

#### Session 4: Fermat's Little Theorem and RSA

Explain that Fermat's Little Theorem relies on raising a number,  $x$ , to a power,  $p$ , when in modulus ' $p$ ' and exploring the outcome.

For example:

$$3^5 = 243 \equiv 3 \pmod{5}$$

$$3^4 = 81 \equiv 1 \pmod{4}$$

In other words:  $x^p \equiv x \pmod{p}$

Students should notice that when  $p$  is prime, the outcome is  $x$ .

Show students Youtube footage of RSA explained. Show them the Wikipedia explanation of the process of RSA:

<http://en.wikipedia.org/wiki/Rsa>

and get them to test it out for their own numbers.