GAYLPC	11	NHFSWJ	18	UOMZDQ	25	BVTGKX
5	HBZMQD	12	OIGTXK	19	VPNAER		
6	ICANRE	13	PJHUYL	20	WQOBFS		

CWU HLY UXN BCM WUH SIO

0	CWUHL Y	7	JDBOSF	14	QKIVZM	21	XRPCGT
1	DXVIMZ	8	KECPTG	15	RLJWAN	22	YSQDHU
2	EYWJNA	9	LFDQUH	16	SMKXBO	23	ZTREIV
3	FZXKOB	10	MGERVI	17	TNLYCP	24	AUSFJW
4	GAYLPC	11	NHFSWJ	18	UOMZDQ	25	BVTGKX
5	HBZMQD	12	OIGTXK	19	VPNAER		
6	ICANRE	13	PJHUYL	20	WQOBFS		

CWU HLY UXN BCM WUH SIO

0	CWUHL Y	7	JDBOSF	14	QKIVZM	21	XRPCGT
1	DXVIMZ	8	KECPTG	15	RLJWAN	22	YSQDHU
2	EYWJNA	9	LFDQUH	16	SMKXBO	23	ZTREIV
3	FZXKOB	10	MGERVI	17	TNLYCP	24	AUSFJW
4	GAYLPC	11	NHFSWJ	18	UOMZDQ	25	BVTGKX
5	HBZMQD	12	OIGTXK	19	VPNAER		
6	ICANRE	13	PJHUYL	20	WQOBFS		

ICA NRE ADT HIS CAN YOU

CWU HLY UXN BCM WUH SIO

0	CWUHL Y	7	JDBOSF	14	QKIVZM	21	XRPCGT
1	DXVIMZ	8	KECPTG	15	RLJWAN	22	YSQDHU
2	EYWJNA	9	LFDQUH	16	SMKXBO	23	ZTREIV
3	FZXKOB	10	MGERVI	17	TNLYCP	24	AUSFJW
4	GAYLPC	11	NHFSWJ	18	UOMZDQ	25	BVTGKX
5	HBZMQD	12	OIGTXK	19	VPNAER		
6	ICANRE	13	PJHUYL	20	WQOBFS		

ICA NRE ADT HIS CAN YOU

I can read this. Can you?

Definition (Congruence)

$a \equiv b \pmod{m}$ if $m \mid b - a$.

Definition (Congruence)

$a \equiv b \pmod{m}$ if $m \mid b - a$.

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
Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Definition (Congruence)

$a \equiv b \pmod{m}$ if $m \mid b - a$.

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
Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
	M	E	E	T	M	E	A	T	M	I	D	N	I	G	H	T										

Definition (Congruence)

$a \equiv b \pmod{m}$ if $m \mid b - a$.

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	
Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
M	E	E	T	M	E	A	T	M	I	D	N	I	G	H	T												
12	4	4	19	12	4	0	19	12	8	3	13	8	6	7	19												

Definition (Congruence)

$a \equiv b \pmod{m}$ if $m \mid b - a$.

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
Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
M	E	E	T	M	E	A	T	M	I	D	N	I	G	H	T											
12	4	4	19	12	4	0	19	12	8	3	13	8	6	7	19											
1	19	19	8	1	19	15	8	1	23	18	7	23	21	22	8											

Definition (Congruence)

$a \equiv b \pmod{m}$ if $m \mid b - a$.

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
Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
M	E	E	T	M	E	A	T	M	I	D	N	I	G	H	T											
12	4	4	19	12	4	0	19	12	8	3	13	8	6	7	19											
1	19	19	8	1	19	15	8	1	23	18	7	23	21	22	8											
B	T	T	I	B	T	P	I	B	X	S	H	X	V	W	I											

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

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

THIS IS A SIMPLE SUBSTITUTION CIPHER

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

THIS IS A SIMPLE SUBSTITUTION CIPHER

O

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

THIS IS A SIMPLE SUBSTITUTION CIPHER
OB

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

THIS IS A SIMPLE SUBSTITUTION CIPHER
OBH

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

THIS IS A SIMPLE SUBSTITUTION CIPHER
OBHM

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

THIS IS A SIMPLE SUBSTITUTION CIPHER
OBHM HM G MHSTNE MVIMOHVOHFD LHTBEU

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

THIS IS A SIMPLE SUBSTITUTION CIPHER
 OBHM HM G MHSTNE MVIMOHVOHFD LHTBEU

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

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

THIS IS A SIMPLE SUBSTITUTION CIPHER
 OBHM HM G MHSTNE MVIMOHVOHFD LHTBEU

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

How many possible keys?

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

THIS IS A SIMPLE SUBSTITUTION CIPHER
 OBHM HM G MHSTNE MVIMOHVOHFD LHTBEU

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

How many possible keys?
 26!

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

THIS IS A SIMPLE SUBSTITUTION CIPHER
 OBHM HM G MHSTNE MVIMOHVOHFD LHTBEU

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

How many possible keys?

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

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

THIS IS A SIMPLE SUBSTITUTION CIPHER
 OBHM HM G MHSTNE MVIMOHVOHFD LHTBEU

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

How many possible keys?

$$26! = 403,291,461,126,605,635,584,000,000 \approx 4 \times 10^{26}$$

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

THIS IS A SIMPLE SUBSTITUTION CIPHER
 OBHM HM G MHSTNE MVIMOHVOHFD LHTBEU

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

How many possible keys?

$$26! = 403,291,461,126,605,635,584,000,000 \approx 4 \times 10^{26} \approx 2^{88}.$$

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

THIS IS A SIMPLE SUBSTITUTION CIPHER
 OBHM HM G MHSTNE MVIMOHVOHFD LHTBEU

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

How many possible keys?

$26! = 403,291,461,126,605,635,584,000,000 \approx 4 \times 10^{26} \approx 2^{88}$.

Not as secure as this looks, because of statistical properties of English.



Giovan Battista Bellaso (1505 – ?)



Giovan Battista Bellaso (1505 – ?)
Invented the Vigenère cipher.



Blaise de Vigenère (1523-1596)



Blaise de Vigenère (1523-1596)
Did not invent the Vigenère cipher.



Blaise de Vigenère (1523-1596)
Did not invent the Vigenère cipher.
Got the credit anyway.



Blaise de Vigenère (1523-1596)
Did not invent the Vigenère cipher.
Got the credit anyway.

Stigler's Law of Eponymy

No scientific discovery is named after its discoverer.



Blaise de Vigenère (1523-1596)
Did not invent the Vigenère cipher.
Got the credit anyway.

Stigler's Law of Eponymy

No scientific discovery is named after its discoverer.
(Attributed to Robert Merton.)

How does it work?

How does it work?

Choose a keyword. Write the keyword down repeatedly until you have a string of letters as long as your message. This is the *keystream*.

How does it work?

Choose a keyword. Write the keyword down repeatedly until you have a string of letters as long as your message. This is the *keystream*. For each letter of your plaintext, add the corresponding letter from your keystream. This gives the ciphertext.

How does it work?

Choose a keyword. Write the keyword down repeatedly until you have a string of letters as long as your message. This is the *keystream*.

For each letter of your plaintext, add the corresponding letter from your keystream. This gives the ciphertext.

To decrypt, generate the keystream as before, and then subtract it from the ciphertext to get the plaintext.

Example

Example

Plaintext | I L O V E C R Y P T O L O G Y

Example

Plaintext		I	L	O	V	E	C	R	Y	P	T	O	L	O	G	Y
Keystream		M	A	T	H	M	A	T	H	M	A	T	H	M	A	T

Example

Plaintext		I	L	O	V	E	C	R	Y	P	T	O	L	O	G	Y
Keystream		M	A	T	H	M	A	T	H	M	A	T	H	M	A	T
Plaintext		8	11	14	21	4	2	17	24	15	19	14	11	14	6	24
Keystream		12	0	19	7	12	0	19	7	12	0	19	7	12	0	19

Example

Plaintext		I	L	O	V	E	C	R	Y	P	T	O	L	O	G	Y
Keystream		M	A	T	H	M	A	T	H	M	A	T	H	M	A	T
Plaintext		8	11	14	21	4	2	17	24	15	19	14	11	14	6	24
Keystream		12	0	19	7	12	0	19	7	12	0	19	7	12	0	19
Ciphertext		20														
Ciphertext		U														

Example

Plaintext		I	L	O	V	E	C	R	Y	P	T	O	L	O	G	Y
Keystream		M	A	T	H	M	A	T	H	M	A	T	H	M	A	T
Plaintext		8	11	14	21	4	2	17	24	15	19	14	11	14	6	24
Keystream		12	0	19	7	12	0	19	7	12	0	19	7	12	0	19
Ciphertext		20	11													
Ciphertext		U	L													

Example

Plaintext		I	L	O	V	E	C	R	Y	P	T	O	L	O	G	Y
Keystream		M	A	T	H	M	A	T	H	M	A	T	H	M	A	T
Plaintext		8	11	14	21	4	2	17	24	15	19	14	11	14	6	24
Keystream		12	0	19	7	12	0	19	7	12	0	19	7	12	0	19
Ciphertext		20	11	7												
Ciphertext		U	L	H												

Example

Plaintext		I	L	O	V	E	C	R	Y	P	T	O	L	O	G	Y
Keystream		M	A	T	H	M	A	T	H	M	A	T	H	M	A	T
Plaintext		8	11	14	21	4	2	17	24	15	19	14	11	14	6	24
Keystream		12	0	19	7	12	0	19	7	12	0	19	7	12	0	19
Ciphertext		20	11	7	2	16	2	10	3	1	19	7	18	0	6	17
Ciphertext		U	L	H	C	Q	C	K	D	B	T	H	S	A	G	R

Example

Plaintext		I	L	O	V	E	C	R	Y	P	T	O	L	O	G	Y
Keystream		M	A	T	H	M	A	T	H	M	A	T	H	M	A	T
Plaintext		8	11	14	21	4	2	17	24	15	19	14	11	14	6	24
Keystream		12	0	19	7	12	0	19	7	12	0	19	7	12	0	19
Ciphertext		20	11	7	2	16	2	10	3	1	19	7	18	0	6	17
Ciphertext		U	L	H	C	Q	C	K	D	B	T	H	S	A	G	R

ILOVECRYPTOLOGY

ULHCQCKDBTHSAGR

Computers encode data in *binary* strings of ones and zeroes.

Computers encode data in *binary* strings of ones and zeroes.
We can view them as using an alphabet with two “letters”.

Computers encode data in *binary* strings of ones and zeroes. We can view them as using an alphabet with two “letters”. Monoalphabetic substitution is totally useless here, because there are $2! = 2$ possible keys. But the Vigenere cipher is not.

Suppose our key “word” is 10010011

Suppose our key “word” is 10010011 and our plaintext message is
01010000 01001111 01001011 01000101 00100000 00110101 00111001
00110100 00110101 00111000 00101100 00110110 00110010.

Suppose our key “word” is 10010011 and our plaintext message is
01010000 01001111 01001011 01000101 00100000 00110101 00111001
00110100 00110101 00111000 00101100 00110110 00110010.

Then keystream is

10010011 10010011 10010011 10010011 10010011 10010011 10010011
10010011 10010011 10010011 10010011 10010011 10010011.

Suppose our key “word” is 10010011 and our plaintext message is
01010000 01001111 01001011 01000101 00100000 00110101 00111001
00110100 00110101 00111000 00101100 00110110 00110010.

Then keystream is

10010011 10010011 10010011 10010011 10010011 10010011 10010011
10010011 10010011 10010011 10010011 10010011 10010011.

Adding the two yields a ciphertext of

11000011 11011100 11011000 11010110 10110011 10100110 10101010
10100111 10100110 10101011 10111111 10100101 10100001.

Vigenère's actual innovation was to use the plaintext itself to form the keystream. In this sort of cipher, the keystream is the keyword followed by the plaintext.

Vigenère's actual innovation was to use the plaintext itself to form the keystream. In this sort of cipher, the keystream is the keyword followed by the plaintext.

Plaintext		I	L	O	V	E	C	R	Y	P	T	O	L	O	G	Y
Keystream		M	A	T	H	I	L	O	V	E	C	R	Y	P	T	O

Vigenère's actual innovation was to use the plaintext itself to form the keystream. In this sort of cipher, the keystream is the keyword followed by the plaintext.

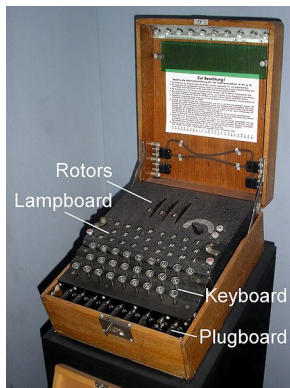
Plaintext		I	L	O	V	E	C	R	Y	P	T	O	L	O	G	Y
Keystream		M	A	T	H	I	L	O	V	E	C	R	Y	P	T	O
Plaintext		8	11	14	21	4	2	17	24	15	19	14	11	14	6	24
Keystream		12	0	19	7	8	11	14	21	4	2	17	24	15	19	14

Vigenère's actual innovation was to use the plaintext itself to form the keystream. In this sort of cipher, the keystream is the keyword followed by the plaintext.

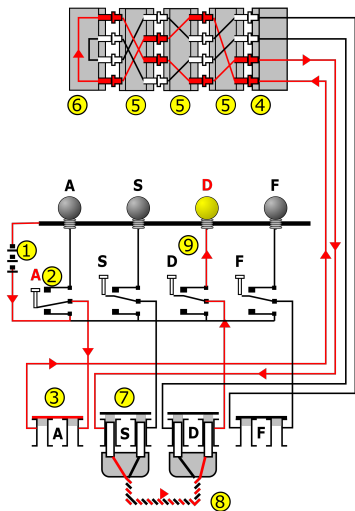
Plaintext	I L O V E C R Y P T O L O G Y
Keystream	M A T H I L O V E C R Y P T O
Plaintext	8 11 14 21 4 2 17 24 15 19 14 11 14 6 24
Keystream	12 0 19 7 8 11 14 21 4 2 17 24 15 19 14
Ciphertext	20 11 7 2 12 13 5 19 19 21 5 9 3 25 12
Ciphertext	U L H C M N F T T V F J D Z M

The Enigma

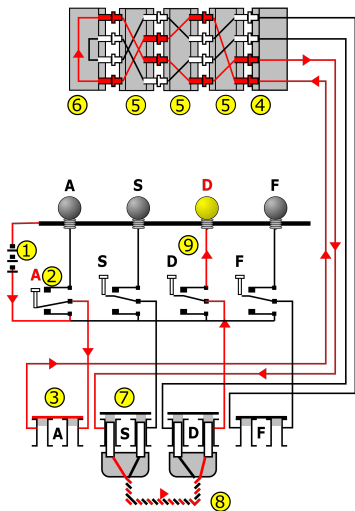
The Enigma



The Enigma Machine



Licensed by MesserWoland under
CC BY-SA 3.0.



Simplified Enigma wiring diagram. Looks complicated, but is just a complicated autokey algorithm.

Licensed by MesserWoland under
CC BY-SA 3.0.

Modern Stream Ciphers

There are a number of modern usable stream cipher algorithms. These usually involve plugging key data into a pseudorandom number generator to generate a keystream.

Modern Stream Ciphers

There are a number of modern usable stream cipher algorithms. These usually involve plugging key data into a pseudorandom number generator to generate a keystream. There are two big weaknesses that limit the use of stream ciphers. In order to maintain security, a stream cipher must:

Modern Stream Ciphers

- There are a number of modern usable stream cipher algorithms. These usually involve plugging key data into a pseudorandom number generator to generate a keystream.
- There are two big weaknesses that limit the use of stream ciphers. In order to maintain security, a stream cipher must:
- Use a different key for every message;

Modern Stream Ciphers

- There are a number of modern usable stream cipher algorithms. These usually involve plugging key data into a pseudorandom number generator to generate a keystream.
- There are two big weaknesses that limit the use of stream ciphers. In order to maintain security, a stream cipher must:
- Use a different key for every message; and
 - Produce a keystream that has a long period before repeating itself.

Modern Stream Ciphers

- There are a number of modern usable stream cipher algorithms. These usually involve plugging key data into a pseudorandom number generator to generate a keystream.
- There are two big weaknesses that limit the use of stream ciphers. In order to maintain security, a stream cipher must:
- Use a different key for every message; and
 - Produce a keystream that has a long period before repeating itself.
- Most cryptography in use today uses other principles, which we will discuss later on in the course.