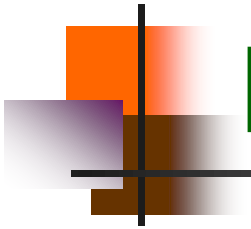
From Math to Society
Numbers, Security and Culture

- Marc Conrad
  - Marc.Conrad@beds.ac.uk
  - http://dr.marcconrad.com



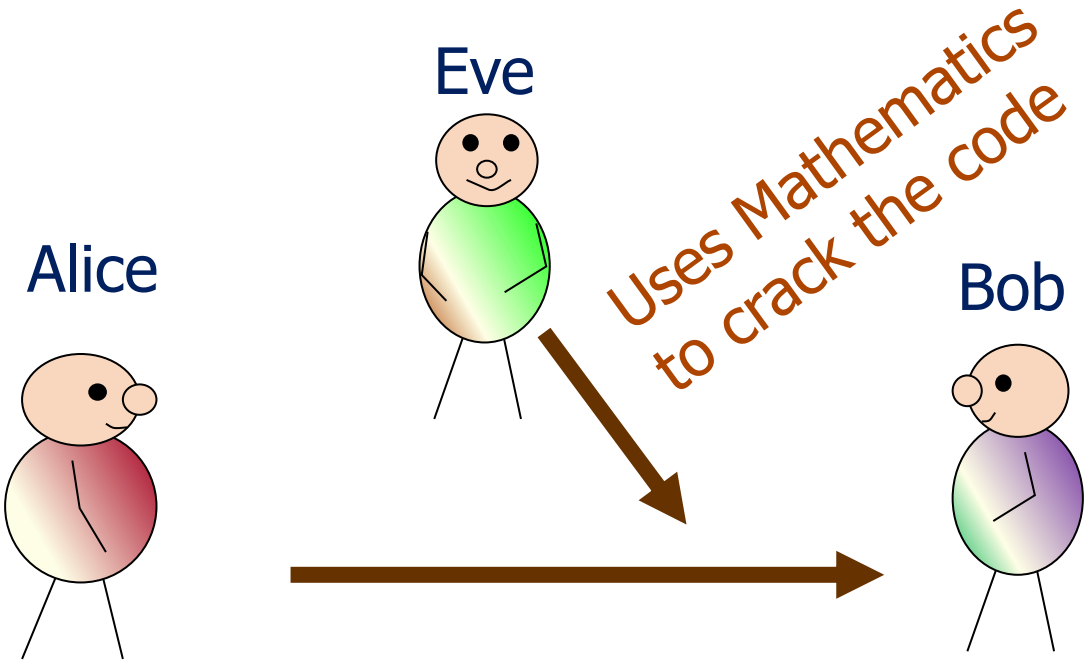
Mathematics

- Algebraic Structures
- Modular arithmetic $\mathbf{Z}/n\mathbf{Z}$; $n = pq$.
- Elliptic curves
- Multiplicative groups
- One-way functions:
  - Multiplication is easy; Factorization is difficult.

2,633 x 3,697 = … (easy)
9,744,731 = … x … (difficult)

RSA
(Rivest–Shamir–Adleman)

- Use Mathematics to do encryption / decryption
- Public Key / Private Key



Mathematics and Computing

- Encode the Mathematics to define your algorithms
  - Maple, C., Conrad, M., French, T., A novel flexible approach to document encryption using an MathML extension to the W3C XML Digital Certificate Standard, Procs. IADIS Conference eSociety 2003, Lisbon, Portugal.
- Later, on a more theoretical level – no longer in the context of security then:
  - Conrad, M., French, T. Exploring the synergies between the object-oriented paradigm and mathematics: a java led approach, International Journal of Mathematical Education in Science and Technology', Vol 35, No.5,733-742, 2004.

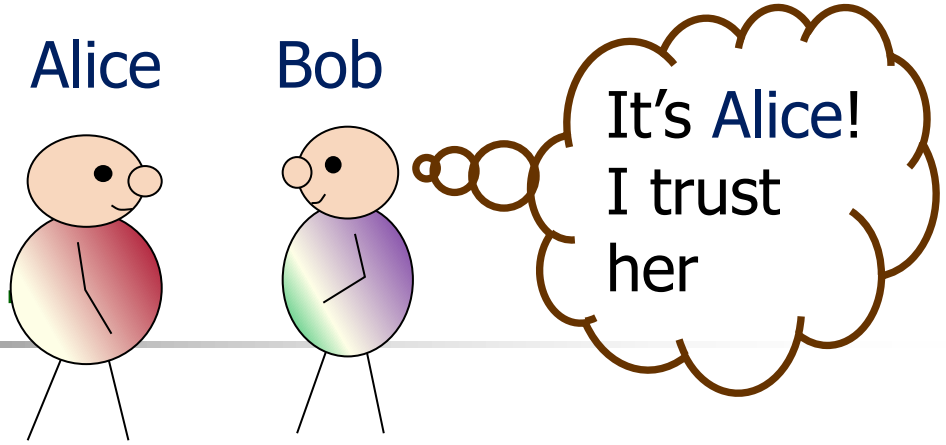
However, Security today

- We are largely OK with the Mathematics
- Social Engineering is the most imminent problem.

Focus e.g., on Authentication Systems

- Alternative forms of authentication
  - Norrington, P., Novel, robust and cost-effective authentication techniques for online services, PhD, University of Bedfordshire 2009.
  - Al-Khateeb, H., Flexible, reliable and secure authentication mechanisms for web applications, PhD, University of Bedfordshire 2010.
  - Gibson, M., Opening the web for all: Designing authentication for accessibility, PhD, University of Bedfordshire 2012.

Or on trust.



- Conrad, M., French, T., Huang, W., Maple, C., A lightweight model of trust propagation in a Multi-Client Network Environment. To what extent does Experience matter? In: 1st International Conference on Availability, Reliability and Security (ARES), Vienna, 2006.
- Pasanajano, P., Bessis, N., Yue, Y., Conrad, M., Brown, A., A Peer-to-Peer Trust Modelling Analysis for Decreasing B2B Monitoring Costs, In: 15th International Conference on Automation and Computing (ICAC'09), September 19th, Luton, 2009 ISBN: 978-0-9555293-4-4, p.p.: 104-108.
- Koshy, L., Conrad, M., Shukla, M., French, T., Trust Score System in Social Networks and Virtual Worlds Based on Digital Identity. 15th International Conference on e-Society 2017, Budapest, Hungary.

However, Security is localized and different between countries

- For instance, there is a difference in Information Security between the United Kingdom and Zanzibar
  - Shabaan, H., The state of information security in the developing countries: the case of Zanzibar, Tanzania, PhD, University of Bedfordshire 2013.
- Culture became an issue; central to this is Hofstede's theory of cultural dimensions - https://geerthofstede.com/

Cross-cultural research

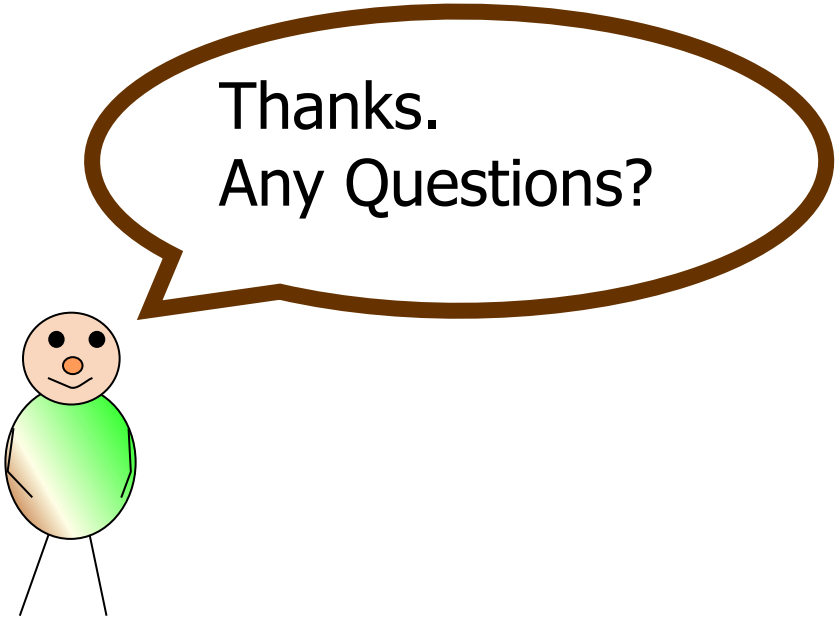
- In Web Design
  - Chessum, K., A Conceptual Framework to Support Cross-cultural User Experience Design for Web Search, PhD, University of Bedfordshire, 2021
- Within Cyberstalking, inspired by NCCR
  - Miftha, A., Conrad, M., Gibson, M., Cyberstalking in India: Challenges on the Social Side and the Underlying Contradictions, In: 20h International Conference e-Society 2022 (online).

More cross-cultural research

- In e-Government
  - Chukwu, J., Conrad, M., Crosbie, T., Data Protection and Privacy Determinants of e-Government Adoption in Nigeria, 15th IADIS International Conference on Information Systems (IS 2022).
- And the Manufacturing Industry
  - Omoyajowo, O., A Systematic Risk Management Approach for Small Medium-sized Enterprises (SMEs) in Nigeria Manufacturing Sector, PhD, University of Bedfordshire, 2022

Summary

- Mathematics
- Security
- Trust
- Culture



http://dr.marcconrad.com