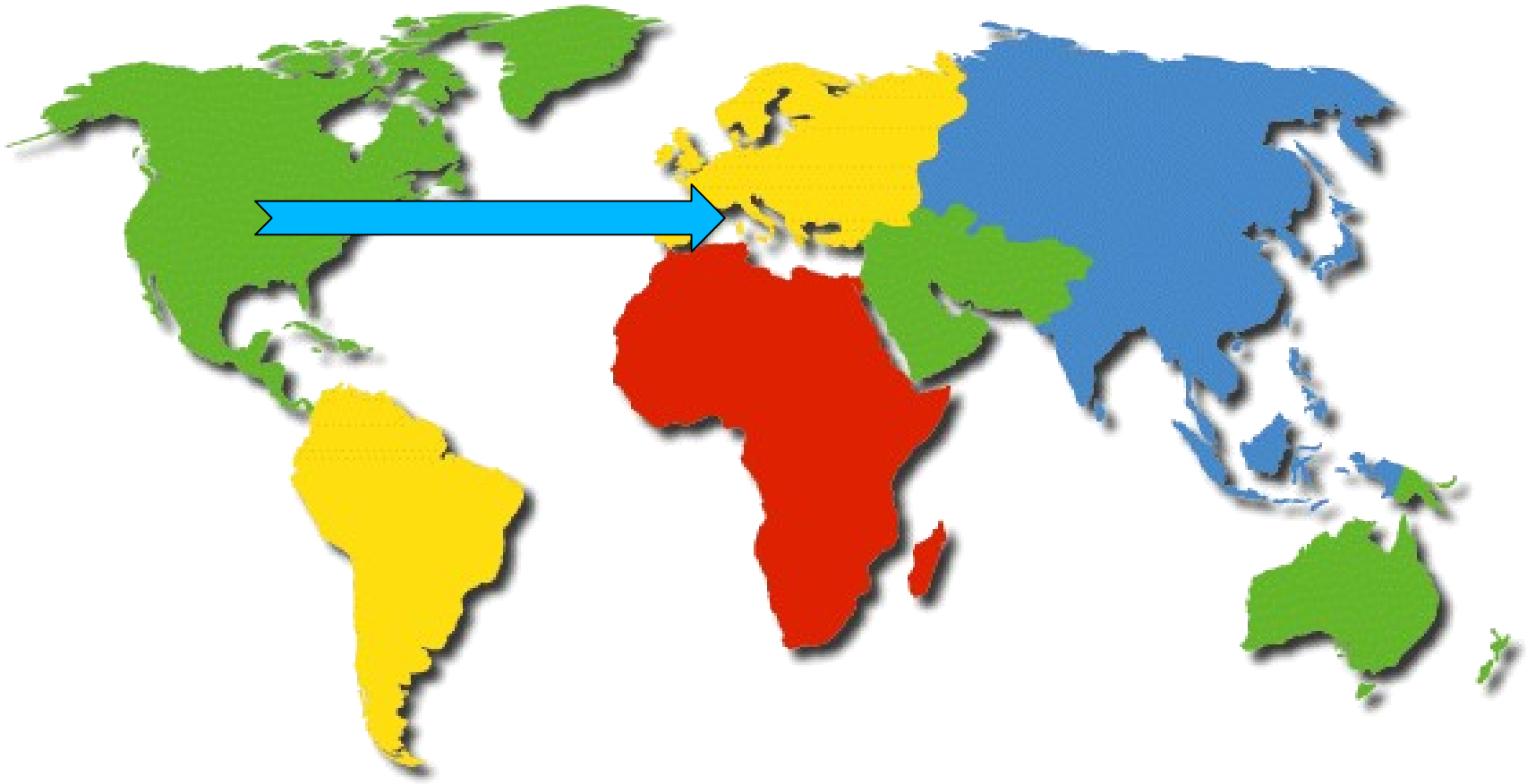
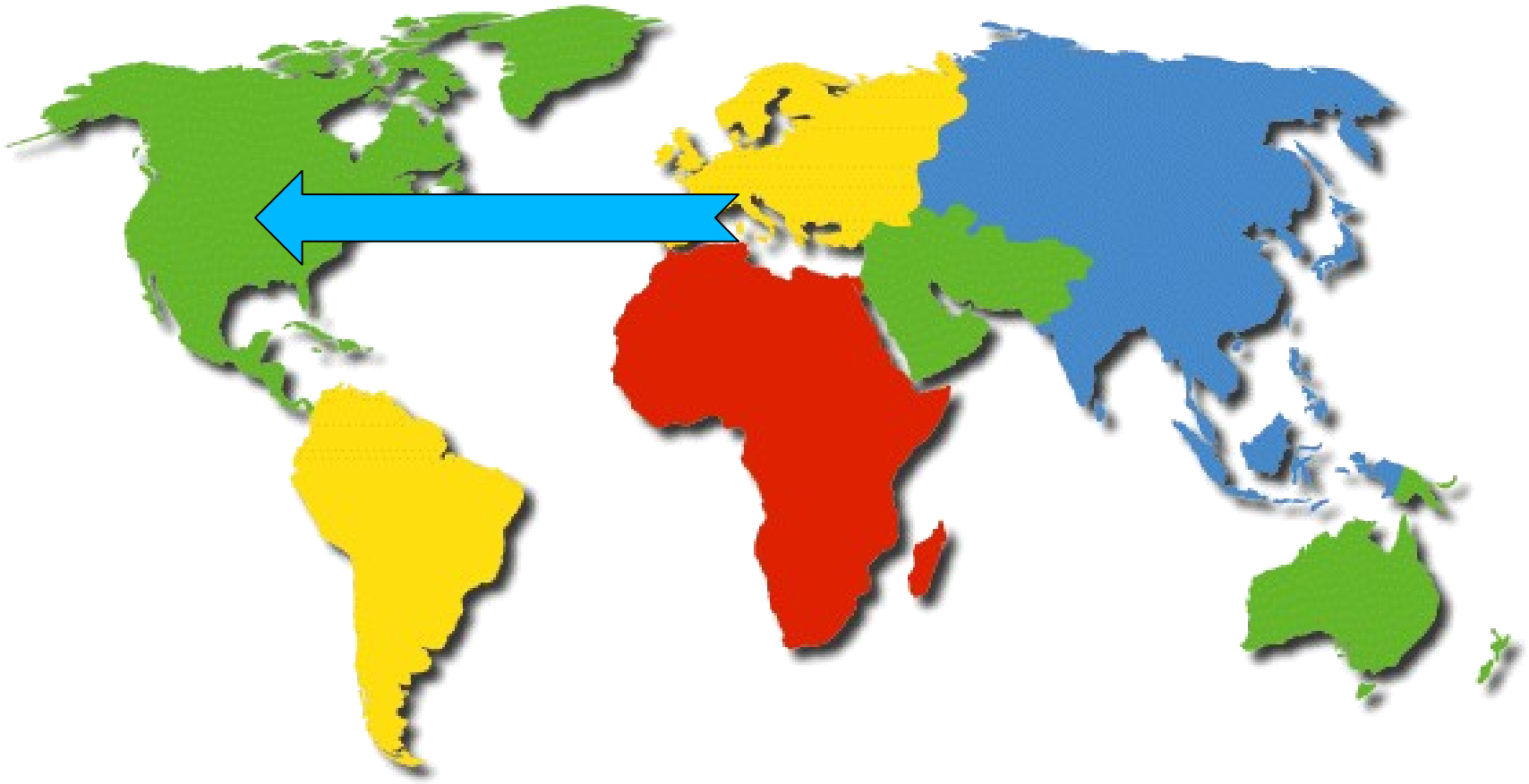
Cryptographic Ash Functions

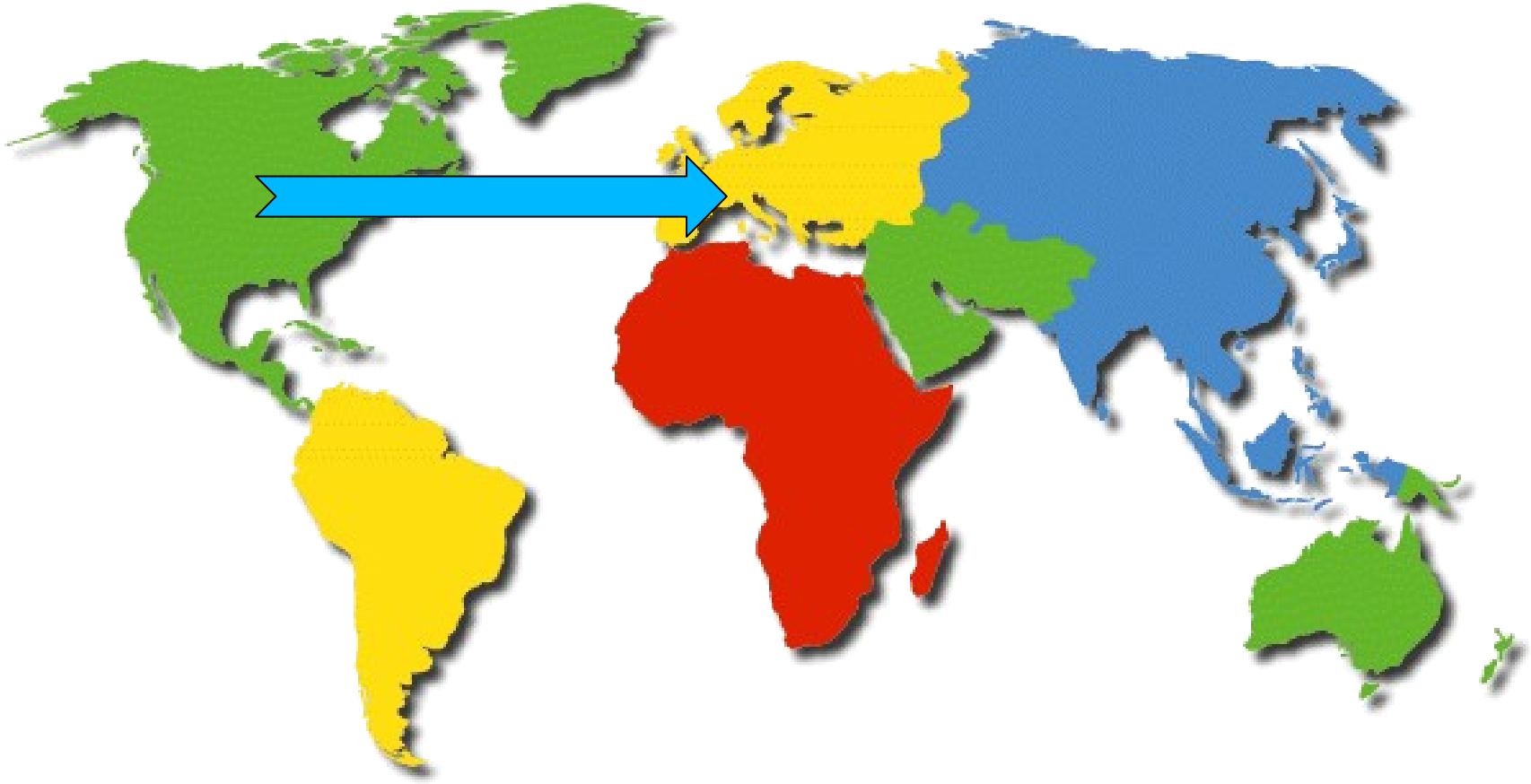
Bijective Functions



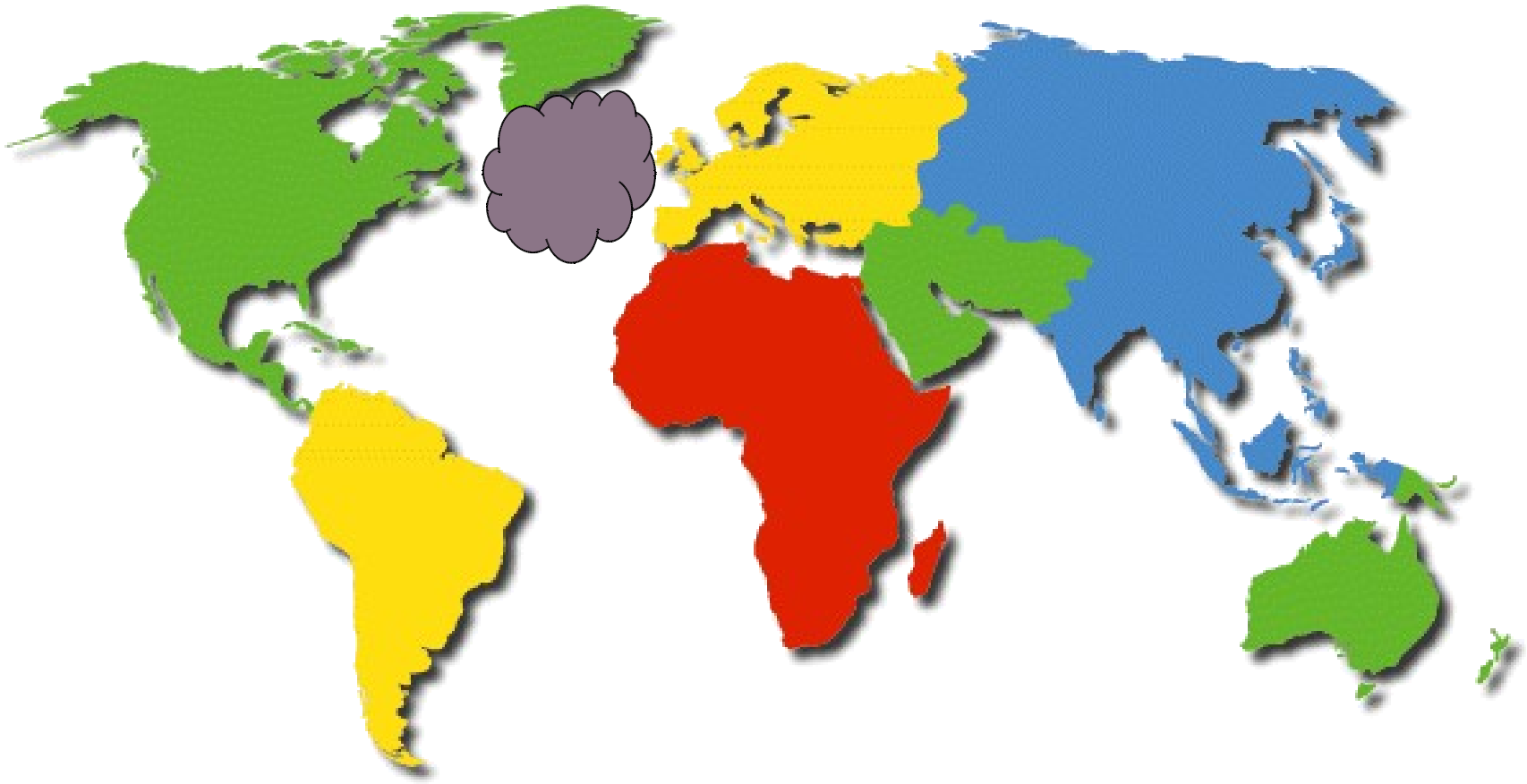
Bijective Functions



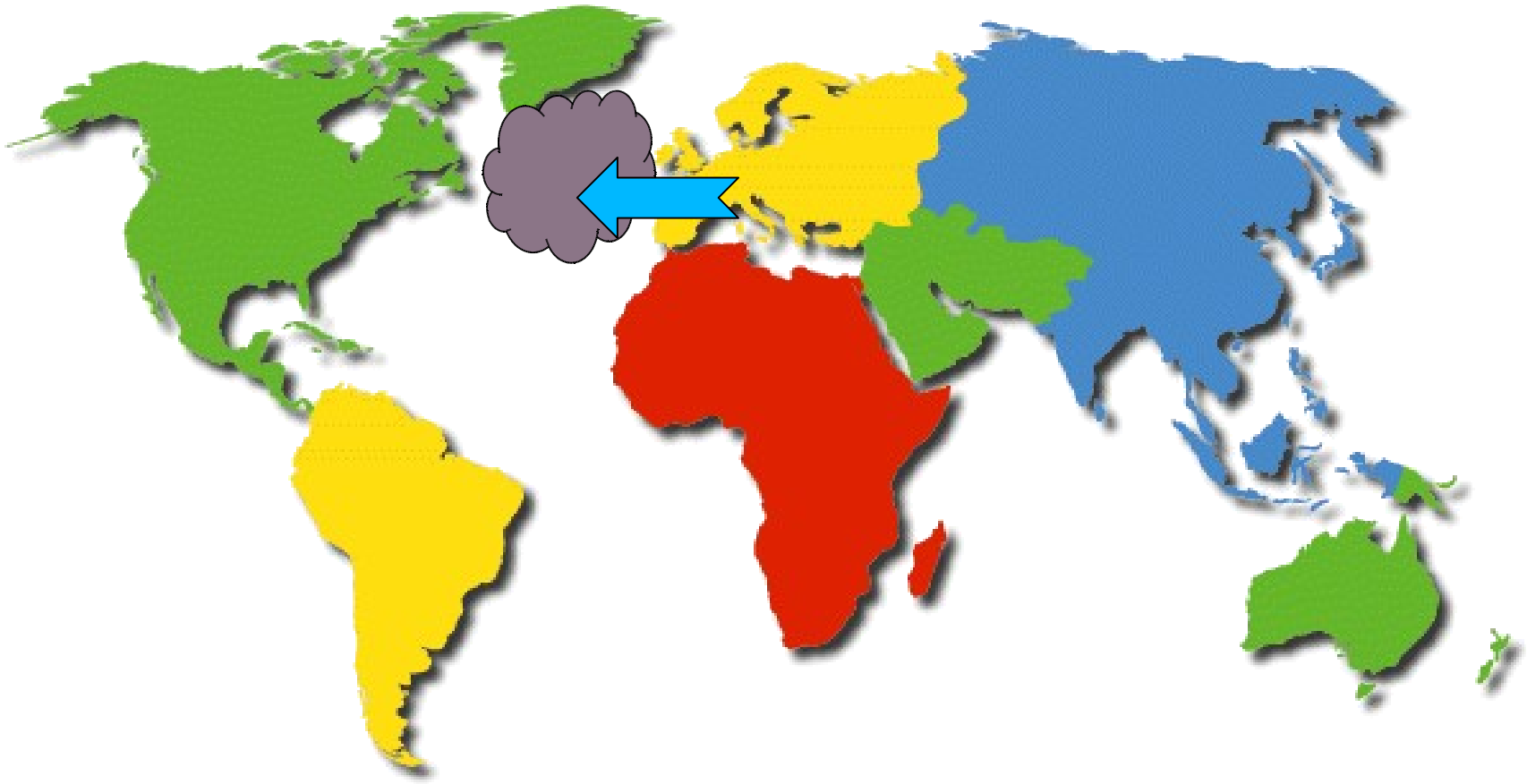
One-Way Ash Function



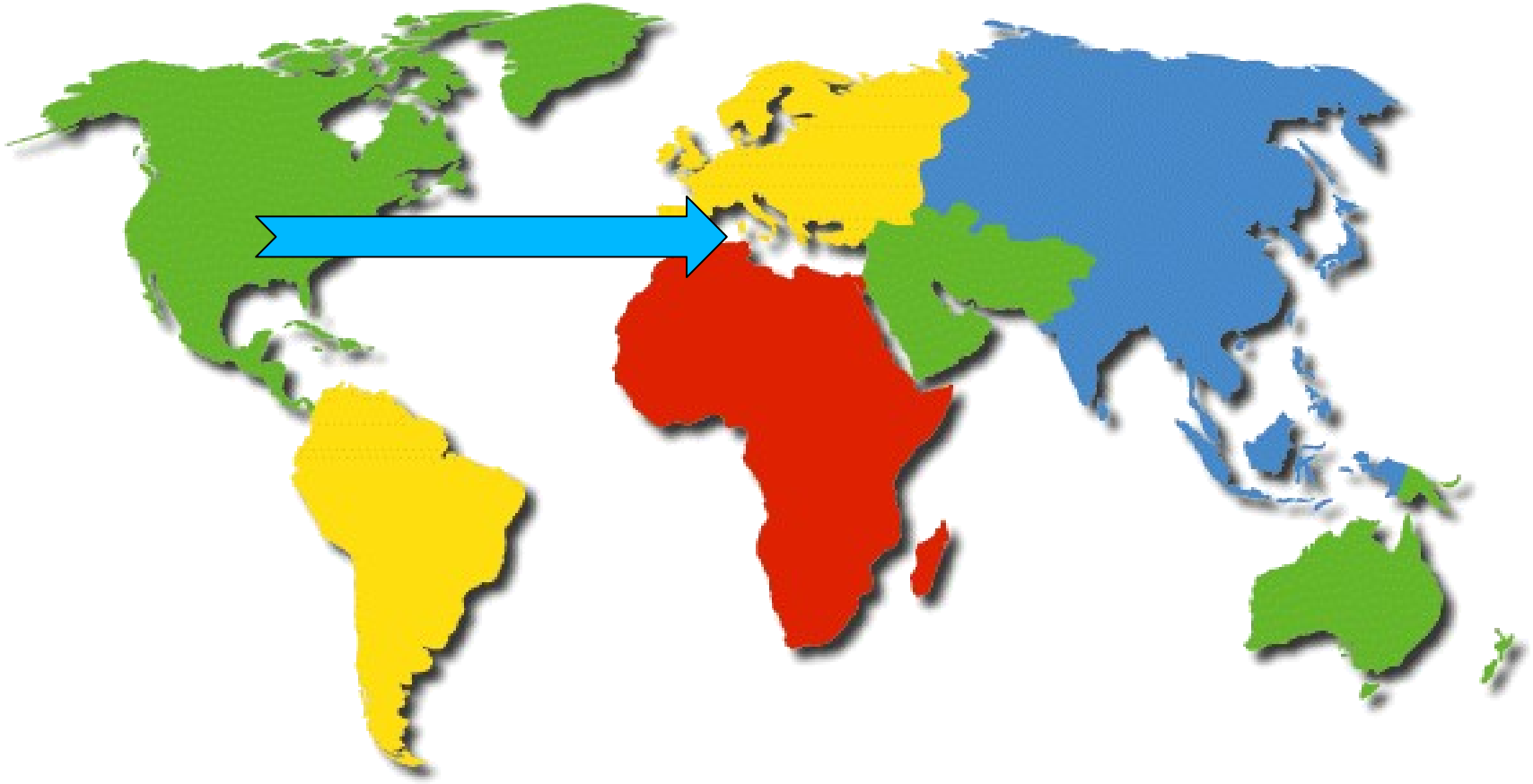
One-Way Ash Function



One-Way Ash Function

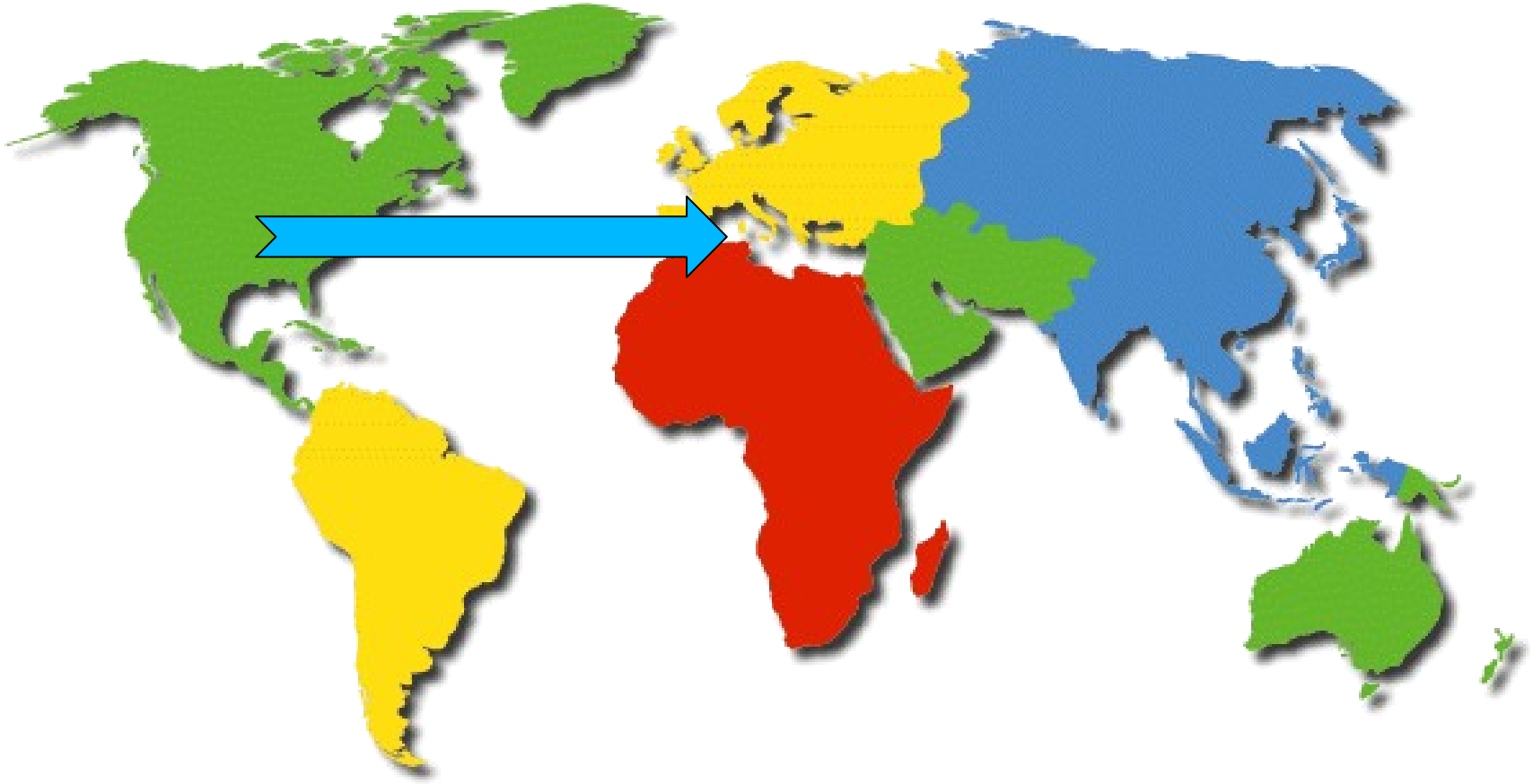


The Function is Lossy
Sometimes you can compute preimages
Sometimes you cant



The Function is Lossy
Sometimes you can compute preimages
Sometimes you cant

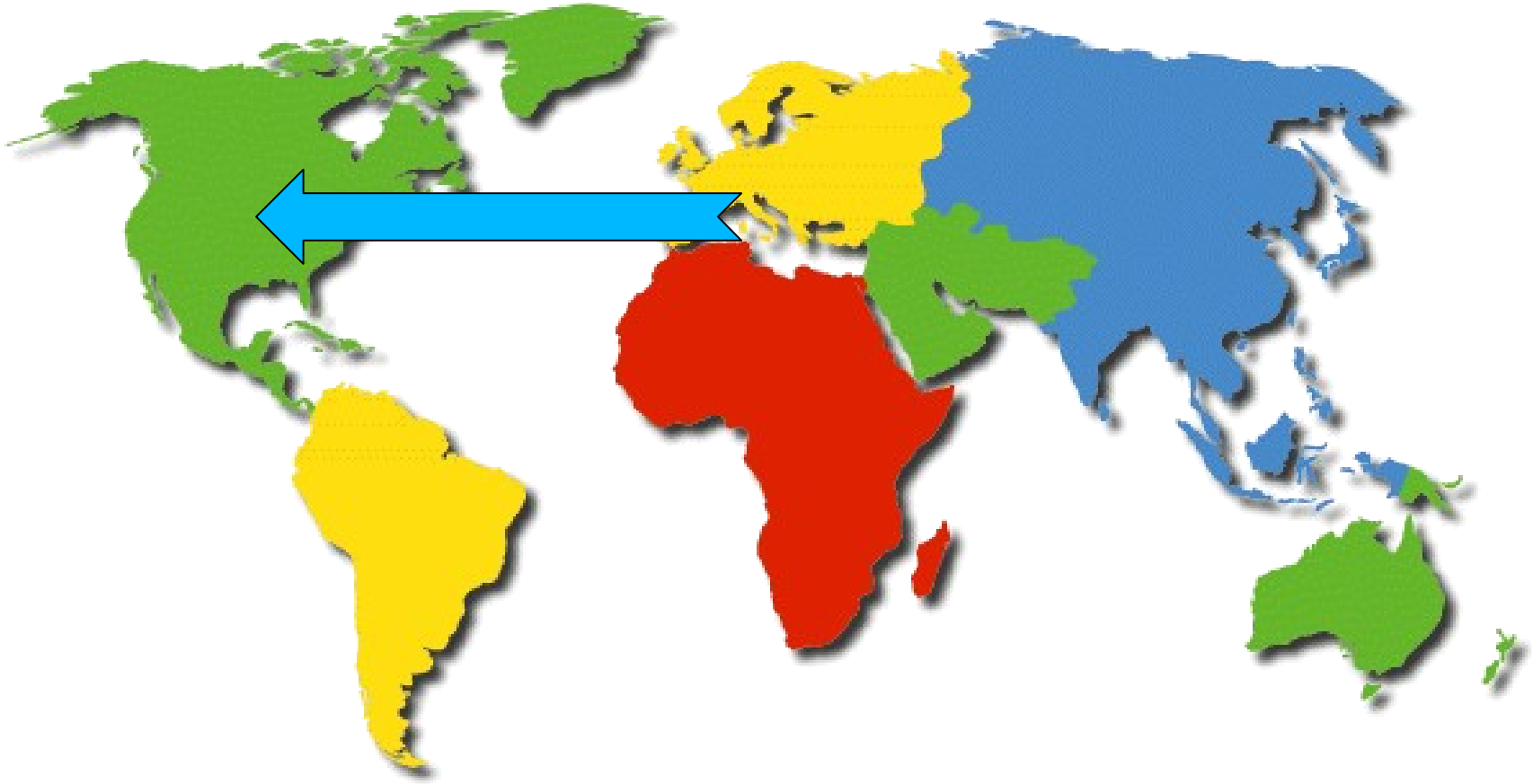
The Function is Lossy
Sometimes you can compute preimages
Sometimes you cant



The Function is Lossy
Sometimes you can compute preimages
Sometimes you cant

The Function is Lossy
Sometimes you can compute preimages
Sometimes you cant

The Function is Lossy
Sometimes you can compute preimages
Sometimes you cant



Random Walks

- It is known that one way to break an ash function is to apply random walks.
- In April many people trying to “invert” the Ash function had to engage in random walk

Previous Work in This Area

- **Isogeny Volcanoes** introduced by D. Kohel in his thesis: Berkeley 1996.

Follow up work

- **Isogeny Volcanoes and the SEA Algorithm**
  - M. Fouquet and F. Morain: ANTS-5
- **Modular Polynomials via Isogeny Volcanoes**
  - R. Broker, K. Lauter and AV. Sutherland: 2010
- **Pairing the Volcano**
  - Ionica and Joux: ANTS 2010

EuroCrapt

Journal of Craptology : Volume 7 is now out

Volume 7 was a special Valentine's edition

J. Crap aims to publish the leading crapto research

www.anagram.com/~jcrap/

Submit via an email to one of the editors:

Nigel Smart

Tom Berson

Raphael C.-W. Phan

Orr Dunkelman

Dan Page

PhD and Post Doc Position

- In area of provable security and group signatures in particular.

- PhD (EU Nationals Only)
  - Closing Date: 6th June

- RA (Anyone with PhD in Crypto)
  - Closing Date: 30th June

www.cs.bris.ac.uk