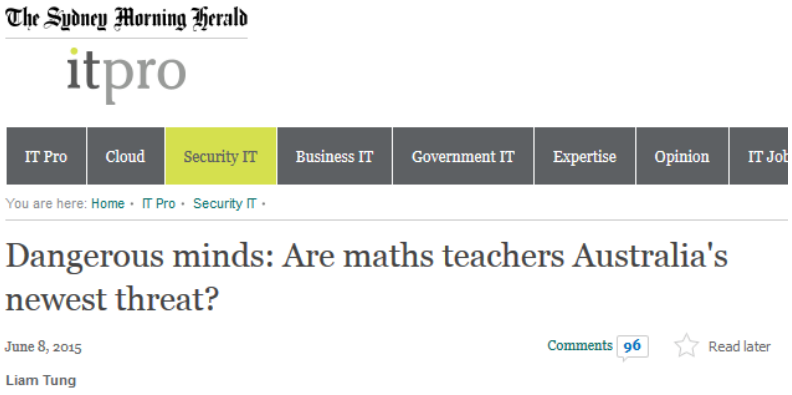
Your calculator as a weapon

Daniel V Mathews

Daniel.Mathews@monash.edu

Recent controversy



The Sydney Morning Herald

itpro

IT Pro | Cloud | Security IT | Business IT | Government IT | Expertise | Opinion | IT Jo

You are here: Home • IT Pro • Security IT •

Dangerous minds: Are maths teachers Australia's newest threat?

June 8, 2015

Comments 96 Read later

Liam Tung

Recent controversy

The Sydney Morning Herald

itpro

IT Pro | Cloud | Security IT | Business IT | Government IT | Expertise | Opinion | IT Jo

You are here: Home • IT Pro • Security IT •

Dangerous minds: Are maths teachers Australia's newest threat?

June 8, 2015

Liam Tung

Comments 96 Read later

THE CONVERSATION

Academic rigour, journalistic flair

Arts + Culture | Business + Economy | Education | Environment + Energy | Health + Medicine | Politics + Society | Scien

Paranoid defence controls could criminalise teaching encryption

May 19, 2015 2.37pm AEST

Recent controversy

The Sydney Morning Herald

itpro

IT Pro | Cloud | Security IT | Business IT | Government IT | Expertise | Opinion | IT Jo

You are here: Home • IT Pro • Security IT •

Dangerous minds: Are maths teachers Australia's newest threat?

June 8, 2015

Liam Tung

Comments 96 Read later

THE CONVERSATION

Academic rigour, journalistic flair

Arts + Culture | Business + Economy | Education | Environment + Energy | Health + Medicine | Politics + Society | Scien

Paranoid defence controls could criminalise teaching encryption

May 19, 2015 2.37pm AEST

Australia's Act of Intellectual Terrorism: DTCA 2012

— Kevin B Korb

In October 2012 the Australian parliament passed the Defence Trade Controls Act. The stated purposes of the act are unobjectionable: implementing the prior Australia-United States Defense Trade Cooperation Treaty, simplifying defence-related trade between Australia, the US and the UK, and tightening the regulation of intangible transfers of military goods, reflecting the growth of the internet in communications. Unfortunately, these good intentions have led the Australian government to adopt an extraordinarily broad definition of military goods and to impose an impossibly harsh regulatory regime on activities concerning them, to the point that what is today ordinary academic research into, for example, Bayesian

Recent controversy

The Sydney Morning Herald

itpro

IT Pro | Cloud | Security IT | Business IT | Government IT | Expertise | Opinion | IT Jobs

You are here: Home • IT Pro • Security IT •

Dangerous minds: Are maths teachers Australia's newest threat?

International Association for Cryptologic Research

Search IACR | Search

Home | Meetings | Publications | Awards | News | Services | Jobs | Members | About

Response to Australia's Defence Trade Controls Act

July 6, 2015

We are deeply concerned about Australia's Defence Trade Controls Act (DTCA). The act prohibits the "intangible supply" of encryption technologies, and hence subjects many ordinary teaching and research activities to unclear, potentially severe, export controls. As an international organization of cryptographic researchers and educators, we are concerned that the DTCA criminalizes the very essence of our association: to advance the theory and practice of cryptography in the service of public welfare.

We affirm that the public welfare of Australians — and society in general — is best served by open research and education in cryptography and cybersecurity. Open, international scientific collaboration is responsible for the encryption technologies that are now vital to individuals, businesses, and world governments alike. The current legislation cuts off Australia from the international cryptographic research community and jeopardizes the supply of qualified workforce in Australia's growing cybersecurity sector.

We call on Australia to amend their export control laws to include clear exemptions for scientific research and for education.

IACR Member Signatories (219): add your signature!

- Christian Cachin, President of the IACR, IBM Research - Zurich, Switzerland
- Nigel Smart, Vice President IACR, University of Bristol, United Kingdom
- Gregory Rose, Cryptography Consultant, Australian citizen and IACR treasurer, United States

ERSATION

Search

Education | Environment + Energy | Health + Medicine | Politics + Society | Scien

fence controls could teaching encryption

of Intellectual A 2012

— Kevin B Korb

nent passed the Defence Trade Controls Act. The stated purposes of the act are unobjectionable: implementing the prior Australia-United States Defense Trade Cooperation Treaty, simplifying defence-related trade between Australia, the US and the UK, and tightening the regulation of intangible transfers of military goods, reflecting the growth of the internet in communications. Unfortunately, these good intentions have led the Australian government to adopt an extraordinarily broad definition of military goods and to impose an impossibly harsh regulatory regime on activities concerning them, to the point that what is today ordinary academic research into, for example, Bayesian

What's it about?

Liam Tung, Fairfax press, June 8:

Australian academics who teach mathematics may need to run new ideas by the Department of Defence before sharing them or risk imprisonment.

What's it about?

Liam Tung, Fairfax press, June 8:

Australian academics who teach mathematics may need to run new ideas by the Department of Defence before sharing them or risk imprisonment.

...

From November 2016 Australian academics could face a potential 10-year prison term for sending information overseas if their ideas fall within the Defence Strategic Goods List (DSGL).

What's it about?

Liam Tung, Fairfax press, June 8:

Australian academics who teach mathematics may need to run new ideas by the Department of Defence before sharing them or risk imprisonment.

...

From November 2016 Australian academics could face a potential 10-year prison term for sending information overseas if their ideas fall within the Defence Strategic Goods List (DSGL).

Put another way, they could be jailed for delivering online course material to foreign students or providing international peers with access to a server hosting that material.

What's it about?

Liam Tung, Fairfax press, June 8:

Australian academics who teach mathematics may need to run new ideas by the Department of Defence before sharing them or risk imprisonment.

...

From November 2016 Australian academics could face a potential 10-year prison term for sending information overseas if their ideas fall within the Defence Strategic Goods List (DSGL).

Put another way, they could be jailed for delivering online course material to foreign students or providing international peers with access to a server hosting that material.

Academics like Kevin Korb are nervous that "overly broad" definitions in the DSGL could land them in court for teaching cryptography... and a number of other fields.

Plan

I'll try to:

- Show you some of these laws and try to make some sense of them
- Explain some related ideas from mathematics and cryptography
- Present a facetious-but-not-that-facetious argument that your calculator could be regarded as a dual-use military-civilian item ("weapon")
- Raise some broader issues

The laws

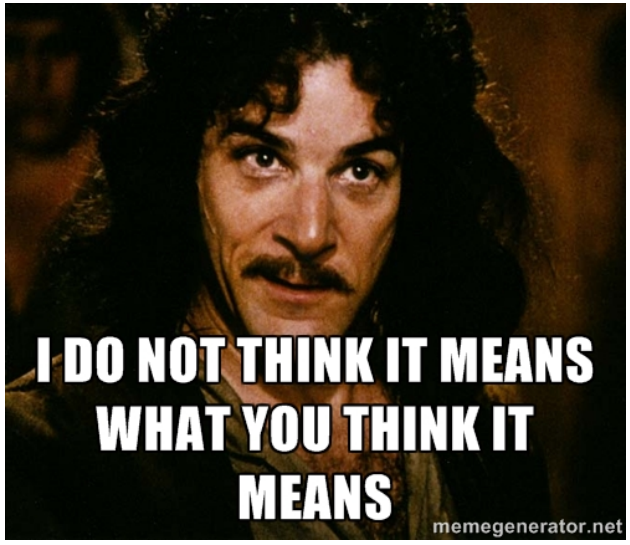
Warning/disclaimer:

- These laws are convoluted.

The laws

Warning/disclaimer:

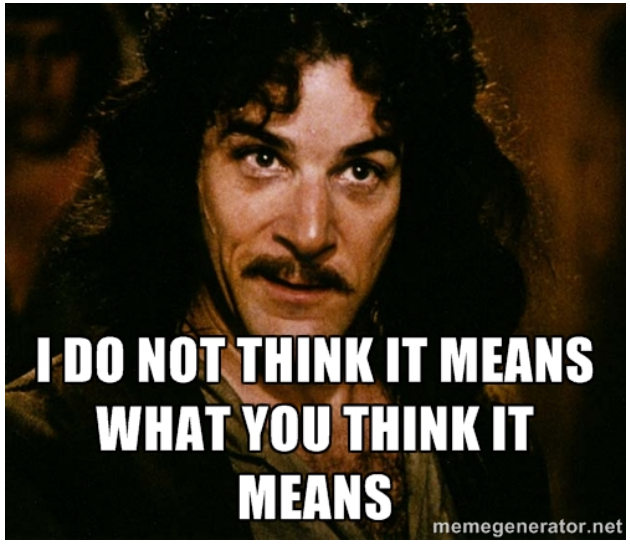
- These laws are convoluted.
- Law is never simple.



The laws

Warning/disclaimer:

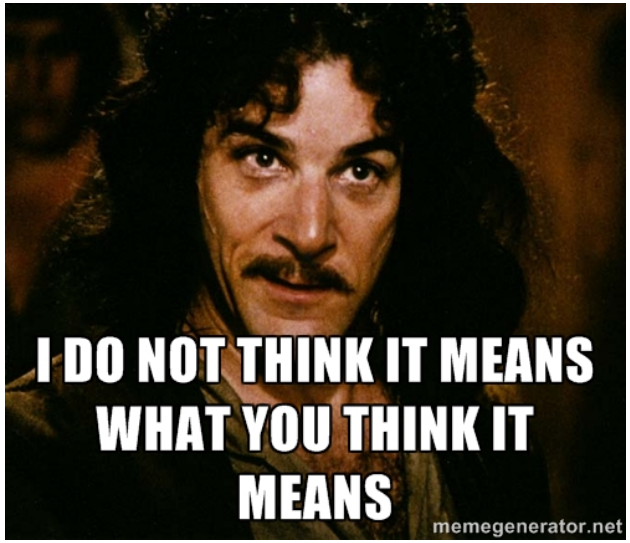
- These laws are convoluted.
- Law is never simple.
- Authoritative interpretation of laws comes from courts via litigation.



The laws

Warning/disclaimer:

- These laws are convoluted.
- Law is never simple.
- Authoritative interpretation of laws comes from courts via litigation.



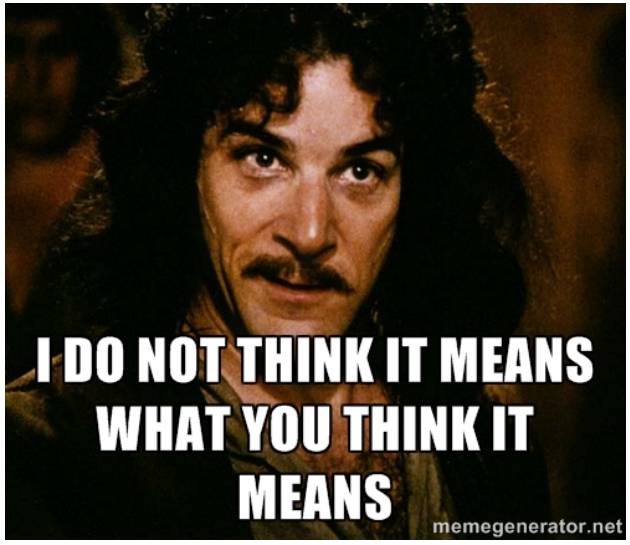
Defence Trade Controls Act (DTCA)

- Passed 2012
- 96 pages long
- Main provisions were due to come into effect 16 May 2015

The laws

Warning/disclaimer:

- These laws are convoluted.
- Law is never simple.
- Authoritative interpretation of laws comes from courts via litigation.



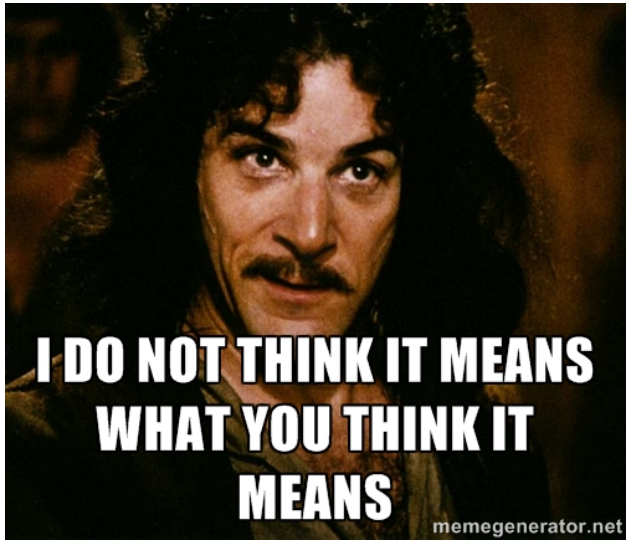
Defence Trade Controls Act (DTCA)

- Passed 2012
- 96 pages long
- Main provisions were due to come into effect 16 May 2015
- Major amendments passed both houses 18 March 2015
- Now 112 pages long

The laws

Warning/disclaimer:

- These laws are convoluted.
- Law is never simple.
- Authoritative interpretation of laws comes from courts via litigation.



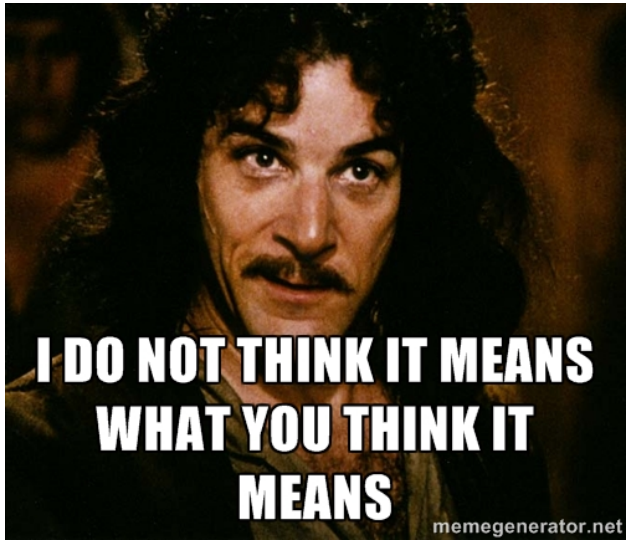
Defence Trade Controls Act (DTCA)

- Passed 2012
- 96 pages long
- Main provisions were due to come into effect 16 May 2015
- Major amendments passed both houses 18 March 2015
- Now 112 pages long
- Royal assent (became law) 2 April 2015
- Main provisions now due to come into effect 2 April 2016

The laws

Warning/disclaimer:

- These laws are convoluted.
- Law is never simple.
- Authoritative interpretation of laws comes from courts via litigation.



Defence Trade Controls Act (DTCA)

- Passed 2012
- 96 pages long
- Main provisions were due to come into effect 16 May 2015
- Major amendments passed both houses 18 March 2015
- Now 112 pages long
- Royal assent (became law) 2 April 2015
- Main provisions now due to come into effect 2 April 2016

Most controversial provision: section 10

- *Offence — supply of DSGL technology*

DTCA section 10

to supply DSGL technology. There is a process for becoming a registered broker.

Division 1—Primary offences

10 Offence—supply of DSGL technology

(1) A person (the ***supplier***) commits an offence if:

(a) the supplier supplies DSGL technology to another person; and

(b) either:

(i) the supply is from a place in Australia to a place outside Australia; or

(ii) if the supply is the provision of access to DSGL technology—at the time of the provision of access, the supplier is in Australia and the other person is outside Australia; and

(c) either:

(i) the supplier does not hold a permit under section 11 authorising the supply ~~of the DSGL technology~~; or

(ii) the supply ~~of the DSGL technology~~ contravenes a condition of a permit that the supplier holds under section 11; and

(d) there is no notice in force under subsection 14(1) in relation to the supplier and the supply.

Penalty: Imprisonment for 10 years or 2,500 penalty units, or both.

Exceptions

(1A) Subsection (1) does not apply if:

(a) the supply is not the provision of access to DSGL technology; and

(b) the supply is made orally; and

(c) the supply is neither for a military end-use nor for use in a Weapons of Mass Destruction program.

Note: A defendant bears an evidential burden in relation to the matter in subsection (1A): see subsection 13.3(3) of the *Criminal Code*.

(2) Subsection (1) does not apply if:

(a) the supply is of DSGL technology in relation to original goods; and

(b) the supply is by an Australian Community member or by a member of the United States Community; and

(c) the supply is to an Australian Community member or a member of the United States Community; and

(d) the supply is for an activity referred to in Article 3(1)(a), (b), (c) or (d) of the Defense Trade Cooperation Treaty; and

(e) at the time of the supply, the original goods are listed in Part 1 of the Defense Trade Cooperation Munitions List; and

(f) at the time of the supply, the original goods are not listed in Part 2 of the Defense Trade Cooperation Munitions List.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2): see subsection 13.3(3) of the *Criminal Code*.

(3) Subsection (1) does not apply if:

(a) the DSGL technology is supplied by or to a person who is a member of the Australian Defence Force, an APS employee, an employee of ASIO, an employee of ASIS, a member or special member of the Australian Federal Police or a member of the police force of a State or Territory; and

(b) the supply occurs ~~he or she supplies the DSGL technology~~ in the course of his or her duties as such a person.

Note: A defendant bears an evidential burden in relation to the matter in subsection (3): see subsection 13.3(3) of the *Criminal Code*.

(3A) Subsection (1) does not apply if:

(a) the supply is of DSGL technology within the scope of Part 2 of the Defence and Strategic Goods List; and

(b) the supply is preparatory to the publication of the DSGL technology to the public or to a section of the public; and

(c) there is neither a notice in force under subsection 14B(1), nor a notice in force under subsection 14C(1), in relation to the supplier and the DSGL technology.

Note: A defendant bears an evidential burden in relation to the matter in subsection (3A): see subsection 13.3(3) of the *Criminal Code*.

(4) Subsection (1) does not apply in the circumstances prescribed by the regulations for the purposes of this subsection.

Note: A defendant bears an evidential burden in relation to the matter in subsection (4): see subsection 13.3(3) of the *Criminal Code*.

~~*Geographical jurisdiction*~~

~~(5) Section 15.2 of the *Criminal Code* (extended geographical jurisdiction—category B) applies to an offence against subsection (1).~~

Definition

(6) In this section:

place includes:

(a) a vehicle, vessel or aircraft; and

(b) an area of water; and

(c) a fixed or floating structure or installation of any kind.

11 Permits for purposes of section 10

(1) A person may apply to the Minister for a permit under this section to supply DSGL technology ~~to another person~~.

Note: Section 66 sets out application requirements.

(2) Without limiting subsection (1), an application by a person under that subsection may do one or more of the following:

(a) cover 2 or more supplies by the person;

(b) cover one or more supplies by the person for a period described in the application;

(c) cover one or more supplies by the person for a project described in the application.

DTCA section 10

A summary of the offence:

- The “supply" of “DSGL technology" overseas without a permit is an offence.
- (But military technology may flow freely US $\leftrightarrow$ Australia.)
- Exemptions for “supplies" which are “oral" or “preparatory to publication" to (a section of) the public.
- Maximum penalty: 10 years imprisonment or $\$450,000$ fine

DTCA section 10

A summary of the offence:

- The “supply" of “DSGL technology" overseas without a permit is an offence.
- (But military technology may flow freely US $\leftrightarrow$ Australia.)
- Exemptions for “supplies" which are “oral" or “preparatory to publication" to (a section of) the public.
- Maximum penalty: 10 years imprisonment or $\$450,000$ fine

supply:

(a) includes supply by way of sale, exchange, gift, lease, hire or hire-purchase; and

(b) in relation to DSGL technology—includes provide access to DSGL technology.

DTCA section 10

A summary of the offence:

- The “supply" of “DSGL technology" overseas without a permit is an offence.
- (But military technology may flow freely US $\leftrightarrow$ Australia.)
- Exemptions for “supplies" which are “oral" or “preparatory to publication" to (a section of) the public.
- Maximum penalty: 10 years imprisonment or $\$450,000$ fine

supply:

(a) includes supply by way of sale, exchange, gift, lease, hire or hire-purchase; and

(b) in relation to DSGL technology—includes provide access to DSGL technology.

DTCA section 10

A summary of the offence:

- The “supply" of “DSGL technology" overseas without a permit is an offence.
- (But military technology may flow freely US $\leftrightarrow$ Australia.)
- Exemptions for “supplies" which are “oral" or “preparatory to publication" to (a section of) the public.
- Maximum penalty: 10 years imprisonment or \$450,000 fine

supply:

(a) includes supply by way of sal
hire-purchase; and

(b) in relation to DSGL technolo
DSGL technology.

Existing Gaps – Intangible Supply

- A permit is required if an Australian physically exports a controlled virus. However, if they email instructions on how to produce or enhance that virus, no permit is currently required.
- The Australian Government has no visibility or control over the electronic export of this information, including whether it is potentially destined for a biological weapons program.

DTCA section 10

“Supply":

- Need not be for payment.
- Can include *email explanations*.

DTCA section 10

“Supply":

- Need not be for payment.
- Can include *email explanations*.

“DSGL technology":

- Refers to the *Defence and Strategic Goods List* (DSGL)
- A list of controlled technology.

DTCA section 10

“Supply":

- Need not be for payment.
- Can include *email explanations*.

“DSGL technology":

- Refers to the *Defence and Strategic Goods List* (DSGL)
- A list of controlled technology.
- Promulgated 1996, amended regularly

DTCA section 10

“Supply":

- Need not be for payment.
- Can include *email explanations*.

“DSGL technology":

- Refers to the *Defence and Strategic Goods List* (DSGL)
- A list of controlled technology.
- Promulgated 1996, amended regularly
- Current version 431 pages long.

DTCA section 10

“Supply":

- Need not be for payment.
- Can include *email explanations*.

“DSGL technology":

- Refers to the *Defence and Strategic Goods List* (DSGL)
- A list of controlled technology.
- Promulgated 1996, amended regularly
- Current version 431 pages long.

DSGL is essentially in two parts:

- Part 1: *Munitions list*
- Part 2: *Dual-use list*

Contents

DSGL

Contents

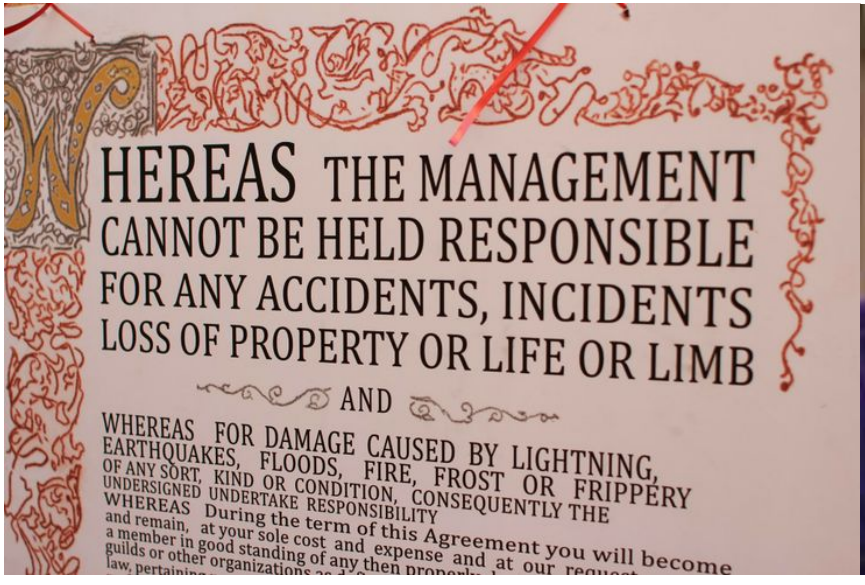
DSGL

Contents

DSGL

Contents

DSGL


HEREAS THE MANAGEMENT
CANNOT BE HELD RESPONSIBLE
FOR ANY ACCIDENTS, INCIDENTS
LOSS OF PROPERTY OR LIFE OR LIMB
AND
WHEREAS FOR DAMAGE CAUSED BY LIGHTNING,
EARTHQUAKES, FLOODS, FIRE, FROST OR FRIPPERY
OF ANY SORT, KIND OR CONDITION, CONSEQUENTLY THE
UNDERSIGNED UNDERTAKE RESPONSIBILITY
WHEREAS During the term of this Agreement you will become
and remain, at your sole cost and expense and at our request
a member in good standing of any then properly
guilds or other organizations
law, pertaining


FOR ANY ACCIDENTS
LOSS OF PROPERTY OR LIFE OR LIM

Category 5 — Telecommunications and “information security"

Part 2 — “INFORMATION SECURITY"

5A2 Systems, Equipment and Components

5A002 “Information security" systems, equipment and components therefor, as follows: ...

a. Systems, equipment, application specific “electronic assemblies", modules and integrated circuits for “information security", as follows and components therefor specially designed for “information security": ...

1. Designed or modified to use “cryptography" employing digital techniques performing any cryptographic function other than authentication, digital signature or the execution of copy-protected “software", and having any of the following: ...
   a. A “symmetric algorithm" employing a key length in excess of 56 bits; or ...
   b. An “asymmetric algorithm" where the security of the algorithm is based on any of the following: ...
      1. Factorisation of integers in excess of 512 bits (e.g., RSA);
      2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); or
      3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2. in excess of 112 bits (e.g., Diffie-Hellman over an elliptic curve);

Category 5 — Telecommunications and “information security"

Part 2 — “INFORMATION SECURITY"

5A2 Systems, Equipment and Components

5A002 “Information security" systems, equipment and components therefor, as follows: ...

a. Systems, equipment, application specific “electronic assemblies", modules and integrated circuits for “information security", as follows and components therefor specially designed for “information security": ...

1. Designed or modified to use “cryptography" employing digital techniques performing any cryptographic function other than authentication, digital signature or the execution of copy-protected “software", and having any of the following: ...
   a. A “symmetric algorithm" employing a key length in excess of 56 bits; or ...
   b. An “asymmetric algorithm" where the security of the algorithm is based on any of the following: ...
      1. Factorisation of integers in excess of 512 bits (e.g., RSA);
      2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); or
      3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2. in excess of 112 bits (e.g., Diffie-Hellman over an elliptic curve);

Category 5 — Telecommunications and “information security"

Part 2 — “INFORMATION SECURITY"

5A2 Systems, Equipment and Components

5A002 “Information security" systems, equipment and components therefor, as follows: ...

a. Systems, equipment, application specific “electronic assemblies", modules and integrated circuits for “information security", as follows and components therefor specially designed for “information security": ...

1. Designed or modified to use “cryptography" employing digital techniques performing any cryptographic function other than authentication, digital signature or the execution of copy-protected “software", and having any of the following: ...
   a. A “symmetric algorithm" employing a key length in excess of 56 bits; or ...
   b. An “asymmetric algorithm" where the security of the algorithm is based on any of the following:
      1. Factorisation of integers in excess of 512 bits (e.g., RSA);
      2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); or
      3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2. in excess of 112 bits (e.g., Diffie-Hellman over an elliptic curve);

DSGL section 5A002.a.1

Essentially:

- Any “system" or “equipment" which does sufficiently strong encryption is covered.
- Encryption strength is measured in various ways (key length, Size of integers factorised, group size)

DSGL section 5A002.a.1

Essentially:

- Any “system" or “equipment" which does sufficiently strong encryption is covered.
- Encryption strength is measured in various ways (key length, Size of integers factorised, group size)

Note there are many exceptions, not all very clear.

- DSGL
- DTCA:

DSGL section 5A002.a.1

Essentially:

- Any “system" or “equipment" which does sufficiently strong encryption is covered.
- Encryption strength is measured in various ways (key length, Size of integers factorised, group size)

Note there are many exceptions, not all very clear.

- DSGL(roughly paraphrased):
  - “Basic scientific research"

- DTCA:

DSGL section 5A002.a.1

Essentially:

- Any “system" or “equipment" which does sufficiently strong encryption is covered.
- Encryption strength is measured in various ways (key length, Size of integers factorised, group size)

Note there are many exceptions, not all very clear.

- DSGL(roughly paraphrased):
  - “Basic scientific research": “*not primarily directed towards a specific practical aim or objective*."

- DTCA:

DSGL section 5A002.a.1

Essentially:

- Any “system" or “equipment" which does sufficiently strong encryption is covered.
- Encryption strength is measured in various ways (key length, Size of integers factorised, group size)

Note there are many exceptions, not all very clear.

- DSGL(roughly paraphrased):
  - “Basic scientific research": “*not primarily directed towards a specific practical aim or objective*."
  - Software already generally available to the public.
  - Technology/information in the public domain.

- DTCA:

DSGL section 5A002.a.1

Essentially:

- Any “system" or “equipment" which does sufficiently strong encryption is covered.
- Encryption strength is measured in various ways (key length, Size of integers factorised, group size)

Note there are many exceptions, not all very clear.

- DSGL(roughly paraphrased):
  - “Basic scientific research": “*not primarily directed towards a specific practical aim or objective*."
  - Software already generally available to the public.
  - Technology/information in the public domain.
  - Software necessary for previously authorised items.
  - Intricate exceptions for specific items.
- DTCA:

DSGL section 5A002.a.1

Essentially:

- Any “system" or “equipment" which does sufficiently strong encryption is covered.
- Encryption strength is measured in various ways (key length, Size of integers factorised, group size)

Note there are many exceptions, not all very clear.

- DSGL(roughly paraphrased):
  - “Basic scientific research": “*not primarily directed towards a specific practical aim or objective*."
  - Software already generally available to the public.
  - Technology/information in the public domain.
  - Software necessary for previously authorised items.
  - Intricate exceptions for specific items.
- DTCA:
  - Supplies preparatory to publication to public.
  - Some oral supplies.

DSGL section 5A002.a.1

Essentially:

- Any “system" or “equipment" which does sufficiently strong encryption is covered.
- Encryption strength is measured in various ways (key length, Size of integers factorised, group size)

Note there are many exceptions, not all very clear.

- DSGL(roughly paraphrased):
  - “Basic scientific research": “*not primarily directed towards a specific practical aim or objective*."
  - Software already generally available to the public.
  - Technology/information in the public domain.
  - Software necessary for previously authorised items.
  - Intricate exceptions for specific items.
- DTCA:
  - Supplies preparatory to publication to public.
  - Some oral supplies.
  - US/Australian military, intelligence, police.

Questions

Preceding provisions are premised on the idea that

sufficiently strong cryptography is a dual-use civilian-military technology.

Questions

Preceding provisions are premised on the idea that

sufficiently strong cryptography is a dual-use civilian-military technology.

Political/moral/legal/policy questions:

- Is this idea right?

Questions

Preceding provisions are premised on the idea that

sufficiently strong cryptography is a dual-use civilian-military technology.

Political/moral/legal/policy questions:

- Is this idea right?
- Even if it has dual uses, is it appropriate to regulate via a permit regime with heavy criminal sanctions?

Questions

Preceding provisions are premised on the idea that

sufficiently strong cryptography is a dual-use civilian-military technology.

Political/moral/legal/policy questions:

- Is this idea right?
- Even if it has dual uses, is it appropriate to regulate via a permit regime with heavy criminal sanctions?
- Even if it is a dual use technology appropriate for such regulation, are there sufficient exceptions?

Questions

Preceding provisions are premised on the idea that

sufficiently strong cryptography is a dual-use civilian-military technology.

Political/moral/legal/policy questions:

- Is this idea right?
- Even if it has dual uses, is it appropriate to regulate via a permit regime with heavy criminal sanctions?
- Even if it is a dual use technology appropriate for such regulation, are there sufficient exceptions?
- Is this the right way to be thinking about cryptography? (Human rights, privacy, freedom of information...)

Questions

Preceding provisions are premised on the idea that

sufficiently strong cryptography is a dual-use civilian-military technology.

Political/moral/legal/policy questions:

- Is this idea right?
- Even if it has dual uses, is it appropriate to regulate via a permit regime with heavy criminal sanctions?
- Even if it is a dual use technology appropriate for such regulation, are there sufficient exceptions?
- Is this the right way to be thinking about cryptography? (Human rights, privacy, freedom of information...)

Applied cryptography question:

- How strong are the specifications in the DSGL?

Questions

Preceding provisions are premised on the idea that

sufficiently strong cryptography is a dual-use civilian-military technology.

Political/moral/legal/policy questions:

- Is this idea right?
- Even if it has dual uses, is it appropriate to regulate via a permit regime with heavy criminal sanctions?
- Even if it is a dual use technology appropriate for such regulation, are there sufficient exceptions?
- Is this the right way to be thinking about cryptography? (Human rights, privacy, freedom of information...)

Applied cryptography question:

- How strong are the specifications in the DSGL? WEAK!

Questions

Preceding provisions are premised on the idea that

sufficiently strong cryptography is a dual-use civilian-military technology.

Political/moral/legal/policy questions:

- Is this idea right?
- Even if it has dual uses, is it appropriate to regulate via a permit regime with heavy criminal sanctions?
- Even if it is a dual use technology appropriate for such regulation, are there sufficient exceptions?
- Is this the right way to be thinking about cryptography? (Human rights, privacy, freedom of information...)

Applied cryptography question:

- How strong are the specifications in the DSGL? WEAK!

Mathematics/computer science questions:

- What do the technical words even mean?

Some mathematics

In abstract algebra there are things called *groups*.

Some mathematics

In abstract algebra there are things called *groups*.
A group consists of:

- A *set* G, and
- A *binary operation* on G:

Some mathematics

In abstract algebra there are things called *groups*.
A group consists of:

- A *set* G, and
- A *binary operation* on G:
  - A way to combine two elements and get another element.
  - A function $G \times G \to G$.

Some mathematics

In abstract algebra there are things called *groups*.
A group consists of:

- A *set* G, and
- A *binary operation* on G:
  - A way to combine two elements and get another element.
  - A function $G \times G \to G$.
- Three technical conditions must be satisfied
  - (associativity, identity, inverses)

Some mathematics

In abstract algebra there are things called *groups*.
A group consists of:

- A *set* G, and
- A *binary operation* on G:
  - A way to combine two elements and get another element.
  - A function $G \times G \to G$.
- Three technical conditions must be satisfied
  - (associativity, identity, inverses)

Examples:

- The *integers* with the operation of *addition* $(\mathbb{Z}, +)$ form a group. $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$

Some mathematics

In abstract algebra there are things called *groups*.
A group consists of:

- A *set* G, and
- A *binary operation* on G:
  - A way to combine two elements and get another element.
  - A function $G \times G \to G$.
- Three technical conditions must be satisfied
  - (associativity, identity, inverses)

Examples:

- The *integers* with the operation of *addition* $(\mathbb{Z}, +)$ form a group. $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$
- The *positive real numbers* with the operation of *multiplication* $(\mathbb{R}_+, \times)$.

Modular arithmetic

An interesting and important source of groups: *remainders*.

Modular arithmetic

An interesting and important source of groups: *remainders*. Example:

- The set of “remainders after dividing by 12" or *integers modulo 12* forms a group under addition $(\mathbb{Z}_{12}, +)$.
- Telling the time.

Modular arithmetic

An interesting and important source of groups: *remainders*. Example:

- The set of “remainders after dividing by 12" or *integers modulo 12* forms a group under addition $(\mathbb{Z}_{12}, +)$.
- Telling the time.

$$1 + 1 = 2 \qquad 11 + 2 = 1$$

$$3 + 6 = 9 \qquad 9 + 8 = 5$$

Modular arithmetic

An interesting and important source of groups: *remainders*. Example:

- The set of “remainders after dividing by 12" or *integers modulo 12* forms a group under addition $(\mathbb{Z}_{12}, +)$.
- Telling the time.

$$1 + 1 = 2 \qquad 11 + 2 = 1 \qquad 12 = 0$$

$$3 + 6 = 9 \qquad 9 + 8 = 5$$

Modular arithmetic

An interesting and important source of groups: *remainders*. Example:

- The set of “remainders after dividing by 12" or *integers modulo 12* forms a group under addition $(\mathbb{Z}_{12}, +)$.
- Telling the time.

$$1 + 1 = 2 \qquad 11 + 2 = 1 \qquad 12 = 0$$

$$3 + 6 = 9 \qquad 9 + 8 = 5 \qquad -3 = 9$$

Modular arithmetic

An interesting and important source of groups: *remainders*. Example:

- The set of “remainders after dividing by 12" or *integers modulo 12* forms a group under addition $(\mathbb{Z}_{12}, +)$.
- Telling the time.

$$1 + 1 = 2 \qquad 11 + 2 = 1 \qquad 12 = 0$$
$$3 + 6 = 9 \qquad 9 + 8 = 5 \qquad -3 = 9$$

- Similarly, we can take “remainders after dividing by n" and obtain *integers modulo n* with addition $(\mathbb{Z}_n, +)$.

Modular arithmetic

If p is a prime, integers modulo p form a group with the operation of *multiplication!*

Modular arithmetic

If p is a prime, integers modulo p form a group with the operation of *multiplication!*

- (Except you have to remove 0; you can't undo multiplication by zero.)

Modular arithmetic

If p is a prime, integers modulo p form a group with the operation of *multiplication!*

- (Except you have to remove 0; you can't undo multiplication by zero.)

E.g. $p = 7$: $(\mathbb{Z}_7^*, \times)$.

$1 \times 2 = 2$

$3 \times 6 = 18 = 4$

Modular arithmetic

If p is a prime, integers modulo p form a group with the operation of *multiplication!*

- (Except you have to remove 0; you can't undo multiplication by zero.)

E.g. $p = 7$: $(\mathbb{Z}_7^*, \times)$.

$1 \times 2 = 2$ $\qquad$ $4 \times 2 = 8 = 1$

$3 \times 6 = 18 = 4$ $\qquad$ $2 \times 2 \times 2 = 1$

Modular arithmetic

If p is a prime, integers modulo p form a group with the operation of *multiplication!*

- (Except you have to remove 0; you can't undo multiplication by zero.)

E.g. $p = 7$: $(\mathbb{Z}_7^*, \times)$.

$1 \times 2 = 2$

$3 \times 6 = 18 = 4$

$4 \times 2 = 8 = 1$

$2 \times 2 \times 2 = 1$

$5 \times 3 = 1$

$3 = 5^{-1}$

Modular arithmetic

If p is a prime, integers modulo p form a group with the operation of *multiplication!*

- (Except you have to remove 0; you can't undo multiplication by zero.)

E.g. $p = 7$: $(\mathbb{Z}_7^*, \times)$.

$1 \times 2 = 2$

$4 \times 2 = 8 = 1$

$5 \times 3 = 1$

$3 \times 6 = 18 = 4$

$2 \times 2 \times 2 = 1$

$3 = 5^{-1}$

A group does not care if its operation is addition, multiplication, or anything else!

Groups

From now on write group operations by $\cdot$ (or juxtaposition).

Groups

From now on write group operations by $\cdot$ (or juxtaposition).

Careful!

Groups

From now on write group operations by $\cdot$ (or juxtaposition).

Careful!

- In $(\mathbb{Z}_7, +)$, $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 10 = 3$.

Groups

From now on write group operations by $\cdot$ (or juxtaposition).

Careful!

- In $(\mathbb{Z}_7, +)$, $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 10 = 3$.
- In $(\mathbb{Z}_7^*, \times)$, $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32 = 4$.

Groups

From now on write group operations by $\cdot$ (or juxtaposition).

Careful!

- In $(\mathbb{Z}_7, +)$, $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 10 = 3$.
- In $(\mathbb{Z}_7^*, \times)$, $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32 = 4$.
- In $(\mathbb{Z}, +)$, $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 10$.

Groups

From now on write group operations by $\cdot$ (or juxtaposition).

Careful!

- In $(\mathbb{Z}_7, +)$, $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 10 = 3$.
- In $(\mathbb{Z}_7^*, \times)$, $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32 = 4$.
- In $(\mathbb{Z}, +)$, $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 10$.
- In $(\mathbb{R}_+, \times)$, $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32$.

Groups

From now on write group operations by $\cdot$ (or juxtaposition).

Careful!

- In $(\mathbb{Z}_7, +)$, $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 10 = 3$.
- In $(\mathbb{Z}_7^*, \times)$, $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32 = 4$.
- In $(\mathbb{Z}, +)$, $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 10$.
- In $(\mathbb{R}_+, \times)$, $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32$.

Whatever operation we have, we can do it repeatedly and obtain *discrete exponentials*.

Groups

From now on write group operations by $\cdot$ (or juxtaposition).

Careful!

- In $(\mathbb{Z}_7, +)$, $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 10 = 3$.
- In $(\mathbb{Z}_7^*, \times)$, $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32 = 4$.
- In $(\mathbb{Z}, +)$, $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 10$.
- In $(\mathbb{R}_+, \times)$, $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32$.

Whatever operation we have, we can do it repeatedly and obtain *discrete exponentials*.

- In $(\mathbb{Z}_7, +)$, $2^5 = 3$.
- In $(\mathbb{Z}_7^*, \times)$, $2^5 = 4$.
- In $(\mathbb{Z}, +)$, $2^5 = 10$.
- In $(\mathbb{R}_+, \times)$, $2^5 = 32$.

Back to the DSGL

“Cryptography"... based on any of the following: ...

2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); or
3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2. in excess of 112 bits

Back to the DSGL

"Cryptography"... based on any of the following: ...

2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); or
3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2. in excess of 112 bits

- Groups!

Back to the DSGL

"Cryptography"... based on any of the following: ...

2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); or
3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2. in excess of 112 bits

- Groups!
- "Multiplicative group": Operation is multiplication.

Back to the DSGL

"Cryptography"... based on any of the following: ...

2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); or
3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2. in excess of 112 bits

- Groups!
- "Multiplicative group": Operation is multiplication.
- Like $(\mathbb{Z}_p^*, \times)$

Back to the DSGL

"Cryptography"... based on any of the following: ...

2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); or
3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2. in excess of 112 bits

- Groups!
- "Multiplicative group": Operation is multiplication.
- Like $(\mathbb{Z}_p^*, \times)$
- Indeed Z/pZ is another name for $\mathbb{Z}_p$!

Back to the DSGL

"Cryptography"... based on any of the following: ...

2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); or
3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2. in excess of 112 bits

- Groups!
- "Multiplicative group": Operation is multiplication.
- Like $(\mathbb{Z}_p^*, \times)$
- Indeed Z/pZ is another name for $\mathbb{Z}_p$!

Group with size 512 or 112 bits?

Back to the DSGL

"Cryptography"... based on any of the following: ...

2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); or
3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2. in excess of 112 bits

- Groups!
- "Multiplicative group": Operation is multiplication.
- Like $(\mathbb{Z}_p^*, \times)$
- Indeed Z/pZ is another name for $\mathbb{Z}_p$!

Group with size 512 or 112 bits?

- Groups have elements, not bits.
- Groups with 2^{512} or 2^{112} elements...

Back to the DSGL

"Cryptography"... based on any of the following: ...

2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); or
3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2. in excess of 112 bits

- Groups!
- "Multiplicative group": Operation is multiplication.
- Like $(\mathbb{Z}_p^*, \times)$
- Indeed Z/pZ is another name for $\mathbb{Z}_p$!

Group with size 512 or 112 bits?

- Groups have elements, not bits.
- Groups with 2^{512} or 2^{112} elements...

"Discrete logarithms"?

Discrete logarithms

- Exponentiation does repeated multiplication eg $2^5 = 32$

Discrete logarithms

- Exponentiation does repeated multiplication eg $2^5 = 32$
- Logarithm asks: *what power of 2 gives you 32?*

Discrete logarithms

- Exponentiation does repeated multiplication eg $2^5 = 32$
- Logarithm asks: *what power of 2 gives you 32?*
  - 5. So $\log_2 32 = 5$.

Discrete logarithms

- Exponentiation does repeated multiplication eg $2^5 = 32$
- Logarithm asks: *what power of 2 gives you 32?*
  - 5. So $\log_2 32 = 5$.

$$32 = 2^5 \text{ means the same as } \log_2 32 = 5.$$

Discrete logarithms

- Exponentiation does repeated multiplication eg $2^5 = 32$
- Logarithm asks: *what power of 2 gives you 32?*
  - 5. So $\log_2 32 = 5$.

$$32 = 2^5 \text{ means the same as } \log_2 32 = 5.$$

In general,

$$a = b^x \quad \Leftrightarrow \quad \log_b a = x.$$

This rule defines a *discrete logarithm* in *any group*.

Discrete logarithms

- Exponentiation does repeated multiplication eg $2^5 = 32$
- Logarithm asks: *what power of 2 gives you 32?*
  - 5. So $\log_2 32 = 5$.

$$32 = 2^5 \text{ means the same as } \log_2 32 = 5.$$

In general,

$$a = b^x \quad \Leftrightarrow \quad \log_b a = x.$$

This rule defines a *discrete logarithm* in *any group*.

- In $(\mathbb{Z}_7, +)$, $2^5 = 3$ so $\log_2 3 = 5$.

Discrete logarithms

- Exponentiation does repeated multiplication eg $2^5 = 32$
- Logarithm asks: *what power of 2 gives you 32?*
  - 5. So $\log_2 32 = 5$.

$$32 = 2^5 \text{ means the same as } \log_2 32 = 5.$$

In general,

$$a = b^x \quad \Leftrightarrow \quad \log_b a = x.$$

This rule defines a *discrete logarithm* in *any group*.

- In $(\mathbb{Z}_7, +)$, $2^5 = 3$ so $\log_2 3 = 5$.
- In $(\mathbb{Z}_7^*, \times)$, $2^5 = 4$ so $\log_2 4 = 5$.

Discrete logarithms

- Exponentiation does repeated multiplication eg $2^5 = 32$
- Logarithm asks: *what power of 2 gives you 32?*
  - 5. So $\log_2 32 = 5$.

$$32 = 2^5 \text{ means the same as } \log_2 32 = 5.$$

In general,

$$a = b^x \quad \Leftrightarrow \quad \log_b a = x.$$

This rule defines a *discrete logarithm* in *any group*.

- In $(\mathbb{Z}_7, +)$, $2^5 = 3$ so $\log_2 3 = 5$.
- In $(\mathbb{Z}_7^*, \times)$, $2^5 = 4$ so $\log_2 4 = 5$.
- In $(\mathbb{Z}, +)$, $2^5 = 10$ so $\log_2 10 = 5$.

Note: In $(\mathbb{Z}, +)$, $\log_2 10$ asks: how many times do you have to add 2 to itself to get 10?

Discrete logarithms

- Exponentiation does repeated multiplication eg $2^5 = 32$
- Logarithm asks: *what power of 2 gives you 32?*
  - 5. So $\log_2 32 = 5$.

$$32 = 2^5 \text{ means the same as } \log_2 32 = 5.$$

In general,

$$a = b^x \quad \Leftrightarrow \quad \log_b a = x.$$

This rule defines a *discrete logarithm* in *any group*.

- In $(\mathbb{Z}_7, +)$, $2^5 = 3$ so $\log_2 3 = 5$.
- In $(\mathbb{Z}_7^*, \times)$, $2^5 = 4$ so $\log_2 4 = 5$.
- In $(\mathbb{Z}, +)$, $2^5 = 10$ so $\log_2 10 = 5$.

Note: In $(\mathbb{Z}, +)$, $\log_2 10$ asks: how many times do you have to add 2 to itself to get 10?

- Discrete logarithm in $\mathbb{Z}$ is also known as...

Discrete logarithms

- Exponentiation does repeated multiplication eg $2^5 = 32$
- Logarithm asks: *what power of 2 gives you 32?*
  - 5. So $\log_2 32 = 5$.

$$32 = 2^5 \text{ means the same as } \log_2 32 = 5.$$

In general,

$$a = b^x \quad \Leftrightarrow \quad \log_b a = x.$$

This rule defines a *discrete logarithm* in *any group*.

- In $(\mathbb{Z}_7, +)$, $2^5 = 3$ so $\log_2 3 = 5$.
- In $(\mathbb{Z}_7^*, \times)$, $2^5 = 4$ so $\log_2 4 = 5$.
- In $(\mathbb{Z}, +)$, $2^5 = 10$ so $\log_2 10 = 5$.

Note: In $(\mathbb{Z}, +)$, $\log_2 10$ asks: how many times do you have to add 2 to itself to get 10?

- Discrete logarithm in $\mathbb{Z}$ is also known as... *division*.

Discrete logarithms and cryptography

Many cryptographic algorithms are based on the idea that

discrete logarithms are hard to compute in $(\mathbb{Z}_p^*, \times)$ *when p is large.*

Discrete logarithms and cryptography

Many cryptographic algorithms are based on the idea that

discrete logarithms are hard to compute in $(\mathbb{Z}_p^*, \times)$ *when p is large.*

- It's easier to compute $3^5 \bmod 7$ than it is to compute $\log_3 5$

Discrete logarithms and cryptography

Many cryptographic algorithms are based on the idea that

discrete logarithms are hard to compute in $(\mathbb{Z}_p^*, \times)$ *when p is large.*

- It's easier to compute $3^5 \bmod 7$ than it is to compute $\log_3 5$

Cryptographic algorithms:

- Encryption and decryption
- Authentication
- Key exchange / establishment

Discrete logarithms and cryptography

Many cryptographic algorithms are based on the idea that

discrete logarithms are hard to compute in $(\mathbb{Z}_p^*, \times)$ *when p is large.*

- It's easier to compute $3^5 \bmod 7$ than it is to compute $\log_3 5$

Cryptographic algorithms:

- Encryption and decryption
- Authentication
- Key exchange / establishment

Key exchange

Two people (Alice and Bob) want to communicate securely.

Key exchange

Two people (Alice and Bob) want to communicate securely.

- A and B have no knowledge of each other.
- A and B can only communicate over a public channel.

Key exchange

Two people (Alice and Bob) want to communicate securely.

- A and B have no knowledge of each other.
- A and B can only communicate over a public channel.
- If A and B can establish a *shared secret*, which they both know but nobody else knows, they can use it to as a *key* to encrypt their communications.

Key exchange

Two people (Alice and Bob) want to communicate securely.

- A and B have no knowledge of each other.
- A and B can only communicate over a public channel.
- If A and B can establish a *shared secret*, which they both know but nobody else knows, they can use it to as a *key* to encrypt their communications.
- The algorithm used will also be public.

Key exchange

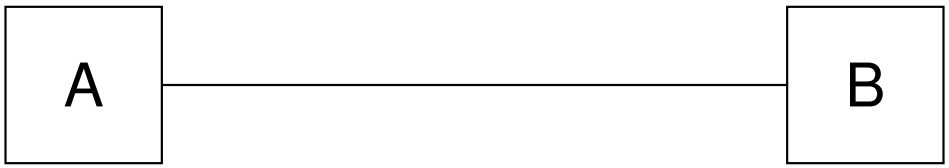
Two people (Alice and Bob) want to communicate securely.

- A and B have no knowledge of each other.
- A and B can only communicate over a public channel.
- If A and B can establish a *shared secret*, which they both know but nobody else knows, they can use it to as a *key* to encrypt their communications.
- The algorithm used will also be public.

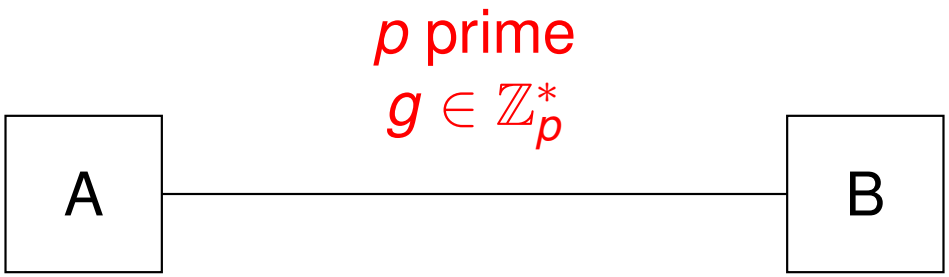
Question

Despite such public conditions, can A and B establish a shared secret?

Diffie-Hellman key exchange

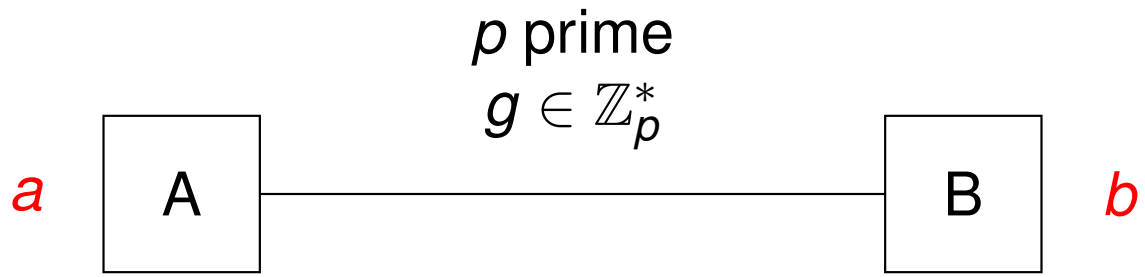


Diffie-Hellman key exchange



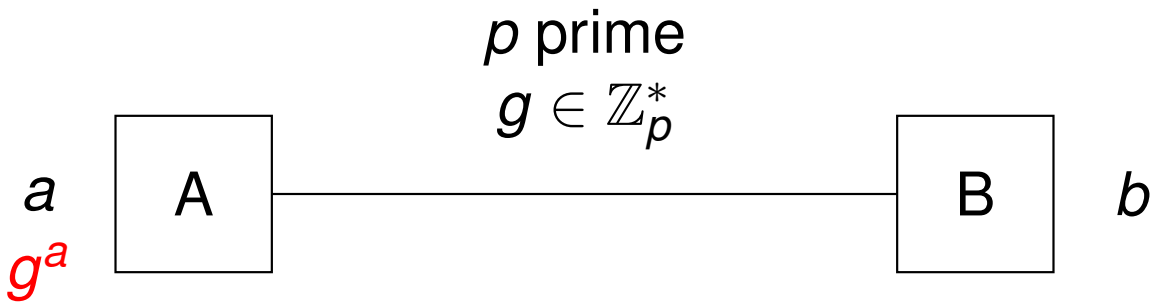
1. A and B agree on a large prime p, and a $g \in \mathbb{Z}_p^*$.
   - Both p and g are publicly known.

Diffie-Hellman key exchange



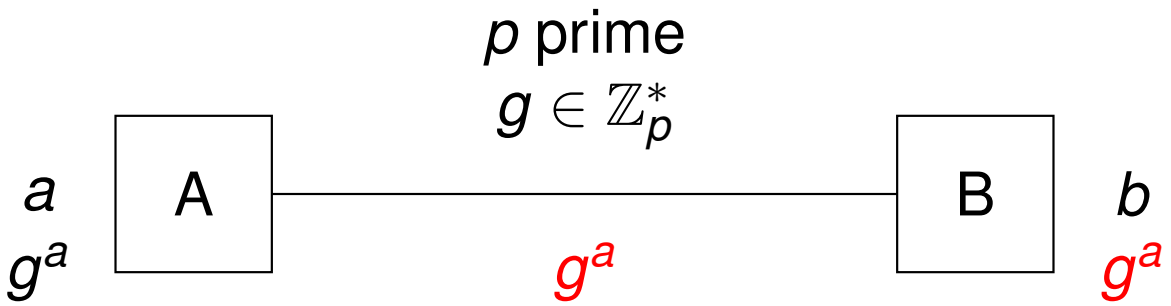
1. A and B agree on a large prime p, and a $g \in \mathbb{Z}_p^*$.
   - Both p and g are publicly known.
2. A and B choose secret numbers a, b at random.

Diffie-Hellman key exchange



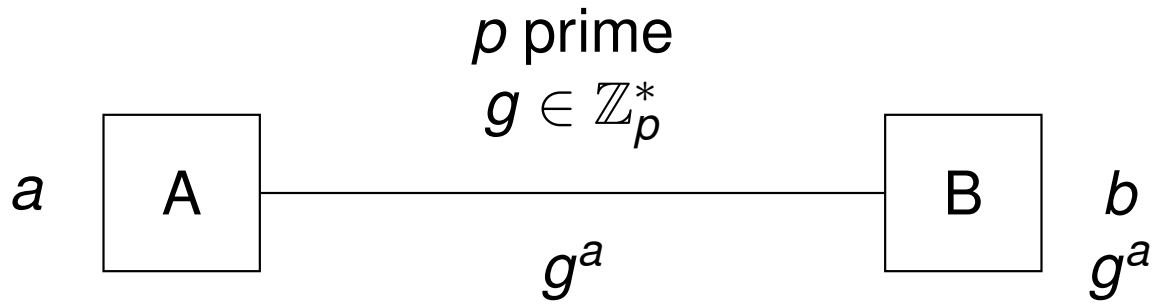
1. A and B agree on a large prime p, and a $g \in \mathbb{Z}_p^*$.
   - Both p and g are publicly known.
2. A and B choose secret numbers a, b at random.
3. A calculates $g^a \pmod{p}$ and sends it to B.

Diffie-Hellman key exchange



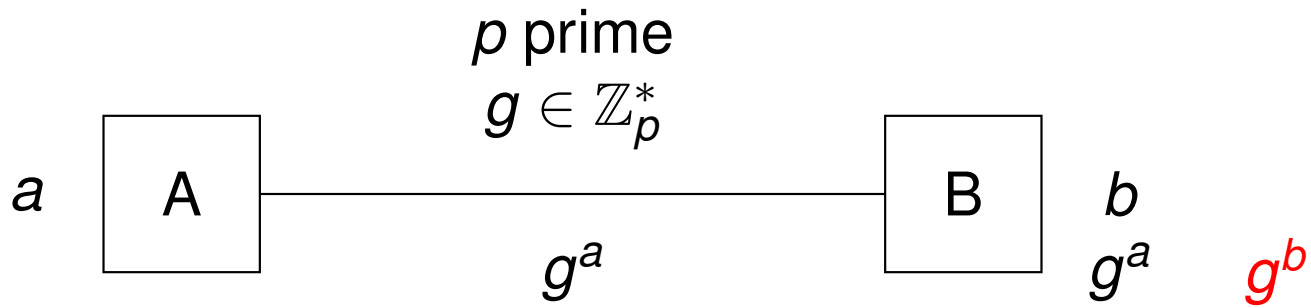
1. A and B agree on a large prime p, and a $g \in \mathbb{Z}_p^*$.
   - Both p and g are publicly known.
2. A and B choose secret numbers a, b at random.
3. A calculates $g^a \pmod p$ and sends it to B.

Diffie-Hellman key exchange



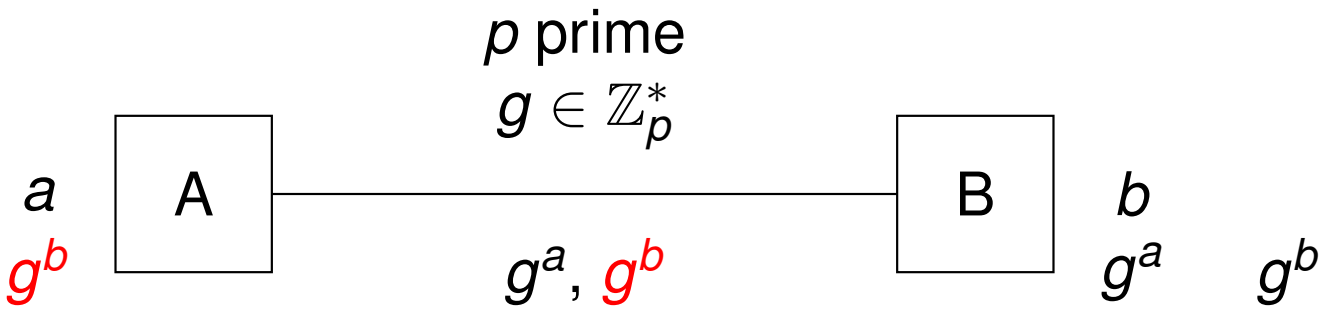
1. A and B agree on a large prime p, and a $g \in \mathbb{Z}_p^*$.
   - Both p and g are publicly known.
2. A and B choose secret numbers a, b at random.
3. A calculates $g^a \pmod{p}$ and sends it to B.

Diffie-Hellman key exchange



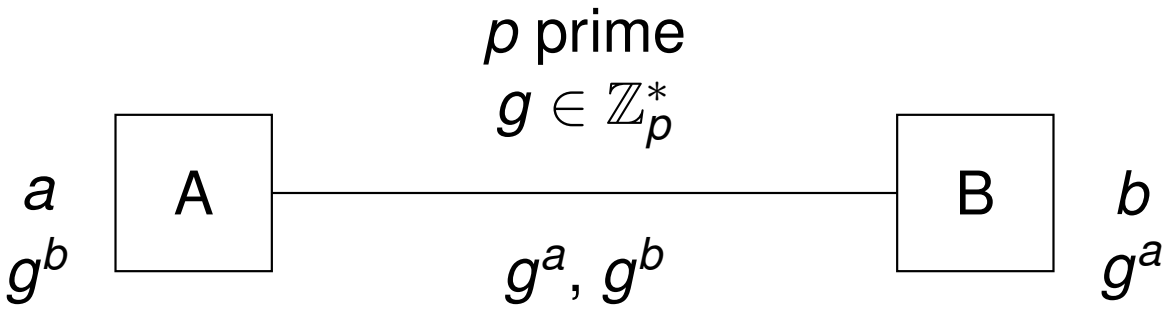
1. A and B agree on a large prime p, and a $g \in \mathbb{Z}_p^*$.
   - Both p and g are publicly known.
2. A and B choose secret numbers a, b at random.
3. A calculates $g^a \pmod p$ and sends it to B.
   B calculates $g^b \pmod p$ and sends it to A.

Diffie-Hellman key exchange



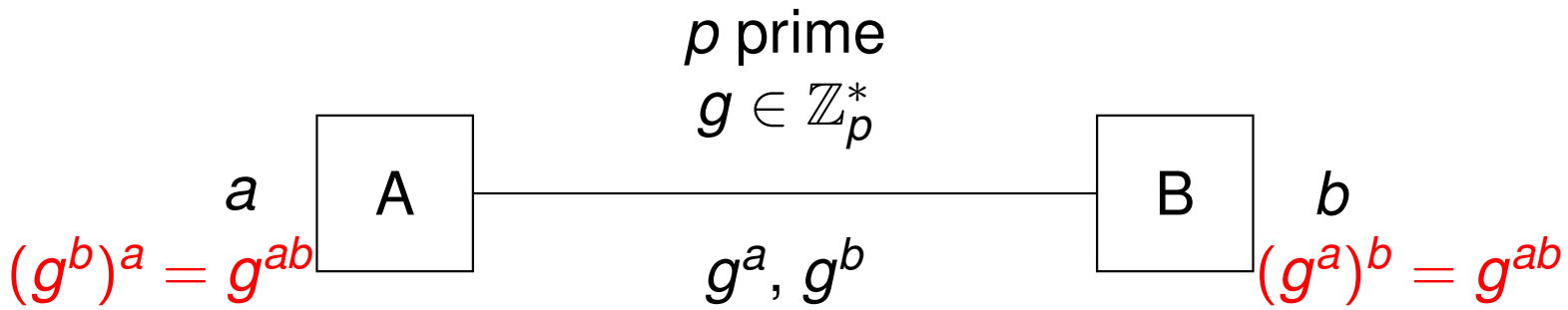
1. A and B agree on a large prime p, and a $g \in \mathbb{Z}_p^*$.
   - Both p and g are publicly known.
2. A and B choose secret numbers a, b at random.
3. A calculates $g^a \pmod p$ and sends it to B.
   B calculates $g^b \pmod p$ and sends it to A.

Diffie-Hellman key exchange



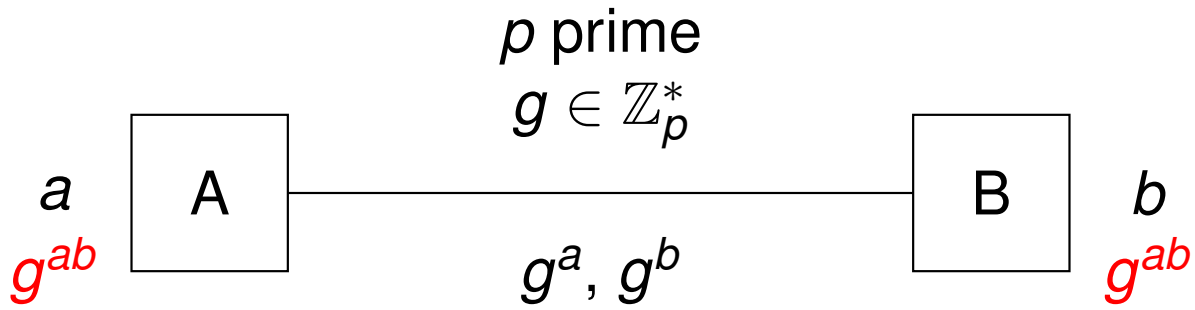
1. A and B agree on a large prime p, and a $g \in \mathbb{Z}_p^*$.
   - Both p and g are publicly known.
2. A and B choose secret numbers a, b at random.
3. A calculates $g^a \pmod p$ and sends it to B.
   B calculates $g^b \pmod p$ and sends it to A.
   - These calculations are “easy" (exponentiation mod p).
   - Now p, g, g^a, g^b are publicly known but a is known only to A and b is known only to B.

Diffie-Hellman key exchange



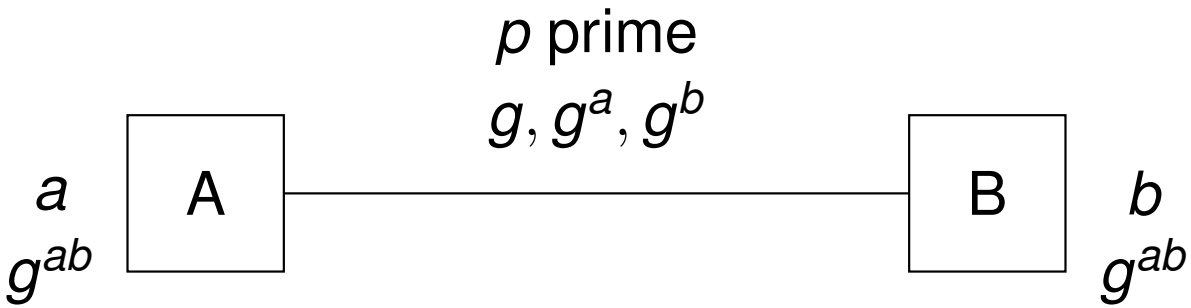
1. A and B agree on a large prime p, and a $g \in \mathbb{Z}_p^*$.
   - Both p and g are publicly known.
2. A and B choose secret numbers a, b at random.
3. A calculates $g^a \pmod p$ and sends it to B.
   B calculates $g^b \pmod p$ and sends it to A.
   - These calculations are “easy" (exponentiation mod p).
   - Now p, g, g^a, g^b are publicly known but a is known only to A and b is known only to B.
4. A calculates $(g^b)^a = g^{ab} \bmod p$.
   B calculates $(g^a)^b = g^{ab} \bmod p$.

Diffie-Hellman key exchange



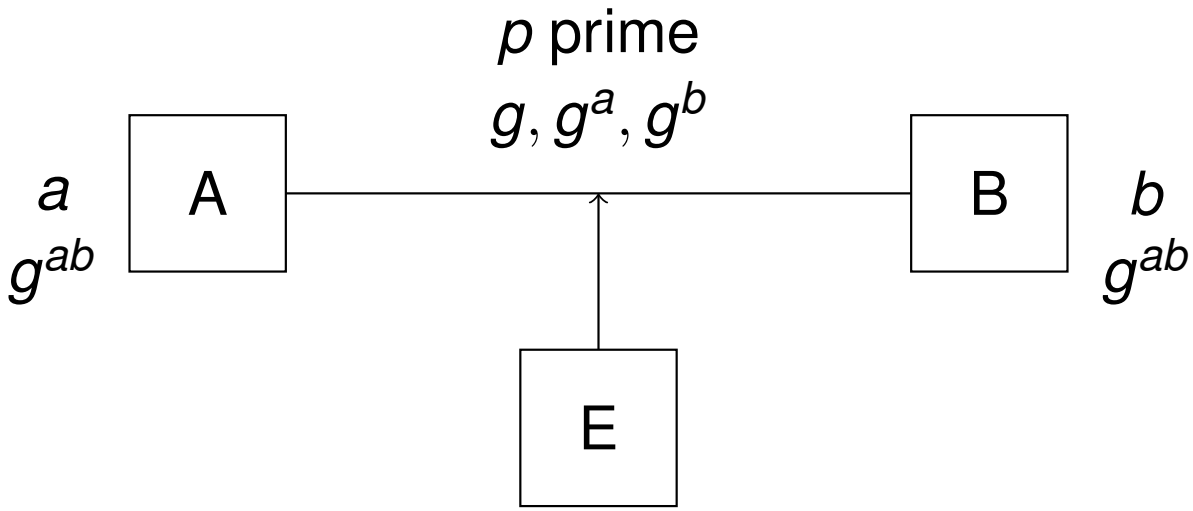
1. A and B agree on a large prime p, and a $g \in \mathbb{Z}_p^*$.
   - Both p and g are publicly known.
2. A and B choose secret numbers a, b at random.
3. A calculates $g^a \pmod p$ and sends it to B.
   B calculates $g^b \pmod p$ and sends it to A.
   - These calculations are “easy" (exponentiation mod p).
   - Now p, g, g^a, g^b are publicly known but a is known only to A and b is known only to B.
4. A calculates $(g^b)^a = g^{ab} \bmod p$.
   B calculates $(g^a)^b = g^{ab} \bmod p$.
   - The number $g^{ab} \pmod p$ is A and B’s *shared secret*.

Diffie-Hellman key exchange



Security of the key exchange:

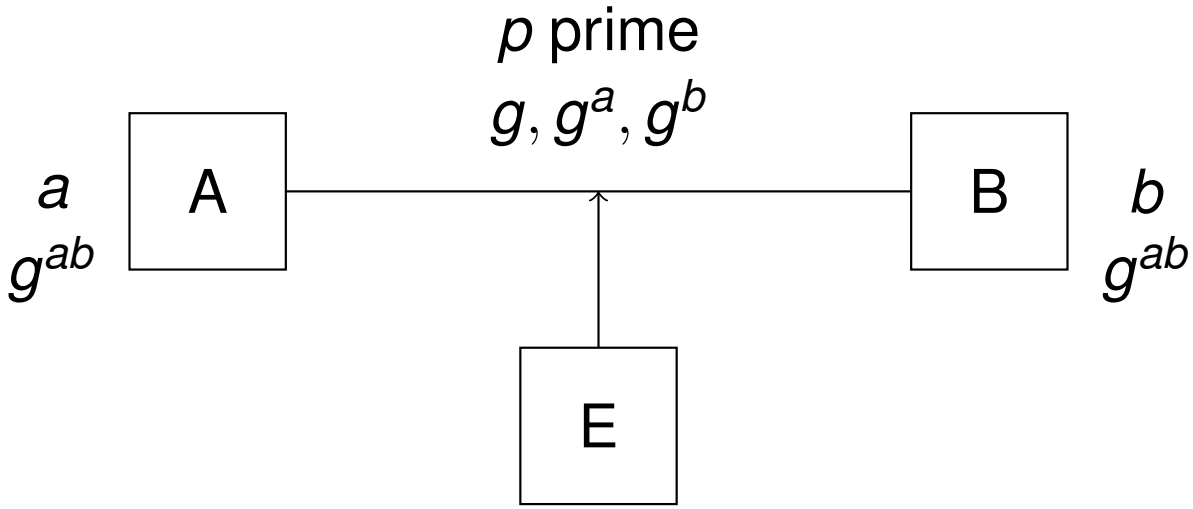
Diffie-Hellman key exchange



Security of the key exchange:

- An eavesdropper Eve must compute shared secret g^{ab} from knowledge of g^a, g^b, p, g only, in order to listen in.

Diffie-Hellman key exchange



Security of the key exchange:

- An eavesdropper Eve must compute shared secret g^{ab} from knowledge of g^a, g^b, p, g only, in order to listen in.
- Finding a or b from g^a, g^b would allow Eve to compute g^{ab}, but this requires finding *discrete logarithms* modulo p.
  - $a = \log_g g^a$, $b = \log_g g^b$

Back to the DSGL

“Cryptography"... based on... An “asymmetric algorithm" where the security of the algorithm is based on any of the following:...

3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in excess of 112 bits [sic]

Back to the DSGL

> “Cryptography"... based on... An “asymmetric algorithm" where the security of the algorithm is based on any of the following:...
>
> 3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in excess of 112 bits [sic]

There is a well-known group “in excess of 112 bits" [sic] where discrete logarithms are simple.

Back to the DSGL

> “Cryptography"... based on... An “asymmetric algorithm" where the security of the algorithm is based on any of the following:...
>
> 3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in excess of 112 bits [sic]

There is a well-known group “in excess of 112 bits" [sic] where discrete logarithms are simple.

- More than $2^{112} = 5{,}192{,}296{,}858{,}534{,}827{,}628{,}530{,}496{,}329{,}220{,}096$ elements.

Back to the DSGL

"Cryptography"... based on... An "asymmetric algorithm" where the security of the algorithm is based on any of the following:...

3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in excess of 112 bits [sic]

There is a well-known group "in excess of 112 bits" [sic] where discrete logarithms are simple.

- More than $2^{112} = 5{,}192{,}296{,}858{,}534{,}827{,}628{,}530{,}496{,}329{,}220{,}096$ elements.

The *integers* $(\mathbb{Z}, +)$!

Back to the DSGL

"Cryptography"... based on... An "asymmetric algorithm" where the security of the algorithm is based on any of the following:...

3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in excess of 112 bits [sic]

There is a well-known group "in excess of 112 bits" [sic] where discrete logarithms are simple.

- More than $2^{112} = 5{,}192{,}296{,}858{,}534{,}827{,}628{,}530{,}496{,}329{,}220{,}096$ elements.

The *integers* $(\mathbb{Z}, +)$!

- Has *infinitely many* elements — far more than 2^{112}!
- Discrete logarithm is just *division*.
  - E.g. $\log_3 18 = 6$.

The BAD algorithm

DSGL s5A002.a.1.b

“Cryptography"... based on... An “asymmetric algorithm" where the security of the algorithm is based on any of the following:...

3. ~~Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in excess of 112 bits~~ Division

The BAD algorithm

DSGL s5A002.a.1.b

"Cryptography"... based on... An "asymmetric algorithm" where the security of the algorithm is based on any of the following:...

3. ~~Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in excess of 112 bits~~ Division

Are there any encryption algorithms based on *division*?

The BAD algorithm

DSGL s5A002.a.1.b

"Cryptography"... based on... An "asymmetric algorithm" where the security of the algorithm is based on any of the following:...

3. ~~Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in excess of 112 bits~~ Division

Are there any encryption algorithms based on *division*?

- Yes!

The BAD algorithm

DSGL s5A002.a.1.b

"Cryptography"... based on... An "asymmetric algorithm" where the security of the algorithm is based on any of the following:...

3. ~~Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in excess of 112 bits~~ Division

Are there any encryption algorithms based on *division*?

- Yes!

(Are there any *good* ones? Not that I know of.)

The BAD algorithm

Dan's Basic Algorithm using Division (BAD)

The BAD algorithm

Dan's Basic Algorithm using Division (BAD)

To encrypt a message:

1. Convert the message to a number m.
2. Choose a *secret encryption key* k.
3. *Multiply* m by k to obtain the *cyphertext* $c = mk$.

The BAD algorithm

Dan's Basic Algorithm using Division (BAD)

To encrypt a message:

1. Convert the message to a number m.
2. Choose a *secret encryption key* k.
3. *Multiply* m by k to obtain the *cyphertext* $c = mk$.

To decrypt a message c:

1. Obtain the *secret decryption key* $\frac{1}{k}$.
2. *Divide* c by k (i.e. multiply by decryption key) to obtain the original message $m = \frac{1}{k}c$.

The BAD algorithm

Dan's Basic Algorithm using Division (BAD)

To encrypt a message:

1. Convert the message to a number m.
2. Choose a *secret encryption key* k.
3. *Multiply* m by k to obtain the *cyphertext* $c = mk$.

To decrypt a message c:

1. Obtain the *secret decryption key* $\frac{1}{k}$.
2. *Divide* c by k (i.e. multiply by decryption key) to obtain the original message $m = \frac{1}{k}c$.

WORST. ALGORITHM. EVER.

The BAD algorithm

But, the BAD algorithm is:

The BAD algorithm

But, the BAD algorithm is:

- A cryptographic algorithm

The BAD algorithm

But, the BAD algorithm is:

- A cryptographic algorithm
- Asymmetric (encryption different from decryption)

The BAD algorithm

But, the BAD algorithm is:

- A cryptographic algorithm
- Asymmetric (encryption different from decryption)
- Security is based on division, i.e. discrete logarithm in a group with more than 2^{112} elements.

The BAD algorithm

But, the BAD algorithm is:

- A cryptographic algorithm
- Asymmetric (encryption different from decryption)
- Security is based on division, i.e. discrete logarithm in a group with more than 2^{112} elements.

Hence (if not public domain or “basic scientific research" etc):

DUAL-USE CIVILIAN-MILITARY ITEM.

The BAD algorithm

But, the BAD algorithm is:

- A cryptographic algorithm
- Asymmetric (encryption different from decryption)
- Security is based on division, i.e. discrete logarithm in a group with more than 2^{112} elements.

Hence (if not public domain or “basic scientific research" etc):

DUAL-USE CIVILIAN-MILITARY ITEM.

- And so is any “system" or “equipment" “designed or modified to use" this algorithm “employing digital techniques"...

The BAD algorithm

But, the BAD algorithm is:

- A cryptographic algorithm
- Asymmetric (encryption different from decryption)
- Security is based on division, i.e. discrete logarithm in a group with more than 2^{112} elements.

Hence (if not public domain or “basic scientific research" etc):

DUAL-USE CIVILIAN-MILITARY ITEM.

- And so is any “system" or “equipment" “designed or modified to use" this algorithm “employing digital techniques"...

Weapons of maths destruction?

Government unlikely to be coming for calculators any time soon...
But...

Weapons of maths destruction?

Government unlikely to be coming for calculators any time soon...
But...

- There are serious issues with these laws.
- These laws affect university education and research directly.
- A small part of broader issues re security, transparency, national security, civil liberties.

Weapons of maths destruction?

Government unlikely to be coming for calculators any time soon...
But...

- There are serious issues with these laws.
- These laws affect university education and research directly.
- A small part of broader issues re security, transparency, national security, civil liberties.
- Laws should be written & implemented by people who understand them.
- Technical knowledge is important in debates on these topics.

Weapons of maths destruction?

Government unlikely to be coming for calculators any time soon...
But...

- There are serious issues with these laws.
- These laws affect university education and research directly.
- A small part of broader issues re security, transparency, national security, civil liberties.
- Laws should be written & implemented by people who understand them.
- Technical knowledge is important in debates on these topics.
- Even if badly written laws are unlikely to be used in bad ways, they *could* be so used.
- We shouldn't have badly written laws in the first place!

History

How did we get here?

- 1990s “crypto wars" over US encryption policy
- US Export controls (ITAR)
- International arms control: Wassenaar Arrangement
- Australian DSGL
- 2007 Australia-US Defence Trade Cooperation Treaty

Conclusion

Finally...

Don’t stop doing mathematics!

THANKS FOR LISTENING.