# MD5 Collisions

Isabelle Stanton

Chalermpong Worawannotai

# Description of MD5

- Takes any message and outputs an 128-bit hash.
- A message is padded so the length is a multiple of 512 by concatenating a 1 then 0's and it's length as a 64 bit number.
- Each 512 bit block is compressed individually

# Continued Description

- The 512-bit block is divided into 16 32-bit words
- There are 4 32-bit registers a, b, c and d. These are initially loaded with $IV_0$ and carry the hash values from one 512-bit block to the next
- It works in an iterative (chaining) process:

$$H_{i+1} = f(H_i, M_i) \qquad IV_0 = H_0$$

where $M_i$ is a 512 bit block.