



## Ben Martin

**Run Tape:** Stop tape at times indicated to raise questions.

00:37 What is cryptography?

01:19 *Note:* A key unlocks a code.

### Activity:

Get students to encode their names using a Caesar Cipher.

[http://en.wikipedia.org/wiki/Caesar\\_cipher](http://en.wikipedia.org/wiki/Caesar_cipher)

<http://secretcodebreaker.com/history2.html>

For example	A	B	C	D	E	F	G	H
			A	B	C	D	E	

This is shift of +3. So NELL becomes QHOO

You can collect all the names and re-distribute them for people to decode.

To de-code the shift is reversed - by subtracting 3.

What would a shift of 26 be?

01:45 What problems can you see with this method of sending a message? (For example it's not a good way to say, "Your house is on fire!")

02:15 What role does cryptography play in wartime?

*Note:* You can read about Enigma in The Code Book by Simon Singh

[http://www.simonsingh.net/Crypto\\_Corner.html](http://www.simonsingh.net/Crypto_Corner.html)

02:52 What is eavesdropping? (For example if you are on a land line to your friend and your mum picks up without your hearing her – whoops!!)

05:58 What is the thing most likely to go wrong with cryptography? Where do you use passwords?

07:55 When you did the exercise with the Caesar Cipher we all shared the same key that meant the code was easy to "crack". If I told you the key and someone was eavesdropping – they would be able to find out what we had been saying to each other – our secret wouldn't be secret any longer. You can read about public key cryptography like RSA in The Code Book by Simon Singh.

If you want to talk to a local mathematician who is very interested in key exchanging call Julia Novak – she will be happy to come and talk to your students.

[novakj@math.auckland.ac.nz](mailto:novakj@math.auckland.ac.nz)