How to really share a secret

Dr Keith Martin
Information Security Group
Department of Mathematics
Royal Holloway

keith.martin@rhul.ac.uk

Who we are?

Activities at Royal Holloway

The Information Security Group at Royal Holloway:

- Part of the Mathematics Department
- One of the largest academic information security groups in the world with 21 staff, 7 visiting professors, and 48 research students
- Conducts research into areas such as design and analysis of cryptographic protocols, smartcards, electronic commerce, security management, integration of security into applications
- Maintains close links and performs contract research and consulting for leading security companies and security users

The Information Security Group runs an MSc in Information Security.

In 2005:

- 180 students on campus
- 100 e-learning students

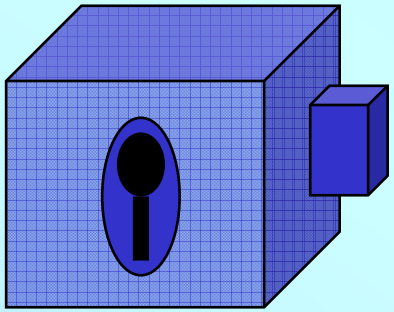
Graduates from these MSc courses are gaining employment as IT security professionals throughout the World in sectors such as finance, telecommunications, computing, etc etc

The Problem

The Bank Safe Problem

10 officials of a bank wish to fix a number of locks onto a safe and then share amongst themselves copies of the various keys to the locks in such a manner that

- any 7 of the officials will have at least one key for every lock
- any 6 of the officials are missing the key to at least one lock



Can this be done?

If so, what is the smallest number of locks needed?

What is the smallest number of keys that each official must carry?

Secret sharing schemes

A **secret sharing scheme** is a way of sharing a **secret** amongst a number of **participants.**

Each participant is given a **share** by a trusted **dealer,** which they must keep private.

These shares are related in such a way that

- the secret can be reconstructed from some shares
- the secret can not be reconstructed from other shares

Threshold Schemes

A **(k,n)-threshold scheme** is a secret sharing scheme defined on n participants, where

- the secret can be reconstructed from any k shares
- the secret can not be reconstructed from any k-1 shares

(n,n)-Threshold Schemes

1 - 11100101000101001000100011101010001010110 1

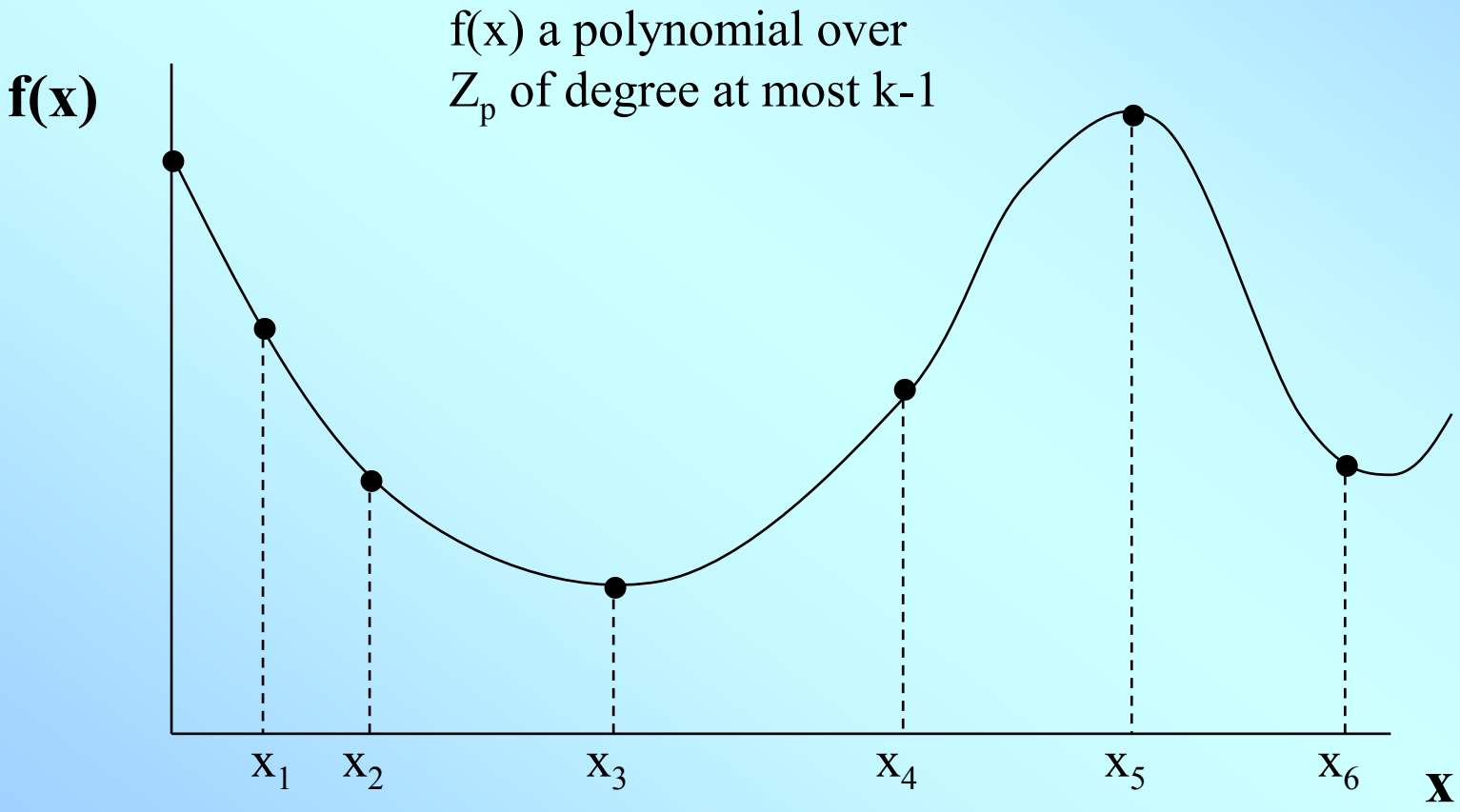
2 - A number between 0 and 99

Perfect Threshold Schemes

A **perfect** (k,n)-threshold scheme is a secret sharing scheme defined on n participants, where

- the secret can be reconstructed from any k shares
- nothing can be learned about the secret by seeing any k-1 shares

Shamir's polynomial threshold scheme

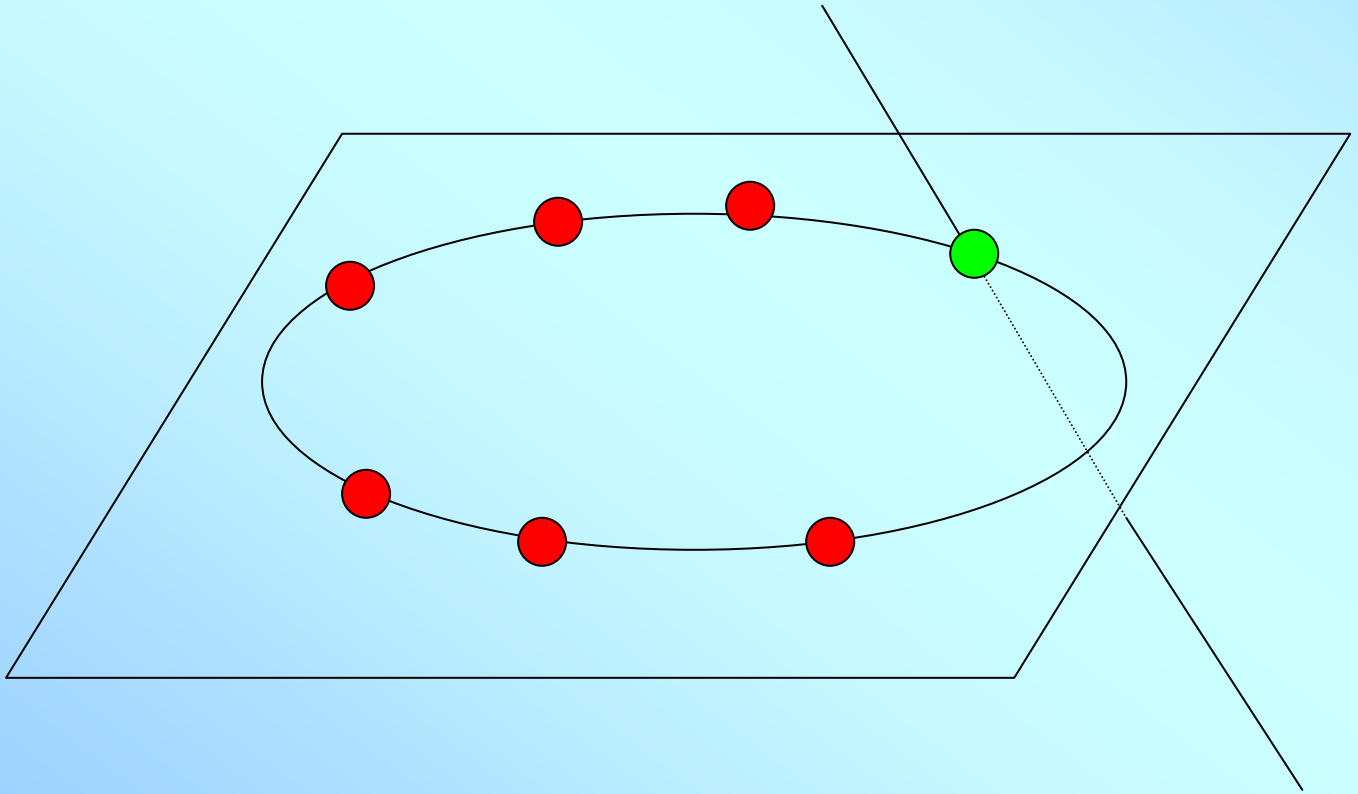


A perfect (2,4)-threshold scheme:

s	0	0	0	0	1	1	1	1	2	2	2	2	3	3	3	3
a	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
b	0	1	2	3	1	0	3	2	2	3	0	1	3	2	1	0
c	0	1	2	3	3	2	1	0	1	0	3	2	2	3	0	1
d	0	1	2	3	2	3	0	1	3	2	1	0	1	0	3	2

Handout 1

Geometrically speaking..



Access Structures

An **access structure** Γ defined on a set of participants **P** is a collection of subsets of **P** such that

if

A belongs to Γ **,** B is a subset of **P,** and A is a subset of B

then

B belongs to Γ**.**

Minimal Sets

Any access structure can be uniquely defined in terms of its minimal sets.

A **minimal set** A for access structure Γ is any set such that:

- A is a member of Γ
- There are no subsets B belonging to Γ that are strictly contained in A

Useful Notation

Example:

If **P = {a,b,c,d}** and

Γ = { {a,b,c}, {a,b,d}, {a,c,d}, {b,c,d}, {a,b,c,d} }

then we write

Γ = abc + abd +acd + bcd

Handout 2

Access Structures on Two Participants

1. ab

Access Structures on Three Participants

1. $ab + ac + bc$
2. abc
3. $ab + ac$

Access Structures on Four Participants

1. ab + ac + bc + ad + bd + cd
2. abc + abd + acd + bcd
3. abcd
4. ab + cd
5. ab + bc + cd
6. ab + ac + ad
7. ab + bc + cd + ad
8. ab + bc + ac + cd
9. ab + ac + ad + bc + bd
10. abc + ad
11. abc + ad + bd
12. abc + ad + bd + cd
13. abc + abd
14. abc + abd + cd
15. abc + abd + acd

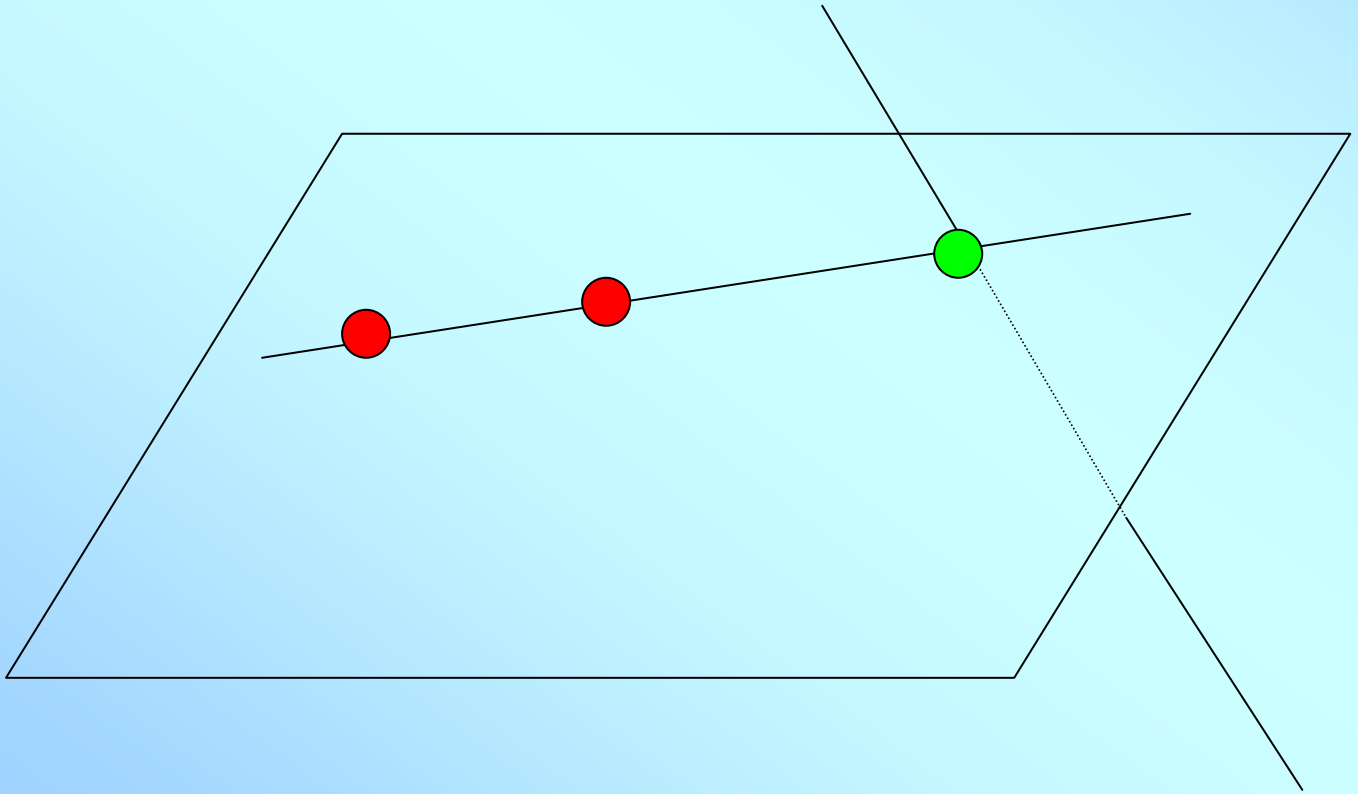
Secret Sharing Schemes

Let Γ be an access structure defined on participant set **P**.

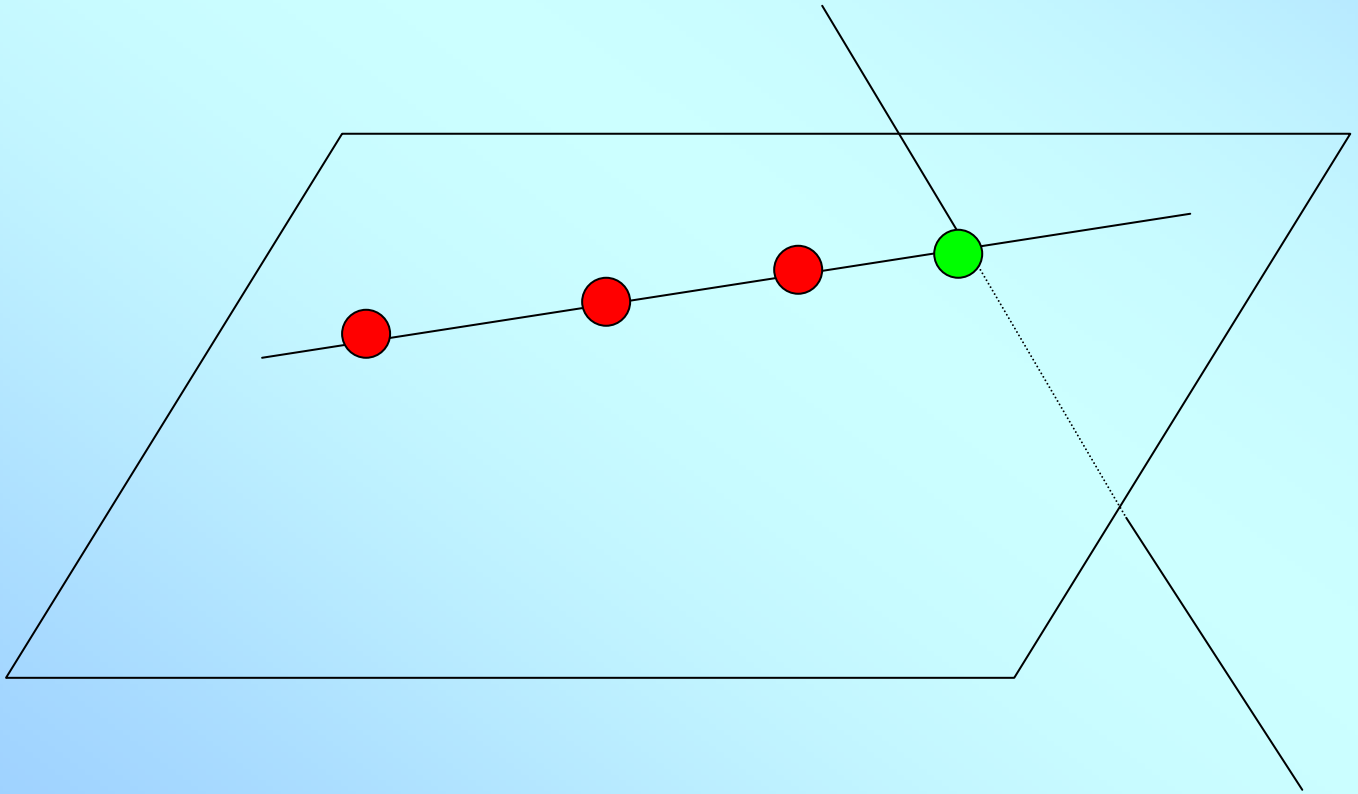
A **perfect secret sharing scheme for** Γ is a secret sharing scheme defined on **P**, where

- the secret can be reconstructed from the shares of any set in Γ
- nothing can be learned about the secret by seeing the shares of any subset of **P** not belonging to Γ.

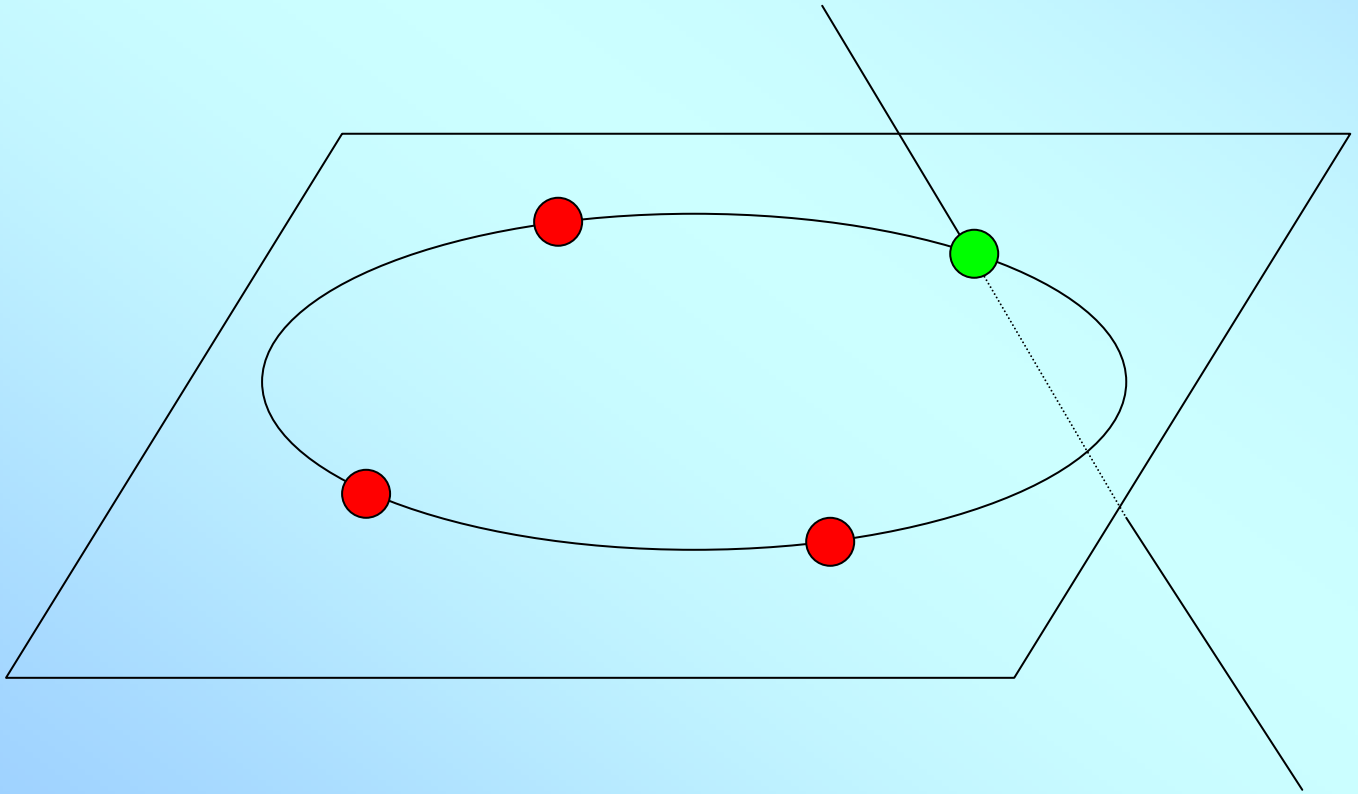
$\Gamma = ab$



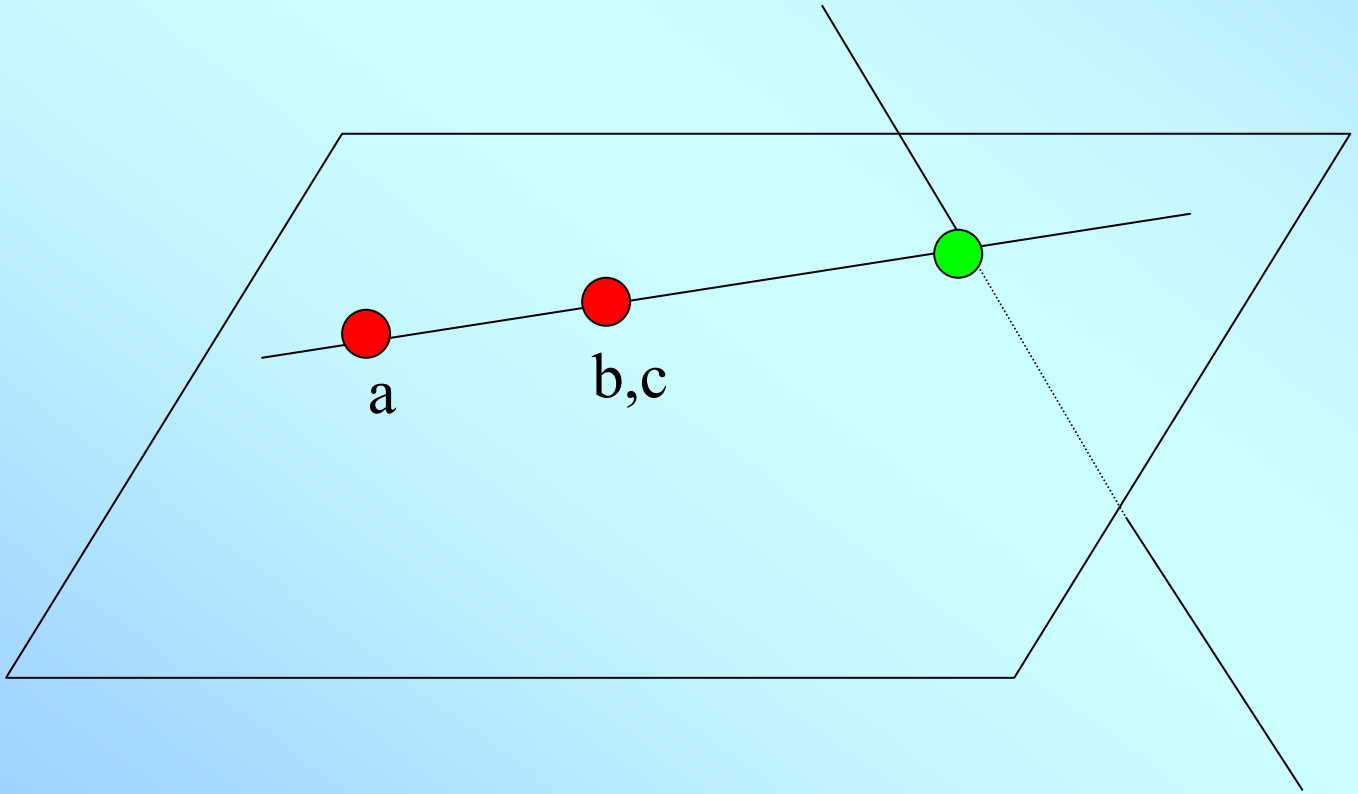
$$\Gamma = ab + ac + bc$$



$\Gamma = abc$

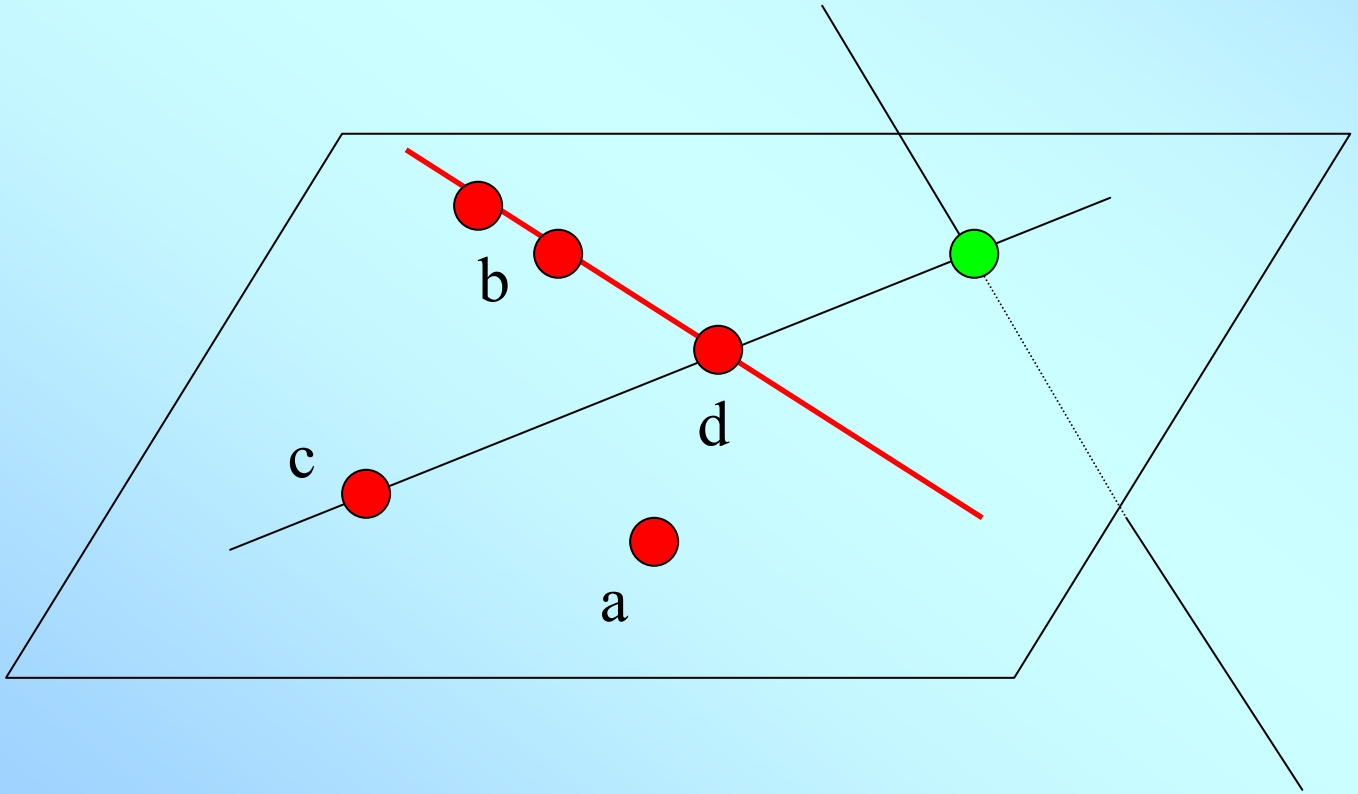


$$\Gamma = ab + ac$$



Handout 3

$$\Gamma = ab + bc + cd \quad (\#5)$$



A general algorithm

Step 1

Associate each **maximal unauthorised** set B in Γ with a key b

Step 2

Give key b to a participant p $\Leftrightarrow$ p does not belong to B

Step 3

To try to reconstruct the secret, a set A gather all the keys that they collectively know

Γ=abc + cd + de

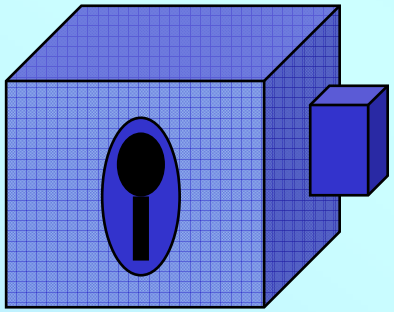
B_1={a,b,d} B_2={a,b,e} B_3={a,c,e} B_4={b,c}

	b_1	b_2	b_3	b_4
a				x
b			x	
c	x	x		
d		x	x	x
e	x			x

The Return of the Bank Safe Problem

10 officials of a bank wish to fix a number of locks onto a safe and then share amongst themselves copies of the various keys to the locks in such a manner that

- any 7 of the officials will have at least one key for every lock
- any 6 of the officials are missing the key to at least one lock



Can this be done?

If so, what is the smallest number of locks needed?

What is the smallest number of keys that each official must carry?

The Bank Safe Solution

- Yes it can be done!

- The smallest number of locks is $\binom{10}{6} = 210$

- The smallest number of keys that each official must carry is

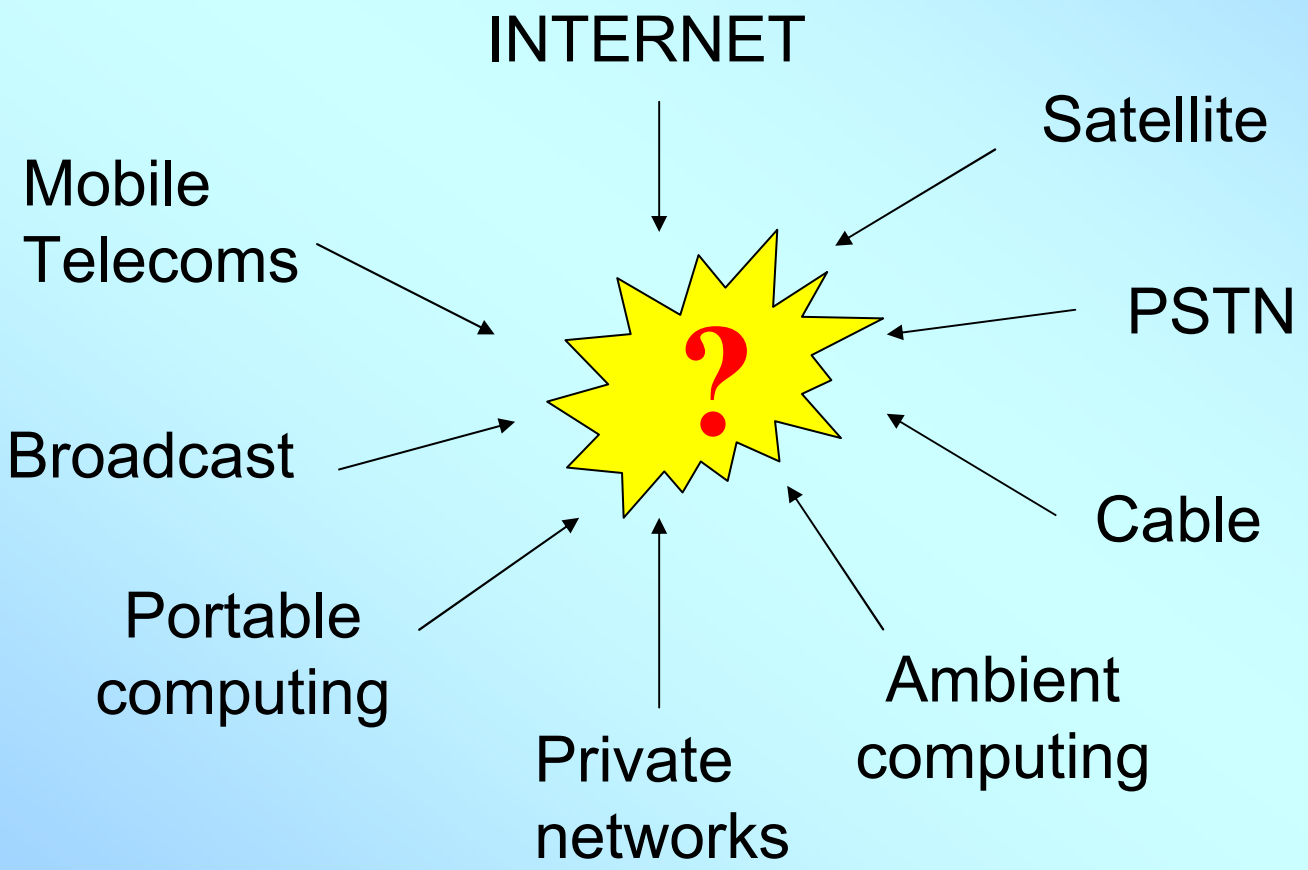
$$\binom{9}{6} = 84$$

Application

Agree or disagree ?

I have taken part in online commerce

Why is this increasingly important?



Agree or disagree ?

It is safe to buy goods over the Internet

A matter of trust

Five issues that lead to lack of confidence in online commerce:

- **Fraud** - abuse or misuse of data
- **Privacy** - the mechanism by which users contain control over their own data
- **Content** - access to material, intellectual property rights
- **Liability** - the legal framework
- **Redress** - resolution of disputes

Fraud

Is the seller authentic?

Will my payment be safe?

Is the buyer genuine?

Will I get my money?

Privacy

Can I be protected from spam?

Are my personal details safe?

Can I use information gathered for marketing purposes?

Content

Can I control access to illegal/immoral material?

Will my intellectual property rights be infringed?

Liability

Can the contract I am entering into be enforced?

Can the contract I am entering into be enforced?

Redress

Is there a clear means of resolving disputes about our transactions?

Three key services

Confidentiality - to ensure that data cannot be read by anyone other than the intended recipients

Integrity - to ensure that data has not been accidentally or deliberately corrupted

Authentication - to ensure that the originator or recipient of material is the person they claim to be

Cryptography

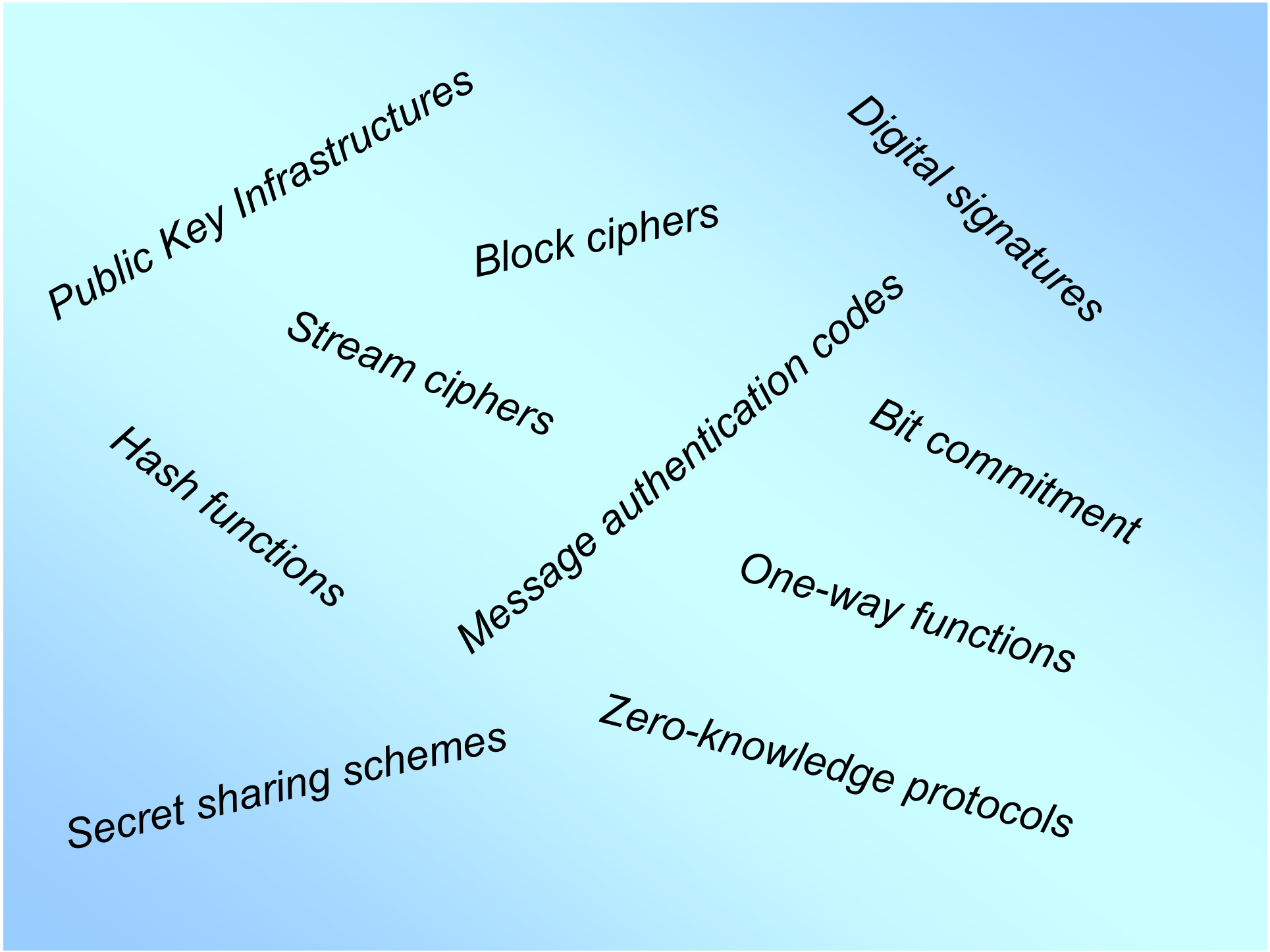
Cryptography is ….

"*the art of secret writing*"

"***the miraculous cure that will solve all computer security problems***"

"*the recognised means of providing integrity, authentication and confidentiality services in an electronic environment* "

"***These days almost all cryptologists are also theoretical mathematicians - they have to be***"


Public Key Infrastructures
Block ciphers
Digital signatures
Stream ciphers
Message authentication codes
Bit commitment
Hash functions
One-way functions
Secret sharing schemes
Zero-knowledge protocols

Confidentiality

Key *k(E)*

Key *k(D)*

message
m

Enciphering Algorithm

cryptogram
c

Deciphering Algorithm

message
m

Interceptor

$c = f(m, k(E))$

$m = g(c, k(D))$

Does
anyone have
any questions?

References

- Fred Piper and Sean Murphy: Cryptography – A very short introduction, Oxford University Press (2002)
- Simon Singh, The Code Book, Fourth Estate (2000)
- Simon Singh, The Code Book for Young People: How to Make it, Break it, Hack it, Crack it, Delacorte Press (2002)
- http://www.isg.rhul.ac.uk/msc/teaching/ic2/ic2resources.shtml
- http://www.simonsingh.net/Crypto_Corner.html