Introduction to Number Theory and Cryptography (MAS3214)

Michael C. White

Newcastle University

2016

Sending Secret Messages

Transmitting over an Open Channel

Sending Secret Messages

Transmitting over an Open Channel

Alice	Bob
$\ominus$!	$\ominus$?
$\leftarrow \Delta \rightarrow$	$\leftarrow \Box \rightarrow$
$\rfloor \lfloor$	$\prod$

Sending Secret Messages

Transmitting over an Open Channel

Alice	Bob
$\ominus$!	$\ominus$?
$\leftarrow \Delta \rightarrow$	$\leftarrow \square \rightarrow$
$\rfloor \lfloor$	$\prod$

$\boxed{\texttt{PLAINTEXT}}$

Sending Secret Messages

Transmitting over an Open Channel

Alice	Bob
$\ominus$!	$\ominus$?
$\leftarrow \Delta \rightarrow$	$\leftarrow \Box \rightarrow$
$\rfloor\lfloor$	$\prod$

$\boxed{\texttt{PLAINTEXT}}$

$\Downarrow$ **Encode**

$\boxed{\texttt{ciphertext}}$

Transmitting over an Open Channel

Alice	Bob
$\ominus$!	$\ominus$?
$\leftarrow \Delta \rightarrow$	$\leftarrow \Box \rightarrow$
$\rfloor\lfloor$	$\prod$

`PLAINTEXT`

$\Downarrow$ **Encode**

`ciphertext` $\xrightarrow{\textit{transmission}}$ `ciphertext`

Sending Secret Messages

Transmitting over an Open Channel

Alice	Bob
$\ominus$!	$\ominus$?
$\leftarrow \Delta \rightarrow$	$\leftarrow \Box \rightarrow$
$\rfloor\lfloor$	$\prod$
$\boxed{\texttt{PLAINTEXT}}$	$\boxed{\texttt{PLAINTEXT}}$
$\Downarrow$ **Encode**	$\Uparrow$ **Decode**

$$\boxed{\texttt{ciphertext}} \xrightarrow{\textit{transmission}} \boxed{\texttt{ciphertext}}$$

Sending Secret Messages

Transmitting over an Open Channel

Alice	Bob
$\ominus$!	$\ominus$?
$\leftarrow \Delta \rightarrow$	$\leftarrow \square \rightarrow$
$\rfloor\lfloor$	$\prod$
$\boxed{\texttt{PLAINTEXT}}$	$\boxed{\texttt{PLAINTEXT}}$
$\Downarrow$ **Encode**	$\Uparrow$ **Decode**

$$\boxed{\texttt{ciphertext}} \quad \xrightarrow{\textit{transmission}} \quad \boxed{\texttt{ciphertext}}$$

Weaknesses

Transmitting over an Open Channel

Alice	Bob
$\ominus$!	$\ominus$?
$\leftarrow \Delta \rightarrow$	$\leftarrow \square \rightarrow$
$\rfloor\lfloor$	$\prod$
$\boxed{\texttt{PLAINTEXT}}$	$\boxed{\texttt{PLAINTEXT}}$
$\Downarrow$ **Encode**	$\Uparrow$ **Decode**

$$\boxed{\texttt{ciphertext}} \xrightarrow{\textit{transmission}} \boxed{\texttt{ciphertext}}$$

Weaknesses

- Bob needs to know how to decipher Alice's message.

Sending Secret Messages

Transmitting over an Open Channel

Alice	Bob
$\ominus$!	$\ominus$?
$\leftarrow \Delta \rightarrow$	$\leftarrow \square \rightarrow$
$\rfloor\lfloor$	$\prod$
$\boxed{\texttt{PLAINTEXT}}$	$\boxed{\texttt{PLAINTEXT}}$
$\Downarrow$ **Encode**	$\Uparrow$ **Decode**

$$\boxed{\texttt{ciphertext}} \xrightarrow{\textit{transmission}} \boxed{\texttt{ciphertext}}$$

Weaknesses

- Bob needs to know how to decipher Alice's message.
- Someone else may work out how to decode the message.

Encryption by Shifting Letters

The Caesar Cipher

Encryption by Shifting Letters

PLAINTEXT		B	R	U	T	E	F	O	R	C	E

encryption $\downarrow$ using $A \mapsto b$

ciphertext		c	s	v	u	f	g	p	s	d	f

The Caesar Cipher

Encryption by Shifting Letters

PLAINTEXT		B	R	U	T	E	F	O	R	C	E

encryption $\downarrow$ using $A \mapsto b$

ciphertext		c	s	v	u	f	g	p	s	d	f

Weaknesses

The Caesar Cipher

Encryption by Shifting Letters

PLAINTEXT		B	R	U	T	E	F	O	R	C	E

encryption $\downarrow$ using $A \mapsto b$

ciphertext		c	s	v	u	f	g	p	s	d	f

Weaknesses

- There are only 26 codes to try. [Rot13 is still used.]

The Caesar Cipher

Encryption by Shifting Letters

PLAINTEXT		B	R	U	T	E	F	O	R	C	E

encryption $\downarrow$ using $A \mapsto b$

ciphertext		c	s	v	u	f	g	p	s	d	f

Weaknesses

- There are only 26 codes to try. [Rot13 is still used.]
- This is a rather easy process to do backwards. [zyxwvutsr. . .]

The Caesar Cipher

Encryption by Shifting Letters

PLAINTEXT		B	R	U	T	E	F	O	R	C	E

encryption $\downarrow$ using $A \mapsto b$

ciphertext		c	s	v	u	f	g	p	s	d	f

Weaknesses

- There are only 26 codes to try. [Rot13 is still used.]
- This is a rather easy process to do backwards. [zyxwvutsr. . .]
- Decode: mpm!

The Caesar Cipher

Encryption by Shifting Letters

PLAINTEXT		B	R	U	T	E	F	O	R	C	E

encryption $\Big\downarrow$ using $A \mapsto b$

ciphertext		c	s	v	u	f	g	p	s	d	f

Weaknesses

- There are only 26 codes to try. [Rot13 is still used.]
- This is a rather easy process to do backwards. [zyxwvutsr. . .]
- Decode: mpm!

- LOL!

The Caesar Cipher

Encryption by Shifting Letters

PLAINTEXT		B	R	U	T	E	F	O	R	C	E

encryption $\downarrow$ using $A \mapsto b$

ciphertext		c	s	v	u	f	g	p	s	d	f

Weaknesses

- There are only 26 codes to try. [Rot13 is still used.]
- This is a rather easy process to do backwards. [zyxwvutsr. . .]
- Decode: mpm!

- LOL!
- How can we make this code more difficult to break?

The Permutation Cipher

Encryption by Swapping Letters

The Permutation Cipher

Encryption by Swapping Letters

I		R	E	A	D		T	H	E		N	O	T	E	S

encryption $\downarrow$ *using a permutation*

b		p	u	t	q		v	k	u		f	x	v	u	o

Encryption by Swapping Letters

I		R	E	A	D		T	H	E		N	O	T	E	S

encryption $\downarrow$ *using a permutation*

b		p	u	t	q		v	k	u		f	x	v	u	o

There are $26! = 26 \times 25 \times \ldots \times 2 \times 1 \approx 4 \times 10^{26}$ codes to try!

The Permutation Cipher

Encryption by Swapping Letters

I		R	E	A	D		T	H	E		N	O	T	E	S

encryption $\downarrow$ *using a permutation*

b		p	u	t	q		v	k	u		f	x	v	u	o

There are $26! = 26 \times 25 \times \ldots \times 2 \times 1 \approx 4 \times 10^{26}$ codes to try!

Weaknesses

The Permutation Cipher

Encryption by Swapping Letters

I		R	E	A	D		T	H	E		N	O	T	E	S

encryption $\downarrow$ *using a permutation*

b		p	u	t	q		v	k	u		f	x	v	u	o

There are $26! = 26 \times 25 \times \ldots \times 2 \times 1 \approx 4 \times 10^{26}$ codes to try!

Weaknesses

- The single letter is probably "A" or "I";

The Permutation Cipher

Encryption by Swapping Letters

I		R	E	A	D		T	H	E		N	O	T	E	S

encryption $\downarrow$ *using a permutation*

b		p	u	t	q		v	k	u		f	x	v	u	o

There are $26! = 26 \times 25 \times \ldots \times 2 \times 1 \approx 4 \times 10^{26}$ codes to try!

Weaknesses

- The single letter is probably "A" or "I";
- The commonest letter is probably "E";

The Permutation Cipher

Encryption by Swapping Letters

I		R	E	A	D		T	H	E		N	O	T	E	S

encryption $\downarrow$ *using a permutation*

b		p	u	t	q		v	k	u		f	x	v	u	o

There are $26! = 26 \times 25 \times \ldots \times 2 \times 1 \approx 4 \times 10^{26}$ codes to try!

Weaknesses

- The single letter is probably "A" or "I";
- The commonest letter is probably "E";
- Words are likely to end with "S", if not "E";

The Permutation Cipher

Encryption by Swapping Letters

I		R	E	A	D		T	H	E		N	O	T	E	S

encryption $\downarrow$ *using a permutation*

b		p	u	t	q		v	k	u		f	x	v	u	o

There are $26! = 26 \times 25 \times \ldots \times 2 \times 1 \approx 4 \times 10^{26}$ codes to try!

Weaknesses

- The single letter is probably "A" or "I";
- The commonest letter is probably "E";
- Words are likely to end with "S", if not "E";
- The commonest (English) letters are: E, T, A, O, I, N, S, H, R, D.

The Permutation Cipher

Encryption by Swapping Letters

I		R	E	A	D		T	H	E		N	O	T	E	S

encryption $\downarrow$ *using a permutation*

b		p	u	t	q		v	k	u		f	x	v	u	o

There are $26! = 26 \times 25 \times \ldots \times 2 \times 1 \approx 4 \times 10^{26}$ codes to try!

Weaknesses

- The single letter is probably "A" or "I";
- The commonest letter is probably "E";
- Words are likely to end with "S", if not "E";
- The commonest (English) letters are: E, T, A, O, I, N, S, H, R, D.
- We might guess:

The Permutation Cipher

Encryption by Swapping Letters

I		R	E	A	D		T	H	E		N	O	T	E	S

encryption $\downarrow$ *using a permutation*

b		p	u	t	q		v	k	u		f	x	v	u	o

There are $26! = 26 \times 25 \times \ldots \times 2 \times 1 \approx 4 \times 10^{26}$ codes to try!

Weaknesses

- The single letter is probably "A" or "I";
- The commonest letter is probably "E";
- Words are likely to end with "S", if not "E";
- The commonest (English) letters are: E, T, A, O, I, N, S, H, R, D.
- We might guess:

I		?	E	?	?		T	H	E		?	?	T	E	S

The Frequency Attack for long messages – Al Kindi

The Frequency Attack for long messages – Al Kindi

I	T		I	S		A		T	R	U	T	H	...
b	v		b	o		t		v	p	l	v	k	...

Breaking the Permutation Cipher

The Frequency Attack for long messages – Al Kindi

I	T		I	S		A		T	R	U	T	H	…
b	v		b	o		t		v	p	l	v	k	…

Weaknesses

Breaking the Permutation Cipher

The Frequency Attack for long messages – Al Kindi

I	T		I	S		A		T	R	U	T	H	...
b	v		b	o		t		v	p	l	v	k	...

Weaknesses

- The commonest letters in English (decreasing order) are:
- E, T, A, O, I, N, S, H, R, D.

Breaking the Permutation Cipher

The Frequency Attack for long messages – Al Kindi

I	T		I	S		A		T	R	U	T	H	⋯
b	v		b	o		t		v	p	l	v	k	⋯

Weaknesses

- The commonest letters in English (decreasing order) are:
- E, T, A, O, I, N, S, H, R, D.
- The commonest encrypted letters (in our full message) are:
- u, v, t, x, b, f, o, k, p, q.

Breaking the Permutation Cipher

The Frequency Attack for long messages – Al Kindi

I	T		I	S		A		T	R	U	T	H	...
b	v		b	o		t		v	p	l	v	k	...

Weaknesses

- The commonest letters in English (decreasing order) are:
- E, T, A, O, I, N, S, H, R, D.
- The commonest encrypted letters (in our full message) are:
- u, v, t, x, b, f, o, k, p, q.
- Decode: `fxvu`

Breaking the Permutation Cipher

The Frequency Attack for long messages – Al Kindi

I	T		I	S		A		T	R	U	T	H	$\cdots$
b	v		b	o		t		v	p	l	v	k	$\cdots$

Weaknesses

- The commonest letters in English (decreasing order) are:
- E, T, A, O, I, N, S, H, R, D.
- The commonest encrypted letters (in our full message) are:
- u, v, t, x, b, f, o, k, p, q.
- Decode: `fxvu`
- NOTE

Breaking the Permutation Cipher

The Frequency Attack for long messages – Al Kindi

I	T		I	S		A		T	R	U	T	H	···
b	v		b	o		t		v	p	l	v	k	···

Weaknesses

- The commonest letters in English (decreasing order) are:
- E, T, A, O, I, N, S, H, R, D.
- The commonest encrypted letters (in our full message) are:
- u, v, t, x, b, f, o, k, p, q.
- Decode: `fxvu`
- NOTE: This leads us to guess the following decryption:

Breaking the Permutation Cipher

The Frequency Attack for long messages – Al Kindi

I	T		I	S		A		T	R	U	T	H	···
b	v		b	o		t		v	p	l	v	k	···

Weaknesses

- The commonest letters in English (decreasing order) are:
- E, T, A, O, I, N, S, H, R, D.
- The commonest encrypted letters (in our full message) are:
- u, v, t, x, b, f, o, k, p, q.
- Decode: `fxvu`
- NOTE: This leads us to guess the following decryption:
- `IT IS A TR?TH ?NI?ERSA??? A??NO??ED?ED THAT A SIN??E ?AN IN ?OSSESSION O? A ?OOD ?ORT?NE ??ST ?E IN ?ANT O? A ?I?E.`

Vigenère Cipher

Defending against the frequency attack

Vigenère Cipher

Defending against the frequency attack

- Keep changing your code!

Vigenère Cipher

Defending against the frequency attack

- Keep changing your code!
- If you change the code with every letter it is hard to break.

Vigenère Cipher

Defending against the frequency attack

- Keep changing your code!
- If you change the code with every letter it is hard to break.
- In the Vigenère Cipher your have a ‘Codeword’, say "ACE".

Vigenère Cipher

Defending against the frequency attack

- Keep changing your code!
- If you change the code with every letter it is hard to break.
- In the Vigenère Cipher your have a ‘Codeword’, say "ACE".
- The Codeword tells you how to change codes:

Vigenère Cipher

Defending against the frequency attack

- Keep changing your code!
- If you change the code with every letter it is hard to break.
- In the Vigenère Cipher your have a ‘Codeword’, say "ACE".
- The Codeword tells you how to change codes:
- "ACE" tells us to move letters on by 1, 3, 5, 1, 3, 5, . . .

Vigenère Cipher

Defending against the frequency attack

- Keep changing your code!
- If you change the code with every letter it is hard to break.
- In the Vigenère Cipher your have a 'Codeword', say "ACE".
- The Codeword tells you how to change codes:
- "ACE" tells us to move letters on by $1, 3, 5, 1, 3, 5, \ldots$

Vigenère Example

Vigenère Cipher

Defending against the frequency attack

- Keep changing your code!
- If you change the code with every letter it is hard to break.
- In the Vigenère Cipher your have a 'Codeword', say "ACE".
- The Codeword tells you how to change codes:
- "ACE" tells us to move letters on by $1, 3, 5, 1, 3, 5, \ldots$

Vigenère Example

I	T	I	S	A	T	R	U	T	H
A	C	E	A	C	E	A	C	E	A

$\downarrow$

j	w	n	t	d	y	s	x	y	i

Vigenère Cipher

Defending against the frequency attack

- Keep changing your code!
- If you change the code with every letter it is hard to break.
- In the Vigenère Cipher your have a ‘Codeword’, say "ACE".
- The Codeword tells you how to change codes:
- "ACE" tells us to move letters on by 1, 3, 5, 1, 3, 5, . . .

Vigenère Example

I	T	I	S	A	T	R	U	T	H
A	C	E	A	C	E	A	C	E	A

$\downarrow$

j	w	n	t	d	y	s	x	y	i

This is harder to decode. However, in this example we just need 3 frequency tables. One for each letter of the Codeword.

One Time Pad

Use Random Shifts for each letter

One Time Pad

Use Random Shifts for each letter

- If your Codeword is long, then the frequency attack is hard.

One Time Pad

Use Random Shifts for each letter

- If your Codeword is long, then the frequency attack is hard.
- It is tempting to use a long text, like "The Bible", as your Codeword.

One Time Pad

Use Random Shifts for each letter

- If your Codeword is long, then the frequency attack is hard.
- It is tempting to use a long text, like "The Bible", as your Codeword.

Vigenère Example

One Time Pad

Use Random Shifts for each letter

- If your Codeword is long, then the frequency attack is hard.
- It is tempting to use a long text, like "The Bible", as your Codeword.

Vigenère Example

I	T	I	S	A	T	R	U	T	H
I	N	T	H	E	B	E	G	I	N

$\downarrow$

r	h	c	a	f	v	w	b	c	v

One Time Pad

Use Random Shifts for each letter

- If your Codeword is long, then the frequency attack is hard.
- It is tempting to use a long text, like "The Bible", as your Codeword.

Vigenère Example

I	T	I	S	A	T	R	U	T	H
I	N	T	H	E	B	E	G	I	N

$\downarrow$

r	h	c	a	f	v	w	b	c	v

- BUT, someone might guess your CodeText.

One Time Pad

Use Random Shifts for each letter

- If your Codeword is long, then the frequency attack is hard.
- It is tempting to use a long text, like "The Bible", as your Codeword.

Vigenère Example

I	T	I	S	A	T	R	U	T	H
I	N	T	H	E	B	E	G	I	N

↓

r	h	c	a	f	v	w	b	c	v

- BUT, someone might guess your CodeText.
- Better to use random shifts, from a One Time Pad.

One Time Pad

Use Random Shifts for each letter

- If your Codeword is long, then the frequency attack is hard.
- It is tempting to use a long text, like "The Bible", as your Codeword.

Vigenère Example

I	T	I	S	A	T	R	U	T	H
I	N	T	H	E	B	E	G	I	N

↓

r	h	c	a	f	v	w	b	c	v

- BUT, someone might guess your CodeText.
- Better to use random shifts, from a One Time Pad.
- How can I securely send something random to you? (like a number in a One Time Pad)

Sending Secret Numbers

Sending Secret Numbers

- How can I tell you how to encrypt a message, without telling you how to decrypt a message?

Sending Secret Numbers

- How can I tell you how to encrypt a message, without telling you how to decrypt a message?

The (3, 100) Cipher

Public Key Cryptography

Sending Secret Numbers

- How can I tell you how to encrypt a message, without telling you how to decrypt a message?

The (3, 100) Cipher

- To send 17 send the last two digits of $17^3 = 17 \times 17 \times 17 = 49113$;

Sending Secret Numbers

- How can I tell you how to encrypt a message, without telling you how to decrypt a message?

The (3, 100) Cipher

- To send 17 send the last two digits of $17^3 = 17 \times 17 \times 17 = 49113$;
- Encode: 17 as the number 13.

Public Key Cryptography

Sending Secret Numbers

- How can I tell you how to encrypt a message, without telling you how to decrypt a message?

The (3, 100) Cipher

- To send 17 send the last two digits of $17^3 = 17 \times 17 \times 17 = 49113$;
- Encode: 17 as the number 13.
- The Public Key is (3, 100).

Public Key Cryptography

Sending Secret Numbers

- How can I tell you how to encrypt a message, without telling you how to decrypt a message?

The (3, 100) Cipher

- To send 17 send the last two digits of $17^3 = 17 \times 17 \times 17 = 49113$;
- Encode: 17 as the number 13.
- The Public Key is (3, 100).
- It is hard to see how to decode this message.

Public Key Cryptography

Sending Secret Numbers

- How can I tell you how to encrypt a message, without telling you how to decrypt a message?

The (3, 100) Cipher

- To send 17 send the last two digits of $17^3 = 17 \times 17 \times 17 = 49113$;
- Encode: 17 as the number 13.
- The Public Key is (3, 100).
- It is hard to see how to decode this message.
- To decode: I compute the last two digits of 13^{27}, [27 is my Secret!]

Public Key Cryptography

Sending Secret Numbers

- How can I tell you how to encrypt a message, without telling you how to decrypt a message?

The (3, 100) Cipher

- To send 17 send the last two digits of $17^3 = 17 \times 17 \times 17 = 49113$;
- Encode: 17 as the number 13.
- The Public Key is (3, 100).
- It is hard to see how to decode this message.
- To decode: I compute the last two digits of 13^{27}, [27 is my Secret!]
- $13^{27} = (((13)^3)^3)^3) \equiv ((97)^3)^3 \equiv 73^3 \equiv 17$.

Public Key Cryptography

Sending Secret Numbers

- How can I tell you how to encrypt a message, without telling you how to decrypt a message?

The (3, 100) Cipher

- To send 17 send the last two digits of $17^3 = 17 \times 17 \times 17 = 49113$;
- Encode: 17 as the number 13.
- The Public Key is (3, 100).
- It is hard to see how to decode this message.
- To decode: I compute the last two digits of 13^{27}, [27 is my Secret!]
- $13^{27} = (((13)^3)^3)^3) \equiv ((97)^3)^3 \equiv 73^3 \equiv 17$.
- Why 27?

Public Key Cryptography

Sending Secret Numbers

- How can I tell you how to encrypt a message, without telling you how to decrypt a message?

The (3, 100) Cipher

- To send 17 send the last two digits of $17^3 = 17 \times 17 \times 17 = 49113$;
- Encode: 17 as the number 13.
- The Public Key is (3, 100).
- It is hard to see how to decode this message.
- To decode: I compute the last two digits of 13^{27}, [27 is my Secret!]
- $13^{27} = (((13)^3)^3)^3) \equiv ((97)^3)^3 \equiv 73^3 \equiv 17$.
- Why 27? "Because" $100 = 2^2 \times 5^2$ and $3 \times 27 = 1 + 2^1(2-1)5^1(5-1) \times 2$.

Public Key Cryptography

Sending Secret Numbers

- How can I tell you how to encrypt a message, without telling you how to decrypt a message?

The (3, 100) Cipher

- To send 17 send the last two digits of $17^3 = 17 \times 17 \times 17 = 49113$;
- Encode: 17 as the number 13.
- The Public Key is (3, 100).
- It is hard to see how to decode this message.
- To decode: I compute the last two digits of 13^{27}, [27 is my Secret!]
- $13^{27} = (((13)^3)^3)^3) \equiv ((97)^3)^3 \equiv 73^3 \equiv 17$.
- Why 27? "Because" $100 = 2^2 \times 5^2$ and $3 \times 27 = 1 + 2^1(2-1)5^1(5-1) \times 2$.
- In practice we use big numbers, which are hard to factor.

Conclusion

Summary

Summary

- The Caesar Cipher quickly hides a message from plain sight.

Conclusion

Summary

- The Caesar Cipher quickly hides a message from plain sight.
- The Permutation Cipher shows that even complicated methods have a weakness whenever there is a pattern.

Conclusion

Summary

- The Caesar Cipher quickly hides a message from plain sight.
- The Permutation Cipher shows that even complicated methods have a weakness whenever there is a pattern.
- The Vigenère Cipher built a better cipher, based on Caesar.

Conclusion

Summary

- The Caesar Cipher quickly hides a message from plain sight.
- The Permutation Cipher shows that even complicated methods have a weakness whenever there is a pattern.
- The Vigenère Cipher built a better cipher, based on Caesar.
- The One Time Pad is ideal, but hard to put into practice.

Conclusion

Summary

- The Caesar Cipher quickly hides a message from plain sight.
- The Permutation Cipher shows that even complicated methods have a weakness whenever there is a pattern.
- The Vigenère Cipher built a better cipher, based on Caesar.
- The One Time Pad is ideal, but hard to put into practice.
- The Public Key Cryptography system allows secure transmission, but really needs a computer to implement.

Conclusion

Summary

- The Caesar Cipher quickly hides a message from plain sight.
- The Permutation Cipher shows that even complicated methods have a weakness whenever there is a pattern.
- The Vigenère Cipher built a better cipher, based on Caesar.
- The One Time Pad is ideal, but hard to put into practice.
- The Public Key Cryptography system allows secure transmission, but really needs a computer to implement.

Further Reading

Conclusion

Summary

- The Caesar Cipher quickly hides a message from plain sight.
- The Permutation Cipher shows that even complicated methods have a weakness whenever there is a pattern.
- The Vigenère Cipher built a better cipher, based on Caesar.
- The One Time Pad is ideal, but hard to put into practice.
- The Public Key Cryptography system allows secure transmission, but really needs a computer to implement.

Further Reading

- Come and join me in MAS3214!

Conclusion

Summary

- The Caesar Cipher quickly hides a message from plain sight.
- The Permutation Cipher shows that even complicated methods have a weakness whenever there is a pattern.
- The Vigenère Cipher built a better cipher, based on Caesar.
- The One Time Pad is ideal, but hard to put into practice.
- The Public Key Cryptography system allows secure transmission, but really needs a computer to implement.

Further Reading

- Come and join me in MAS3214!
- More materials are on Blackboard: Example Sheet, and this talk.

Conclusion

Summary

- The Caesar Cipher quickly hides a message from plain sight.
- The Permutation Cipher shows that even complicated methods have a weakness whenever there is a pattern.
- The Vigenère Cipher built a better cipher, based on Caesar.
- The One Time Pad is ideal, but hard to put into practice.
- The Public Key Cryptography system allows secure transmission, but really needs a computer to implement.

Further Reading

- Come and join me in MAS3214!
- More materials are on Blackboard: Example Sheet, and this talk.
- At Newcastle you begin to study Number Theory in your first term.

Conclusion

Summary

- The Caesar Cipher quickly hides a message from plain sight.
- The Permutation Cipher shows that even complicated methods have a weakness whenever there is a pattern.
- The Vigenère Cipher built a better cipher, based on Caesar.
- The One Time Pad is ideal, but hard to put into practice.
- The Public Key Cryptography system allows secure transmission, but really needs a computer to implement.

Further Reading

- Come and join me in MAS3214!
- More materials are on Blackboard: Example Sheet, and this talk.
- At Newcastle you begin to study Number Theory in your first term.
- sgzmj xnt!

Conclusion

Summary

- The Caesar Cipher quickly hides a message from plain sight.
- The Permutation Cipher shows that even complicated methods have a weakness whenever there is a pattern.
- The Vigenère Cipher built a better cipher, based on Caesar.
- The One Time Pad is ideal, but hard to put into practice.
- The Public Key Cryptography system allows secure transmission, but really needs a computer to implement.

Further Reading

- Come and join me in MAS3214!
- More materials are on Blackboard: Example Sheet, and this talk.
- At Newcastle you begin to study Number Theory in your first term.
- sgzmj xnt! . . . I mean . . . THANK YOU!