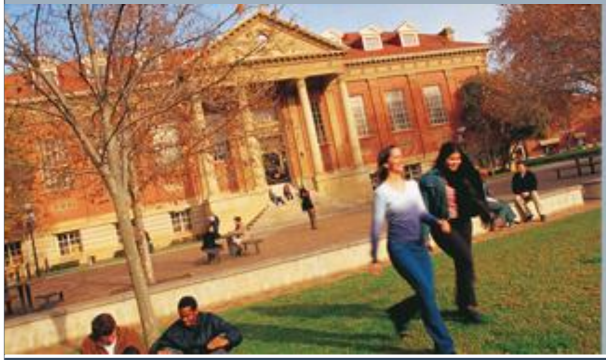
School of Electrical & Electronic Engineering

THE UNIVERSITY of ADELAIDE

Keyless Encryption



Michael Parisotto

Aleks Kojic

Supervisors:
Derek Abbott and James Chappell

Outline

- Introduction
  - Why is Encryption Important?
- One Time Pad
  - Explanation and History
  - Symmetric Key & example of Double Padlock protocol
- Encryption through rotations
  - 2D Rotations
  - 3D Rotations
- Geometric Algebra
  - Allows for generalisation in N-dimensions.
  - Potential for 4D, 6D 8D solution.
- Project Management and Conclusion

Introduction

Public Key Cryptography

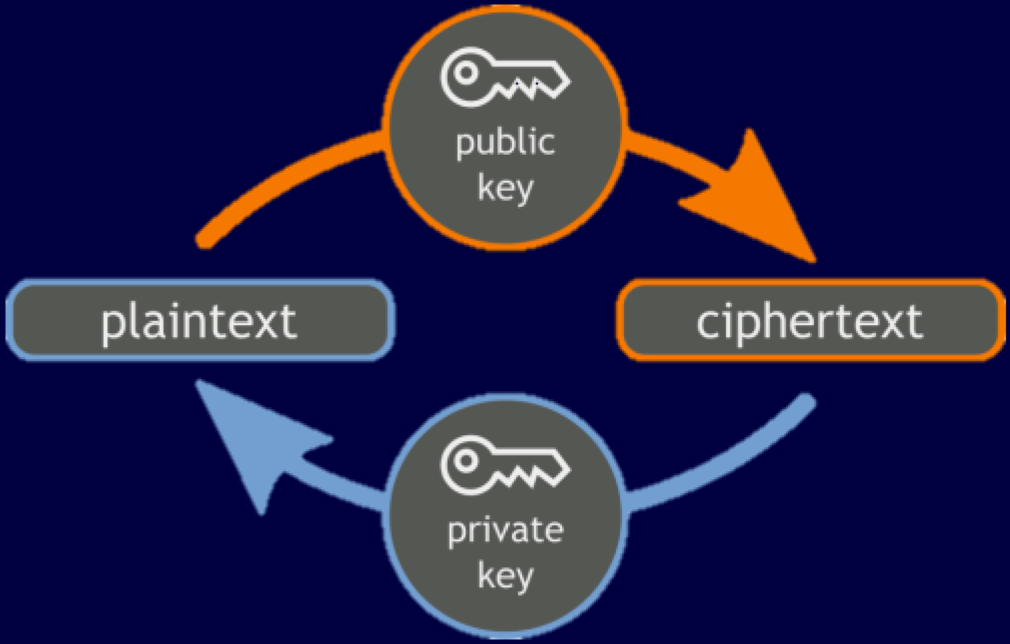
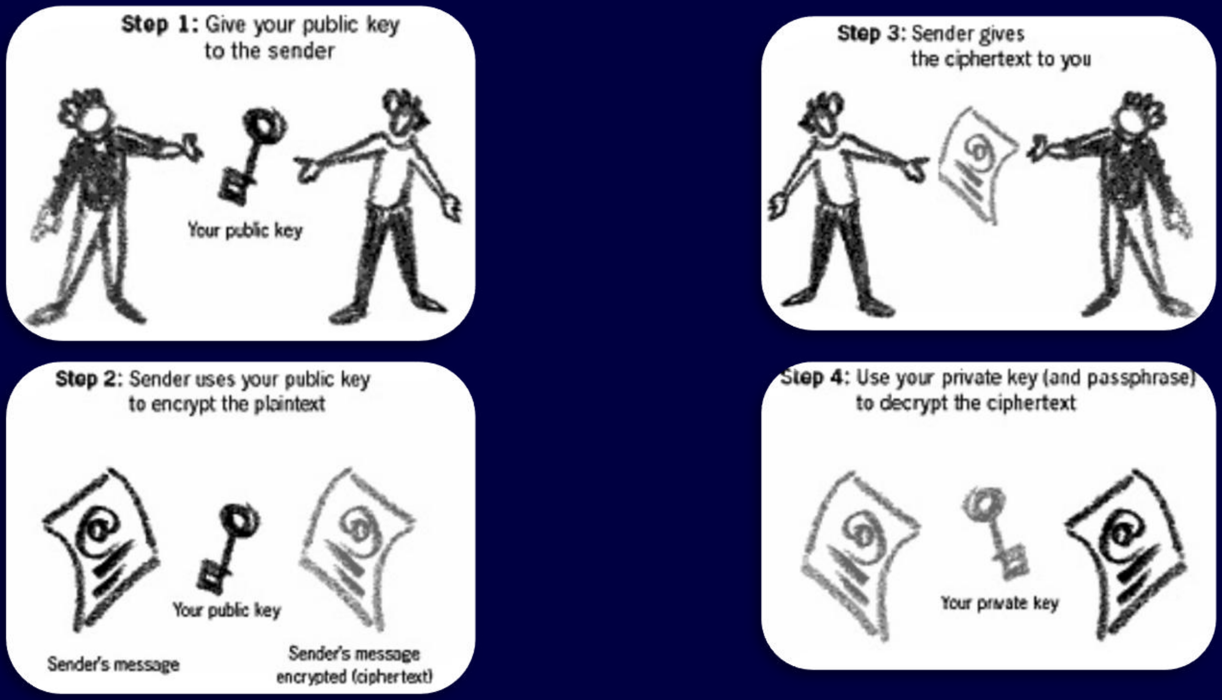


Image: http://dougvitale.wordpress.com/2012/02/20/ssh-the-secure-shell/

Introduction

Symmetric & Asymmetric Key Systems

Vulnerable to a *Man in the Middle Attack*

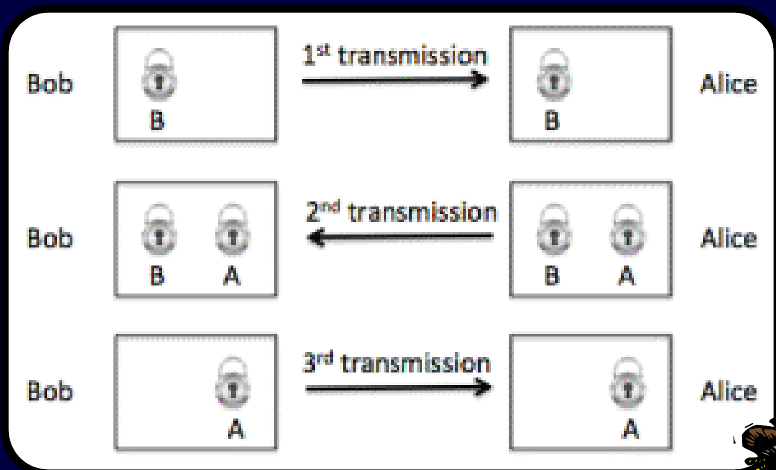


Images: http://www.mxrelease.com/images/mxrelease_security.gif

Introduction

Kish-Sethuraman (KS) Cipher - The Double Padlock Protocol

What it would mean?

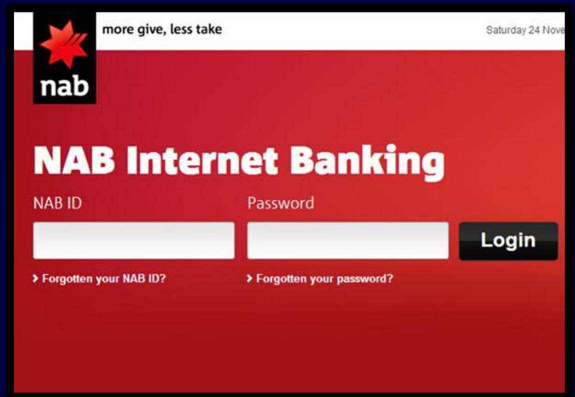


Laszlo Bela Kish
Professor, Texas A&M University

Image: J. Chappell and D. Abbott, The Double –Padlock Problem, http://scholar.google.com.au/citations?user=fVJ8twEAAAAJ&hl=en

Introduction

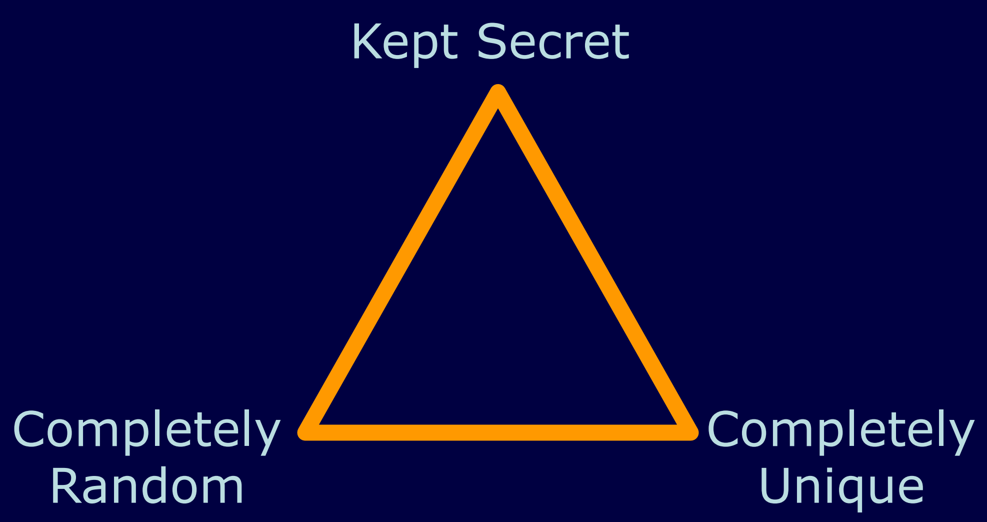
Project Significance & Implications

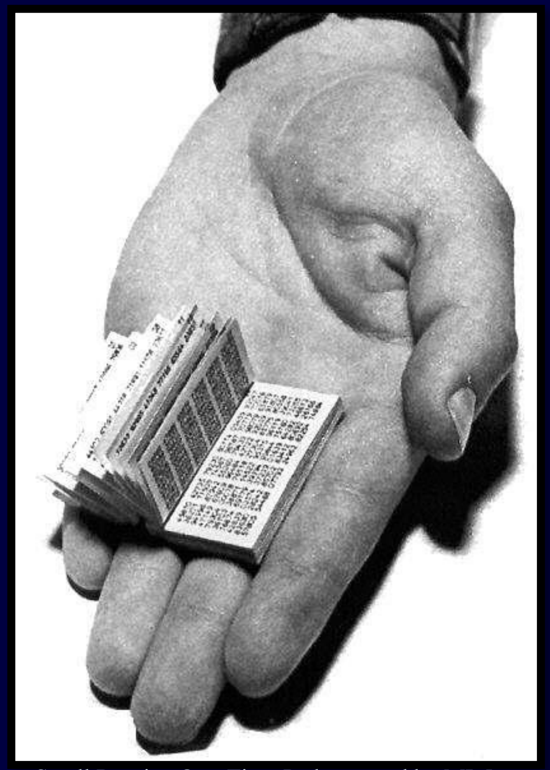


Images: aerospace.firetench.com, http://www.nab.com.au, http://www.jyi.org/wp-content/uploads//GPS_Satellite_NASA_art-iif.jpg

The One-Time Pad

Key Elements of the OTP





Small Russian One-Time Pad captured by MI-5

Image: www.ranum.com/security/computer_security/papers/otp-faq/

The One-Time Pad

Example – Bitwise XOR Operations

Message ⊕ Key = Ciphertext

Ciphertext ⊕ Key = Message

Alice

Message: 1010

⊕

Key: 1001

Ciphertext: 0011

Bob

Ciphertext: 0011

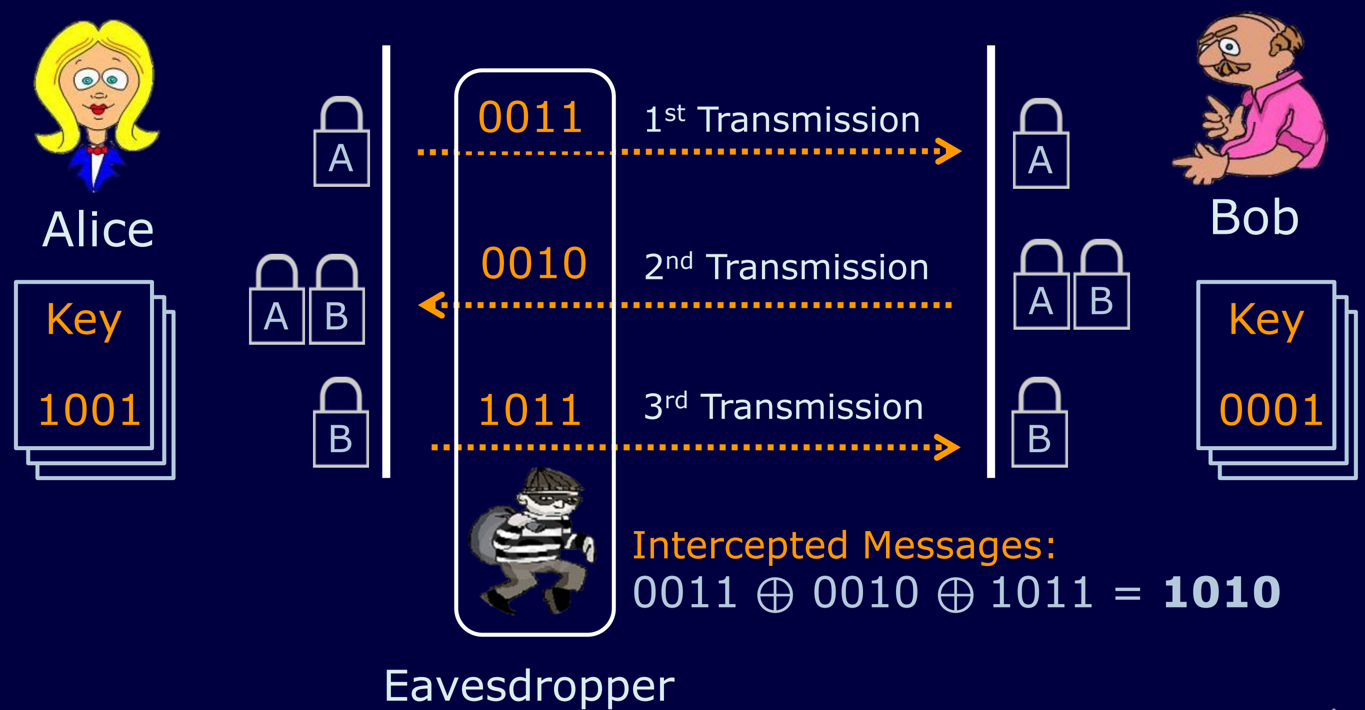
⊕

Key: 1001

The One-Time Pad

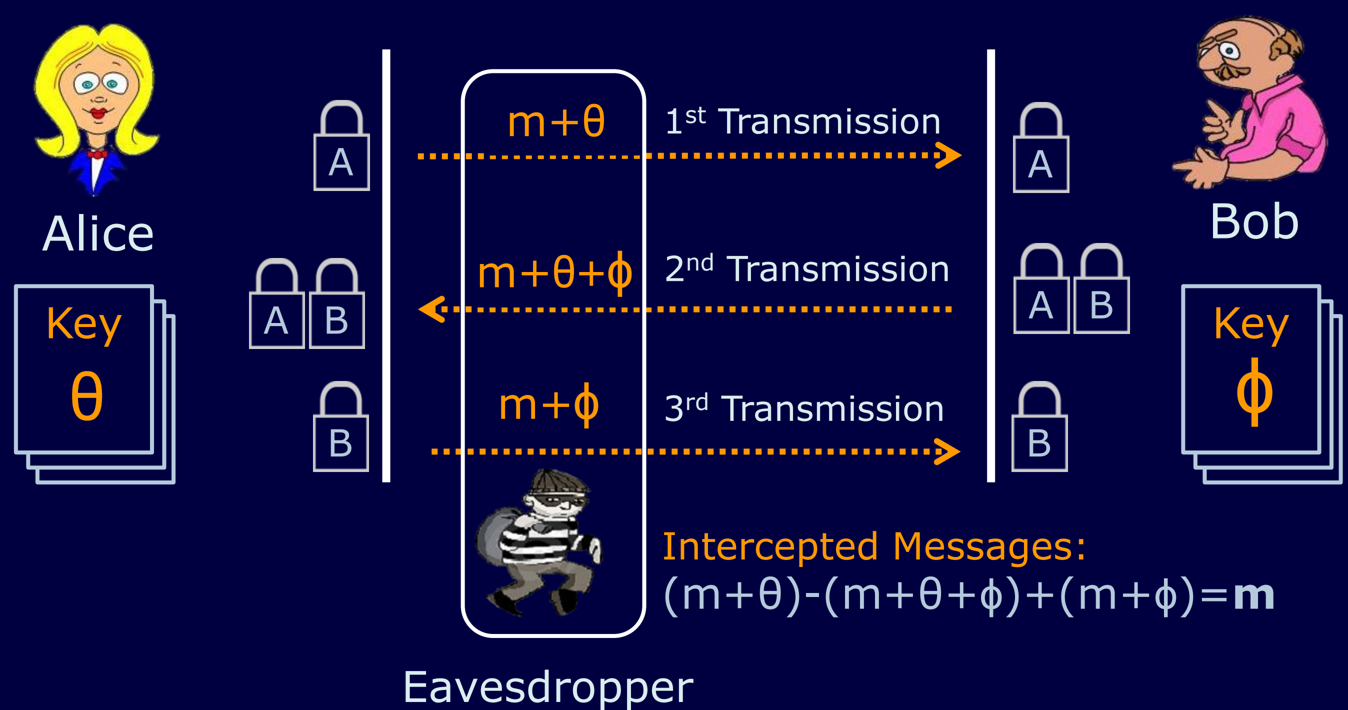
What if Alice & Bob each had their own unique OTP?

The initial Message is 1010



2D Rotations

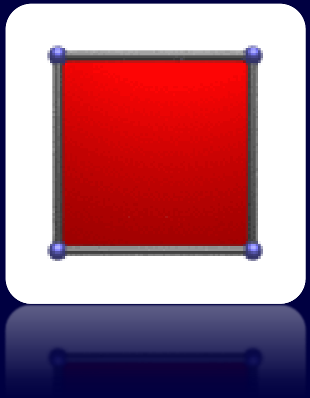
The XOR approach can be generalised to rotations in 2D

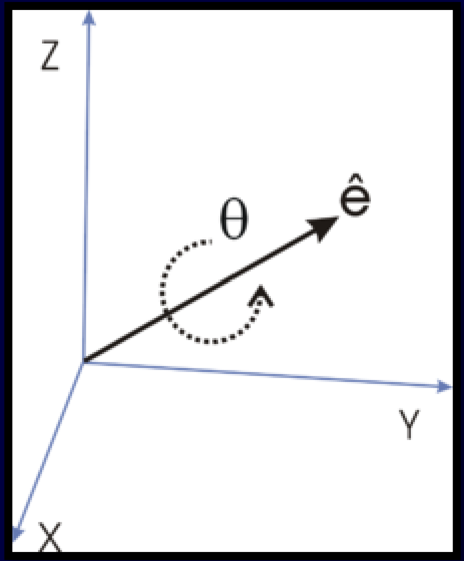


3D Rotations

Secure

The extra rotation axis provides ambiguity for eavesdroppers.





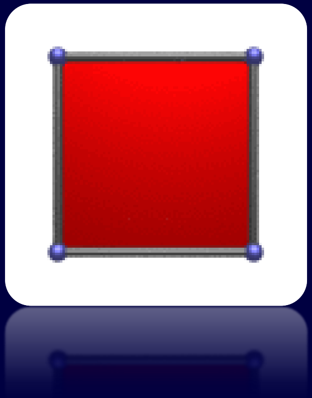


Image: http://eusebeia.dyndns.org/4d/vis/10-rot-1

Geometric Algebra

A Powerful Mathematical Tool

Ability to easily handle rotations in N-dimensions

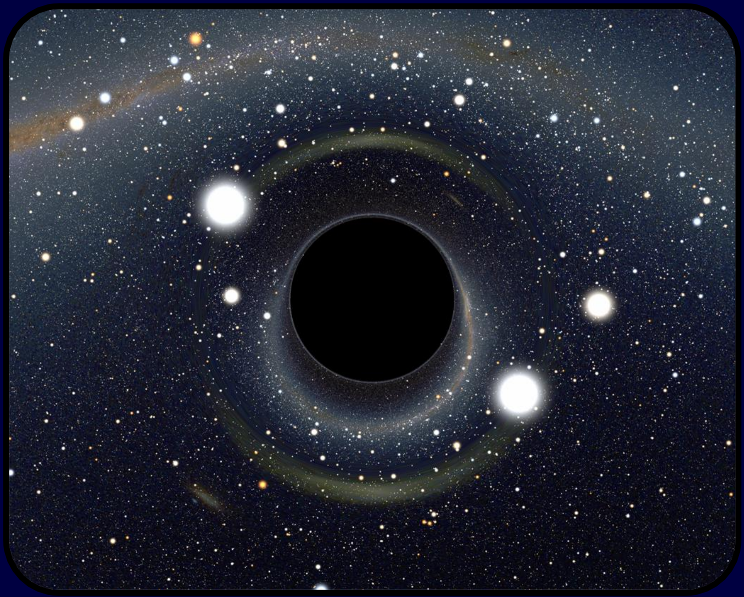


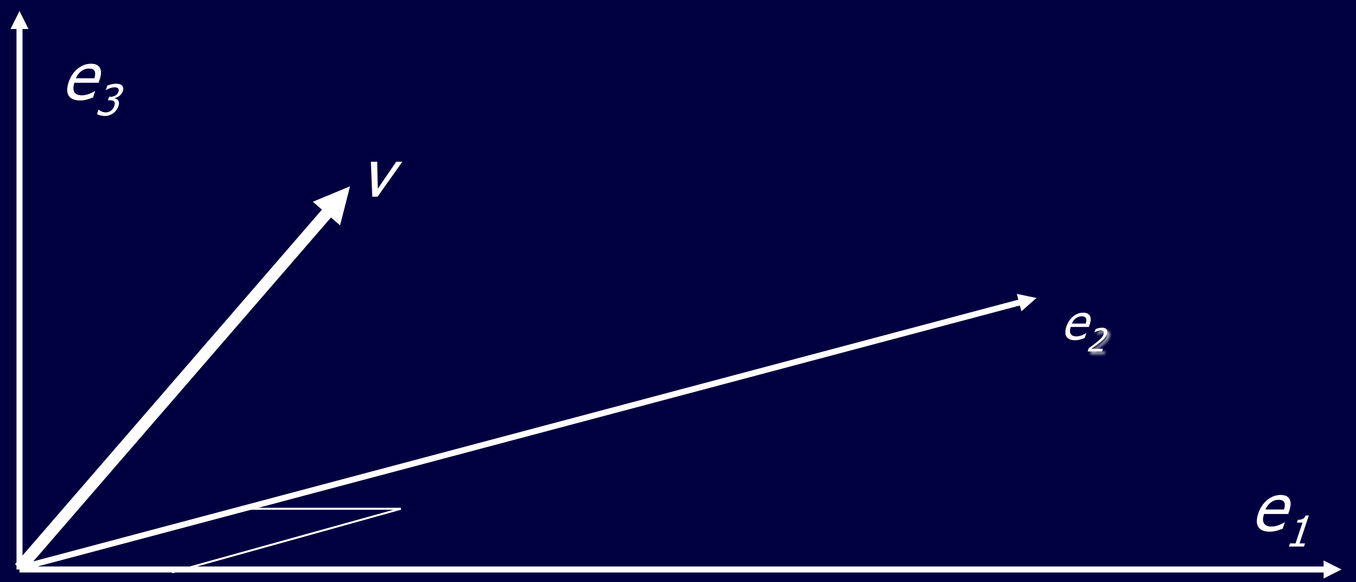
Image: apod.nasa.gov

Geometric Algebra

Vector v is defined as $v = a_1e_1 + a_2e_2 + a_3e_3$

$e_1^2 = e_2^2 = e_3^2 = 1$, and $i = e_1e_2e_3$

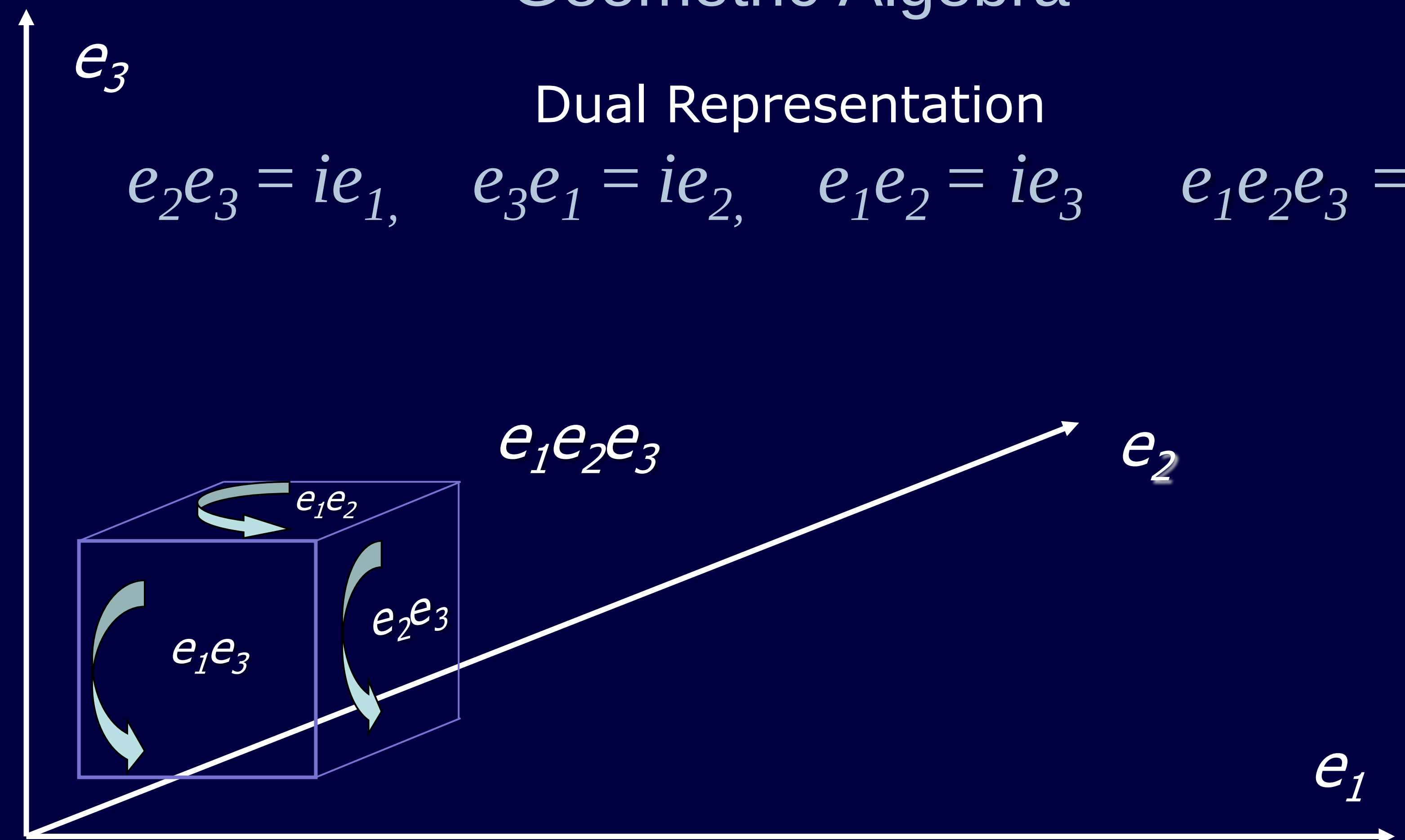
Anti-commuting, that is $e_1e_2 = -e_2e_1$



Geometric Algebra

Dual Representation

$$e_2e_3 = ie_1, \quad e_3e_1 = ie_2, \quad e_1e_2 = ie_3 \quad e_1e_2e_3 = i$$



Geometric Algebra

So why don't 3D rotations commute?

$$uv$$

$$= (e_1u_1 + e_2u_2 + e_3u_3)\,(e_1v_1 + e_2v_2 + e_3v_3)$$

$$= u_1v_1 + u_2v_2 + u_3v_3 + (u_2v_3 - v_2u_3)e_2e_3 + (u_1v_3 - v_1u_3)e_1e_3 + (u_1v_2 - v_1u_2)e_1e_2$$

$$= u_i\,v_i + i[(u_2v_3 - v_2u_3)e_1 + (u_1v_3 - v_1u_3)e_2 + (u_1v_2 - v_1u_2)e_3]$$

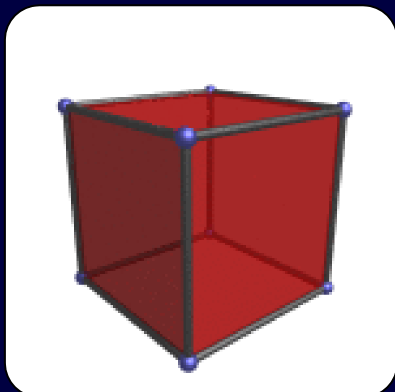
$$= u \cdot v + iu \times v$$

Since $v \cdot u = u \cdot v$,

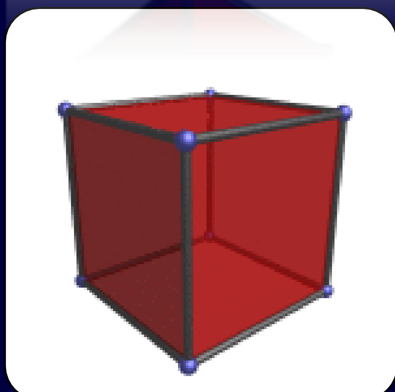
$uv = vu$ only when $u \times v = v \times u = 0$

Source: James Chappell

Geometric Algebra



$$v' = e^{i\theta/2}.v.e^{-i\theta/2}$$



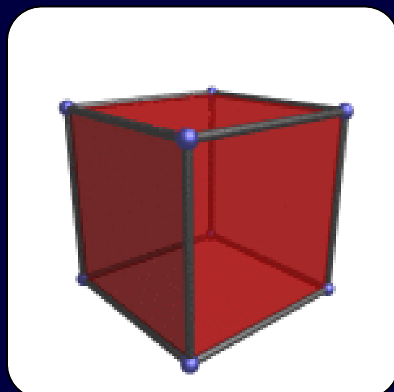


Image: http://eusebeia.dyndns.org/4d/vis/10-rot-1

What now?

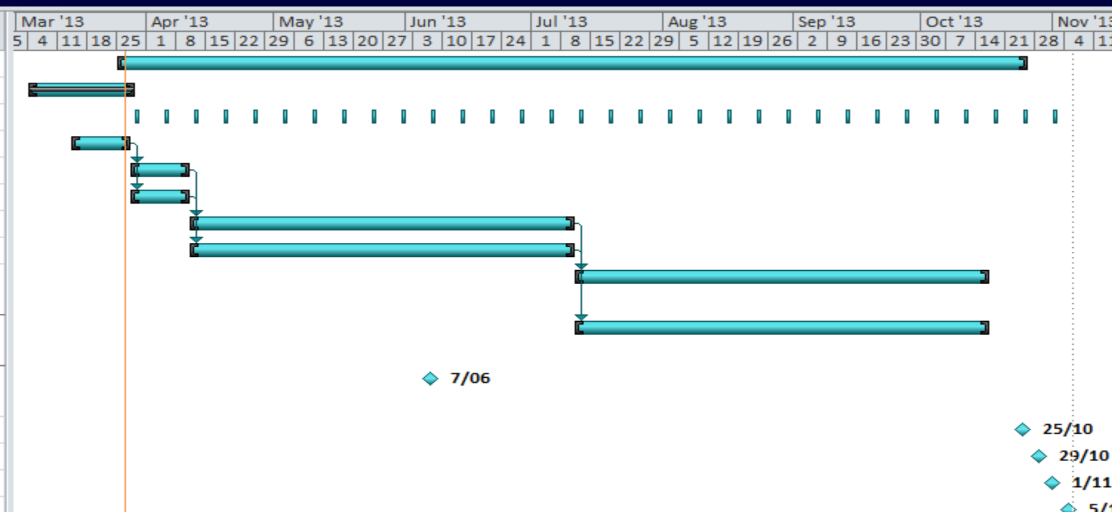
Pascal's Triangle

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1

Project Plan

Gantt Chart & Team Management

Task Name	Duration	Start	Finish
Documentation	155 days	Mon 25/03/13	Fri 25/10/13
Proposal Seminar	19 days	Mon 4/03/13	Thu 28/03/13
Weekly Reports	**156 days**	**Fri 29/03/13**	**Fri 1/11/13**
GA Introduction	10 days	Thu 14/03/13	Wed 27/03/13
3D Rotations: Practical	10 days	Thu 28/03/13	Wed 10/04/13
3D Rotations: Analytical	10 days	Thu 28/03/13	Wed 10/04/13
4D Rotations: Practical	65 days	Thu 11/04/13	Wed 10/07/13
4D Rotations: Analytical	65 days	Thu 11/04/13	Wed 10/07/13
N Dimension Rotations: Practical	70 days	Thu 11/07/13	Wed 16/10/13
N Dimension Rotations: Analytical	70 days	Thu 11/07/13	Wed 16/10/13
Semester A Progress Report Due	0 days	Fri 7/06/13	Fri 7/06/13
Wiki Finalised	0 days	Fri 25/10/13	Fri 25/10/13
Exhibition Posters Due	0 days	Tue 29/10/13	Tue 29/10/13
Project Exhibition Day	0 days	Fri 1/11/13	Fri 1/11/13
Project Closeout	0 days	Tue 5/11/13	Tue 5/11/13



Risk Management Plan

Project Risks

Risk	Likelihood	Severity	Avoidance/Mitigation Strategies
Unavailability of Team Member	Low	Medium	Both members are well versed in each aspect of the project and the overall progress.
SVN Blackout	Very Low	Low	Group members will ensure that all progress is shared via the wiki and by email so that we have several working copies available.
A Lack of Technical Knowledge	Low	High	We'll need to ensure that we're maintaining communication with each other and our supervisors to make sure that we understand the technical elements of the project – mainly GA.
Falling Behind Schedule as a result of the increased complexity of the project.	Low	Medium	Re-evaluate our expectations of the project, and perhaps increase the focus in lower dimensions (such as 4, 5 and 6) before even considering the higher dimensions.
Not finding a solution for keyless encryption	Very High	Very Low	Ensure that out work is completely documented, so that regardless of what we've found we have something to show at the project closing.

Question Time

References

[1] S. Palmira, 'Advantages and Disadvantages of Secure Communication *http://www.buzzle.com/articles/advantages-and-disadvantages-of-electronic-communication.html* (March 2012)

[2] 'Visualizing 4D Visualization' *http://eusebeia.dyndns.org/4d/vis/10-rot-1* (August 2012)

[3] J. Chappell and D. Abbott, 'The double-padlock problem: is secure classical information transmission possible without key exchange?' (March 2013)

[4] J. Chappell, 'Geometric Algebra Project Slides' (March 2013)

[5] RSA Labs 'What is Public Key Cryptography', *http://www.rsa.com/rsalabs/node.asp?id=2165*

[6] L. B. Kish and J. A. Bergou, 'An absolutely secure QKD scheme with no detection noise, entanglement and classical communication' (Sep 2005)