

# THE FUTURE OF COMPUTER SECURITY

Richard Harvey



**GRESHAM**  
COLLEGE

# THE FUTURE OF COMPUTER SECURITY

Richard Harvey

IT Livery Company Professor of Information  
Technology, Gresham College



**GRESHAM**

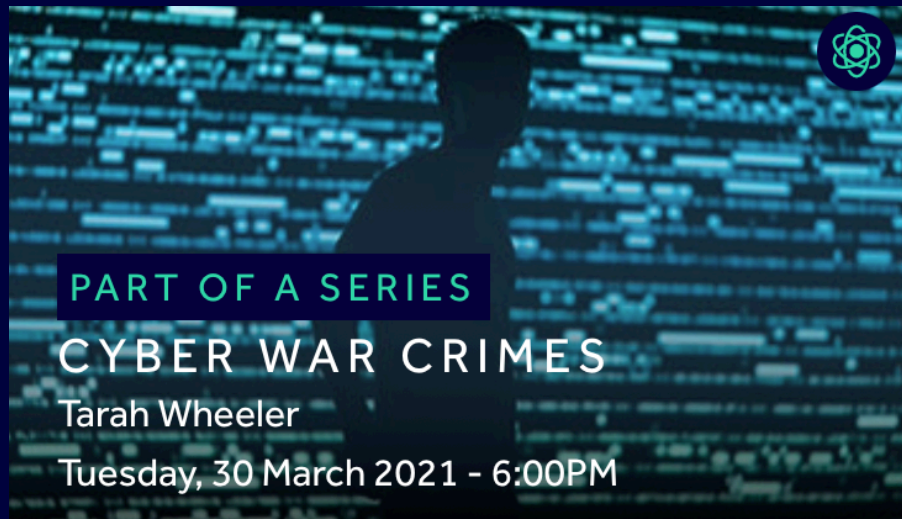
**COLLEGE**

UEA


[www.prof-richard.org](http://www.prof-richard.org)



# Gresham recap



**PART OF A SERIES**  
**CYBER WAR CRIMES**  
Tarah Wheeler  
Tuesday, 30 March 2021 - 6:00PM



**PART OF A SERIES**  
**COMPUTERS AND THE FUTURE**  
Professor Martyn Thomas CBE  
Tuesday, 12 June 2018 - 6:00PM



**PART OF A SERIES**  
**SHOULD WE TRUST COMPUTERS?**  
Professor Martyn Thomas CBE  
Tuesday, 20 October 2015 - 6:00PM



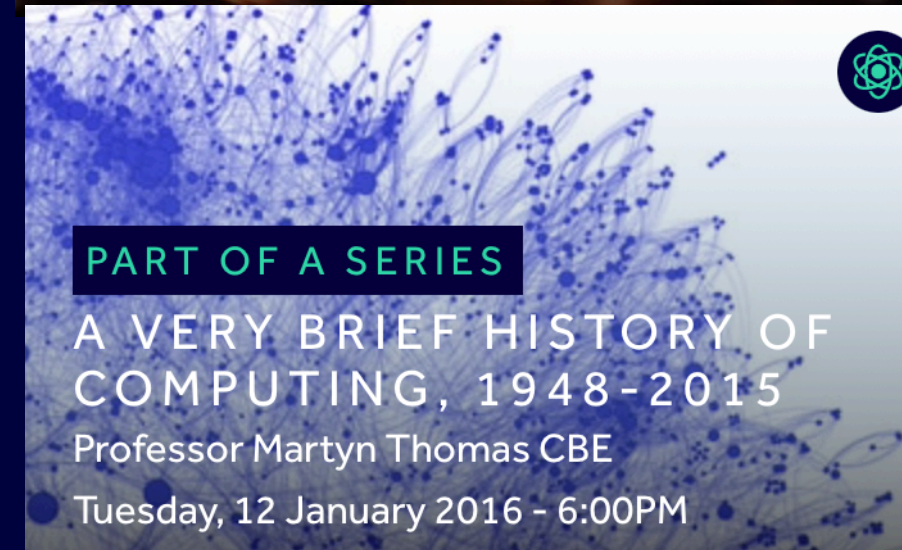
**PART OF A SERIES**  
**CYBERSECURITY**  
Professor Martyn Thomas CBE  
Tuesday, 3 May 2016 - 6:00PM



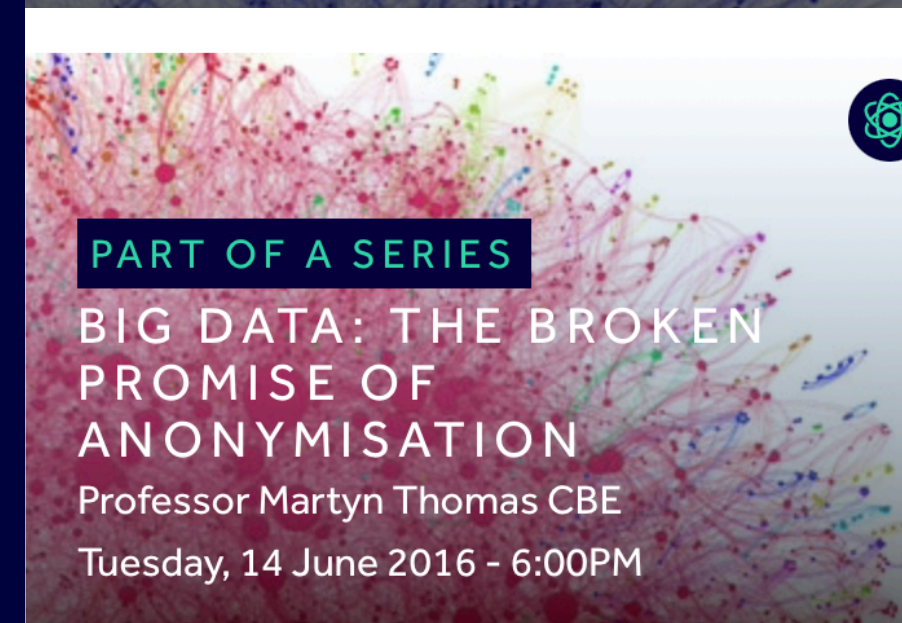
**PART OF A SERIES**  
**MAKING SOFTWARE 'CORRECT BY CONSTRUCTION'**  
Professor Martyn Thomas CBE  
Tuesday, 2 May 2017 - 6:00PM



**PART OF A SERIES**  
**WILL BITCOIN AND THE BLOCK CHAIN CHANGE THE WAY WE LIVE AND WORK?**  
Professor Martyn Thomas CBE  
Tuesday, 9 January 2018 - 6:00PM



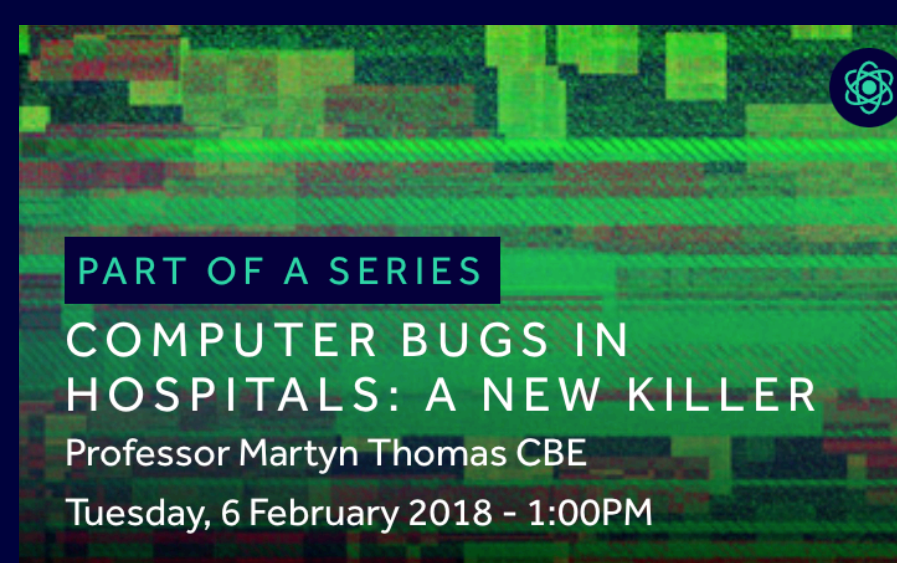
**PART OF A SERIES**  
**A VERY BRIEF HISTORY OF COMPUTING, 1948-2015**  
Professor Martyn Thomas CBE  
Tuesday, 12 January 2016 - 6:00PM



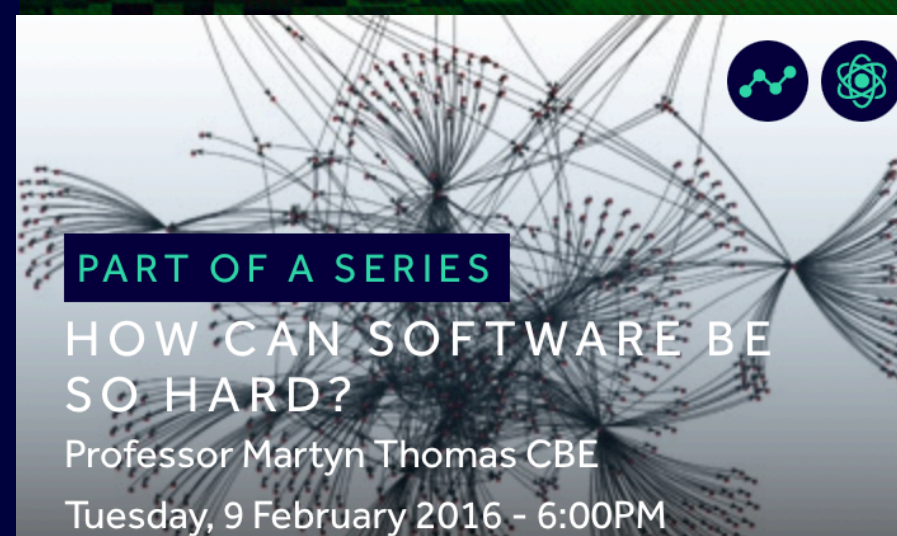
**PART OF A SERIES**  
**BIG DATA: THE BROKEN PROMISE OF ANONYMISATION**  
Professor Martyn Thomas CBE  
Tuesday, 14 June 2016 - 6:00PM



**PART OF A SERIES**  
**COMPUTERS AND WARFARE**  
Professor Martyn Thomas CBE  
Tuesday, 29 May 2018 - 6:00PM



**PART OF A SERIES**  
**COMPUTER BUGS IN HOSPITALS: A NEW KILLER**  
Professor Martyn Thomas CBE  
Tuesday, 6 February 2018 - 1:00PM



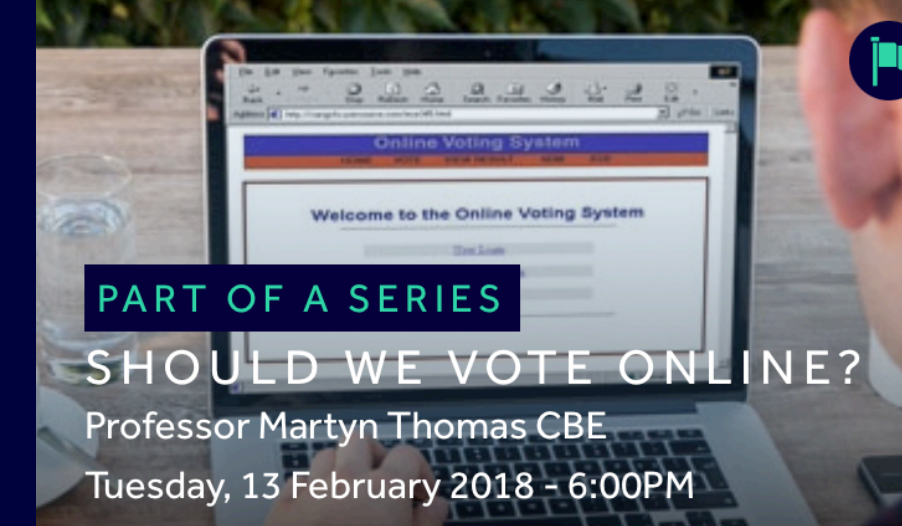
**PART OF A SERIES**  
**HOW CAN SOFTWARE BE SO HARD?**  
Professor Martyn Thomas CBE  
Tuesday, 9 February 2016 - 6:00PM



**PART OF A SERIES**  
**ARE YOU THE CUSTOMER OR THE PRODUCT?**  
Professor Martyn Thomas CBE  
Tuesday, 18 October 2016 - 6:00PM



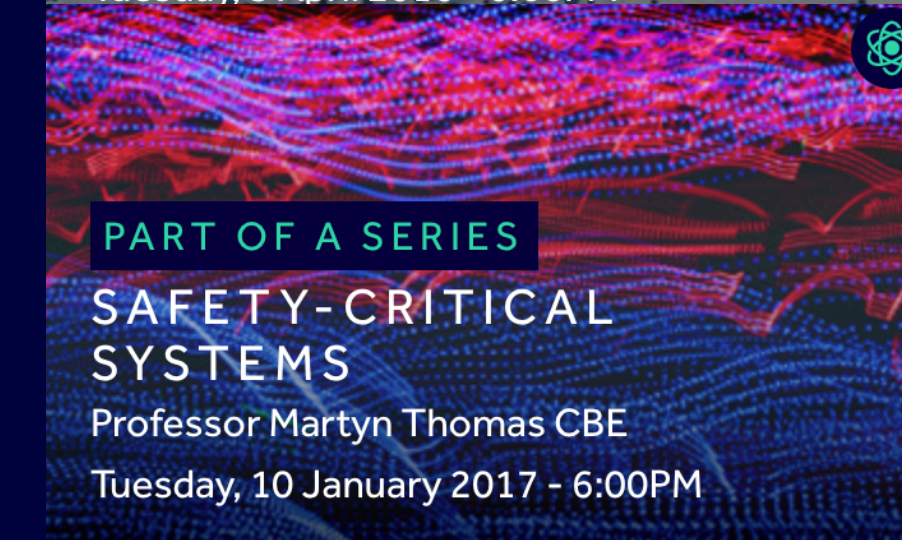
**PART OF A SERIES**  
**THE INTERNET OF THINGS**  
Professor Martyn Thomas CBE  
Tuesday, 20 March 2018 - 6:00PM



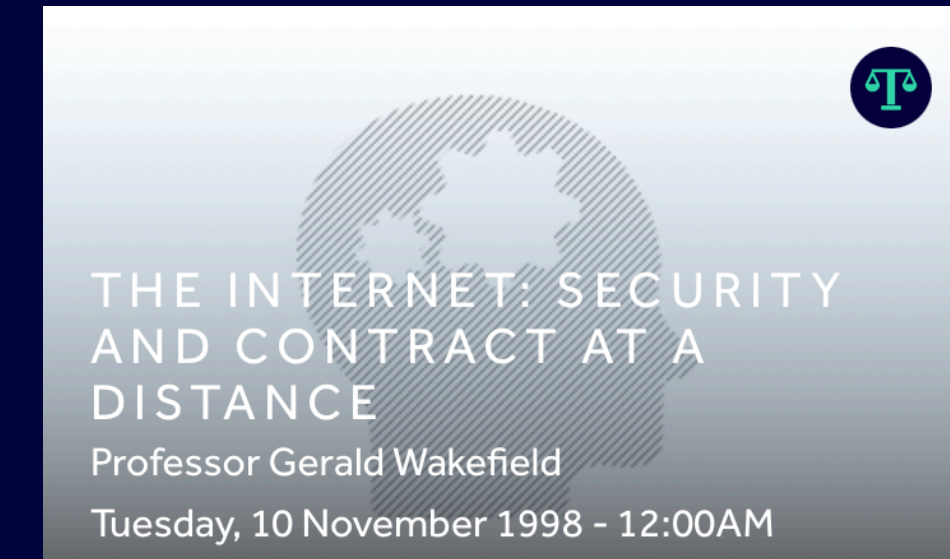
**PART OF A SERIES**  
**SHOULD WE VOTE ONLINE?**  
Professor Martyn Thomas CBE  
Tuesday, 13 February 2018 - 6:00PM



**PART OF A SERIES**  
**COMPUTERS, PEOPLE AND THE REAL WORLD**  
Professor Martyn Thomas CBE  
Tuesday, 5 April 2016 - 6:00PM



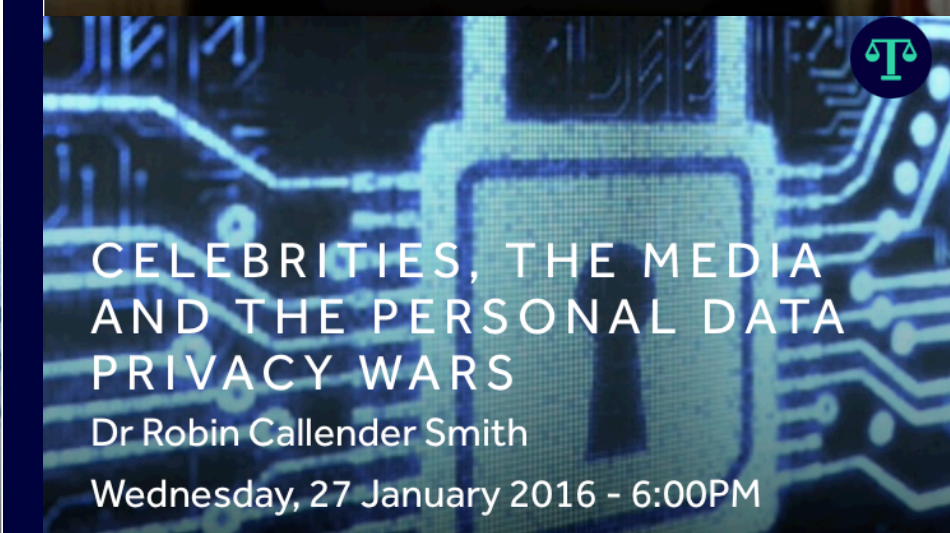
**PART OF A SERIES**  
**SAFETY-CRITICAL SYSTEMS**  
Professor Martyn Thomas CBE  
Tuesday, 10 January 2017 - 6:00PM



**THE INTERNET: SECURITY AND CONTRACT AT A DISTANCE**  
Professor Gerald Wakefield  
Tuesday, 10 November 1998 - 12:00AM



**RECENT LAW REFORMS AND IT**  
Richard Susskind  
Monday, 23 April 2001 - 12:00AM



**CELEBRITIES, THE MEDIA AND THE PERSONAL DATA PRIVACY WARS**  
Dr Robin Callender Smith  
Wednesday, 27 January 2016 - 6:00PM



**PART OF A SERIES**  
**THE DILEMMAS OF PRIVACY AND SURVEILLANCE**  
Professor Martyn Thomas CBE  
Tuesday, 7 February 2017 - 6:00PM



# Recap

Developers make mistakes

 Baddies exploit those mistakes

 Goodies, trying to stop other baddies, exploit these mistakes

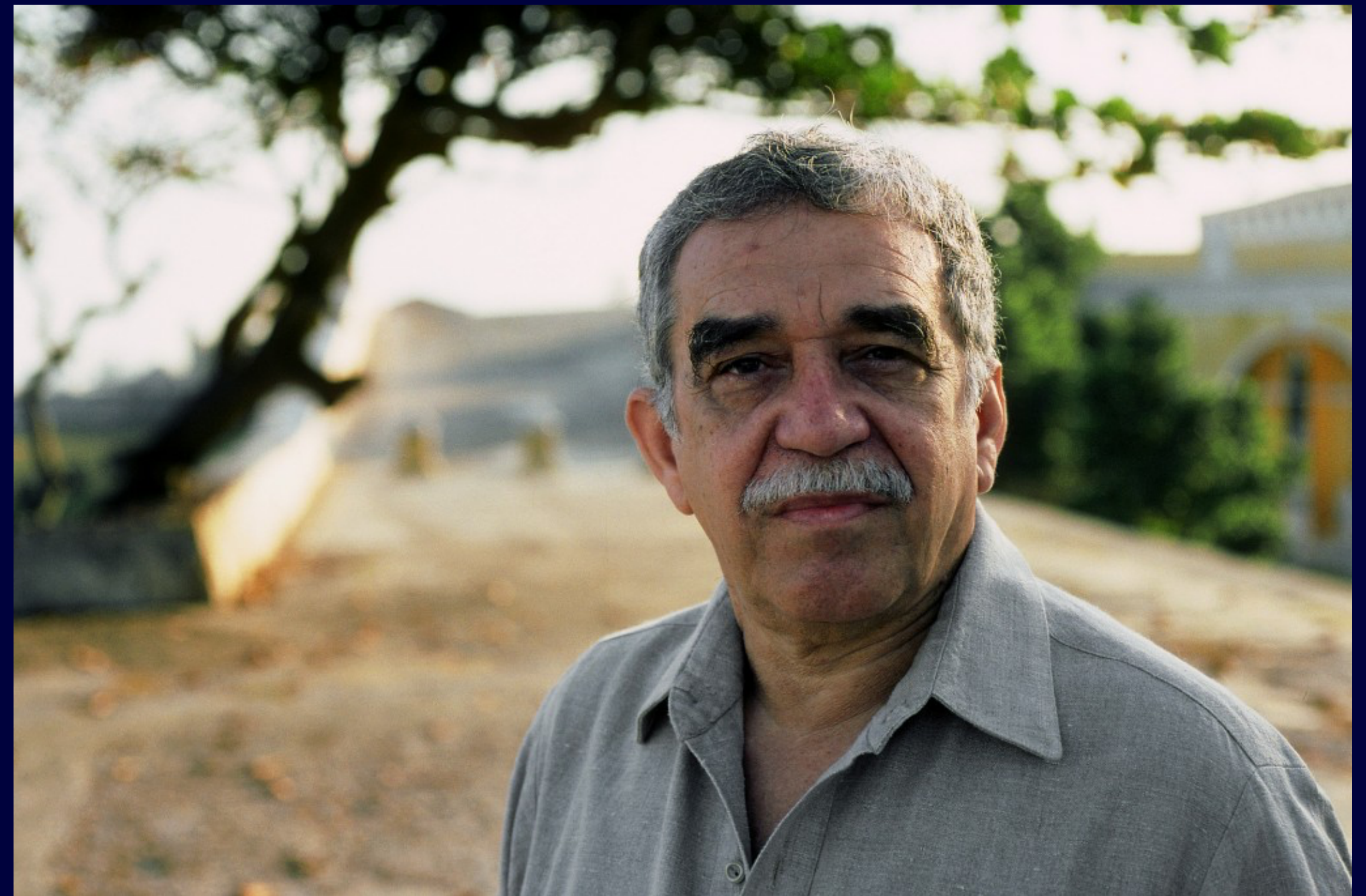
It's all getting out of hand and innocent people are dying

 Root cause:  
the internet uses unencrypted packets



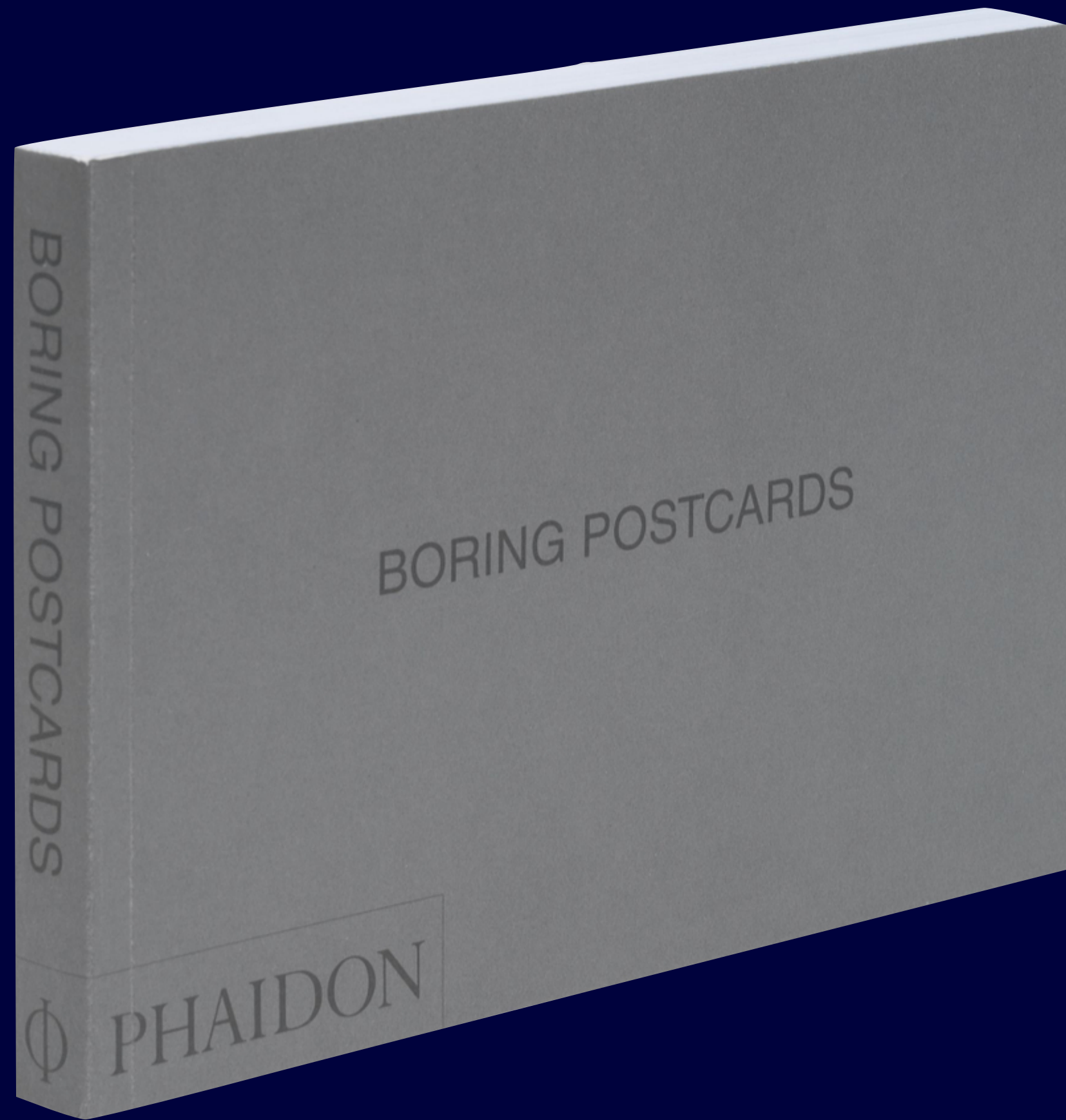
# What this lecture is not about.

“Everyone has three lives:  
a public life, a private life  
and a secret life.”





**If there was only one form of  
communication...**





# Four danger factors

1. Internet packets are open
2. Internet laws do not mirror in-person laws
3. People are disinhibited on the internet
4. Birds of a feather can easily flock together



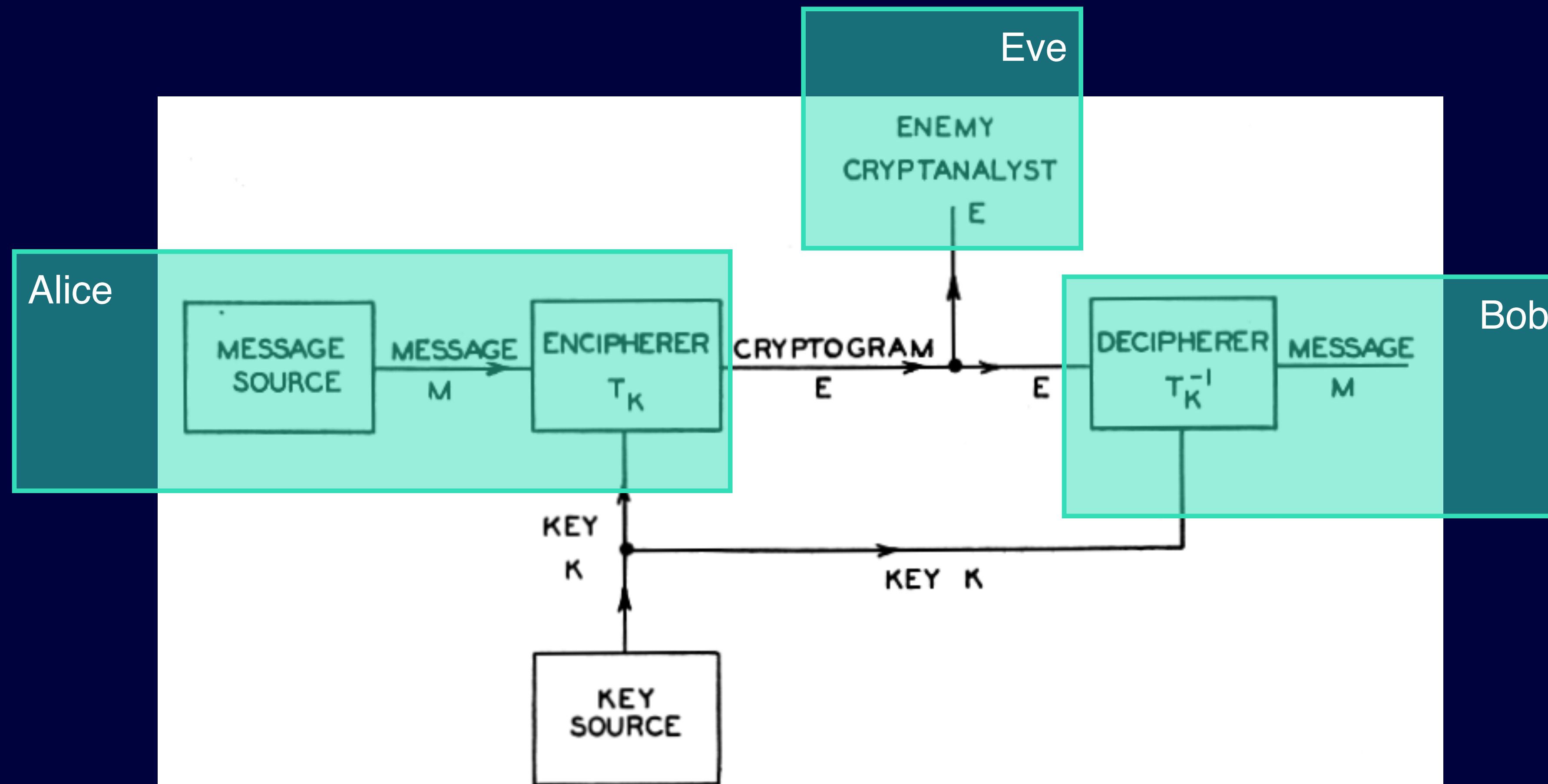


Fig. 1—Schematic of a general secrecy system.



# Diffie Hellman Merkle Key Exchange

Basic idea:

Publicise two numbers,  $G$ , and,  $p$ , and use the following equation to compute public number,  $K$ :

$$G^{key} \bmod p = K$$

What does this mean?



# Modulo arithmetic

Let's choose a base,  $G = 5$

$G^1 = 5$ ;  $G^2 = 25$ ;  $G^3 = 125$ ;  $G^4 = 625 \dots$

Now what if we use *modulo* arithmetic, let's choose  $p = 23$ .

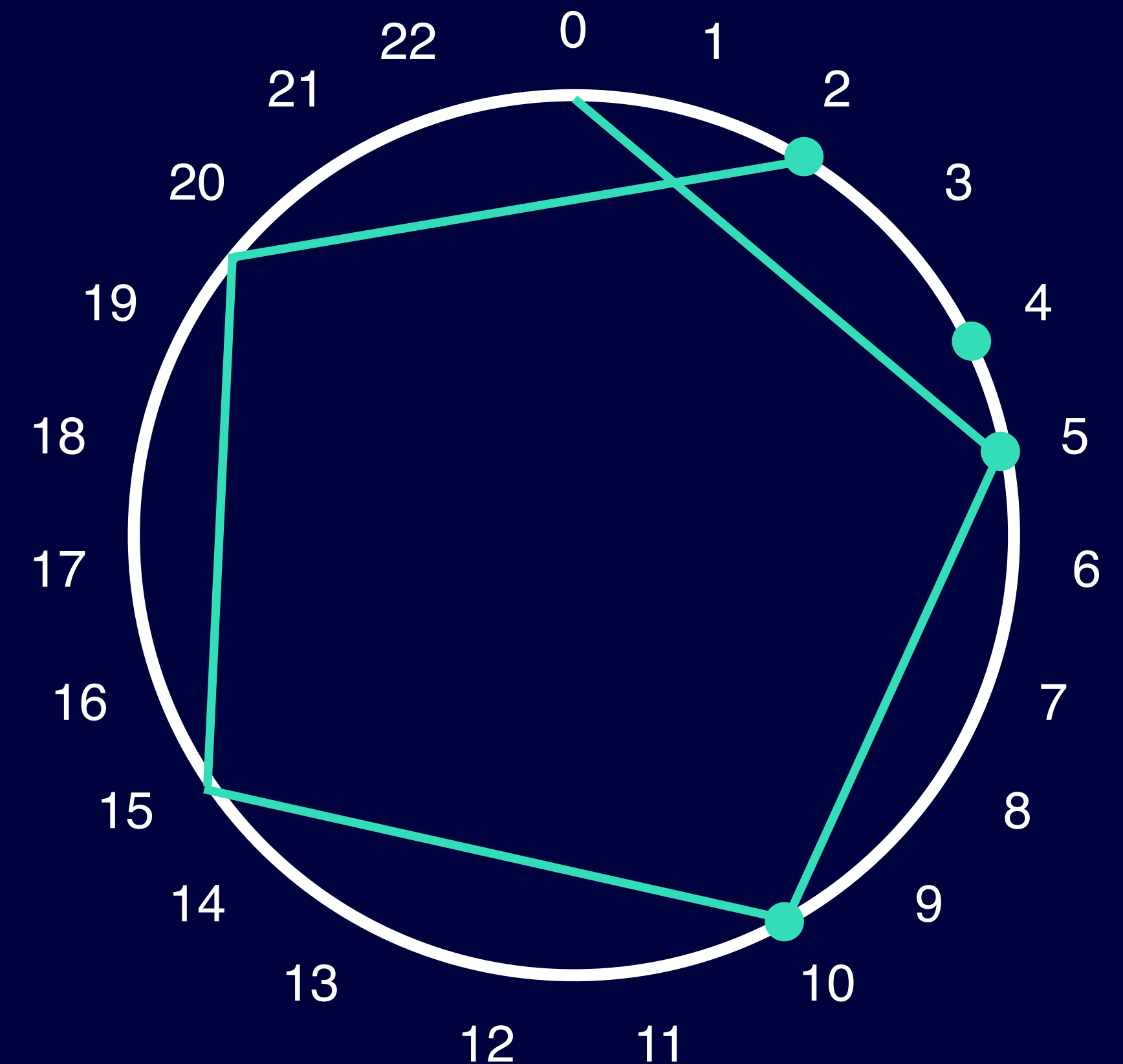
So we divide by  $p = 23$  and compute the remainder

$G^1 \bmod 23 = 5$ ;

$G^2 \bmod 23 = 2$ ;

$G^3 \bmod 23 = 10$ ;

$G^4 \bmod 23 = 4$



# Diffie Hellman Merkle Key Exchange

Alice

Secret key  $a = 6$ ;

Compute public key,

$$A = G^a \bmod p = 5^6 \bmod 23 = 8$$

Compute shared secret key

$$s_a = B^a \bmod p = 19^6 \bmod 23 = 2$$

Public (Eve)

$$p = 23; G = 5;$$

$$A = 8$$

$$B = 19$$

Bob

Secret key  $b = 15$ ;

Compute public key,  $B = 5^{15} \bmod 23 = 19$

Compute shared secret key

$$s_b = A^b \bmod p = 8^{15} \bmod 23 = 2$$

$$\begin{aligned} s_a &= B^a \bmod p \\ &= (G^b \bmod p)^a \bmod p \\ &= G^{ab} \bmod p = s_b \end{aligned}$$



# How to break Diffie Hellman Merkle

We know the base,  $G = 5$ , we know the modulo number  $p = 23$ .

Alice has just sent us her encoded key  $A = 8$ .

Exhaustive search...

$5^1 \bmod 23 = 5$  No!

$5^2 \bmod 23 = 2$  No!

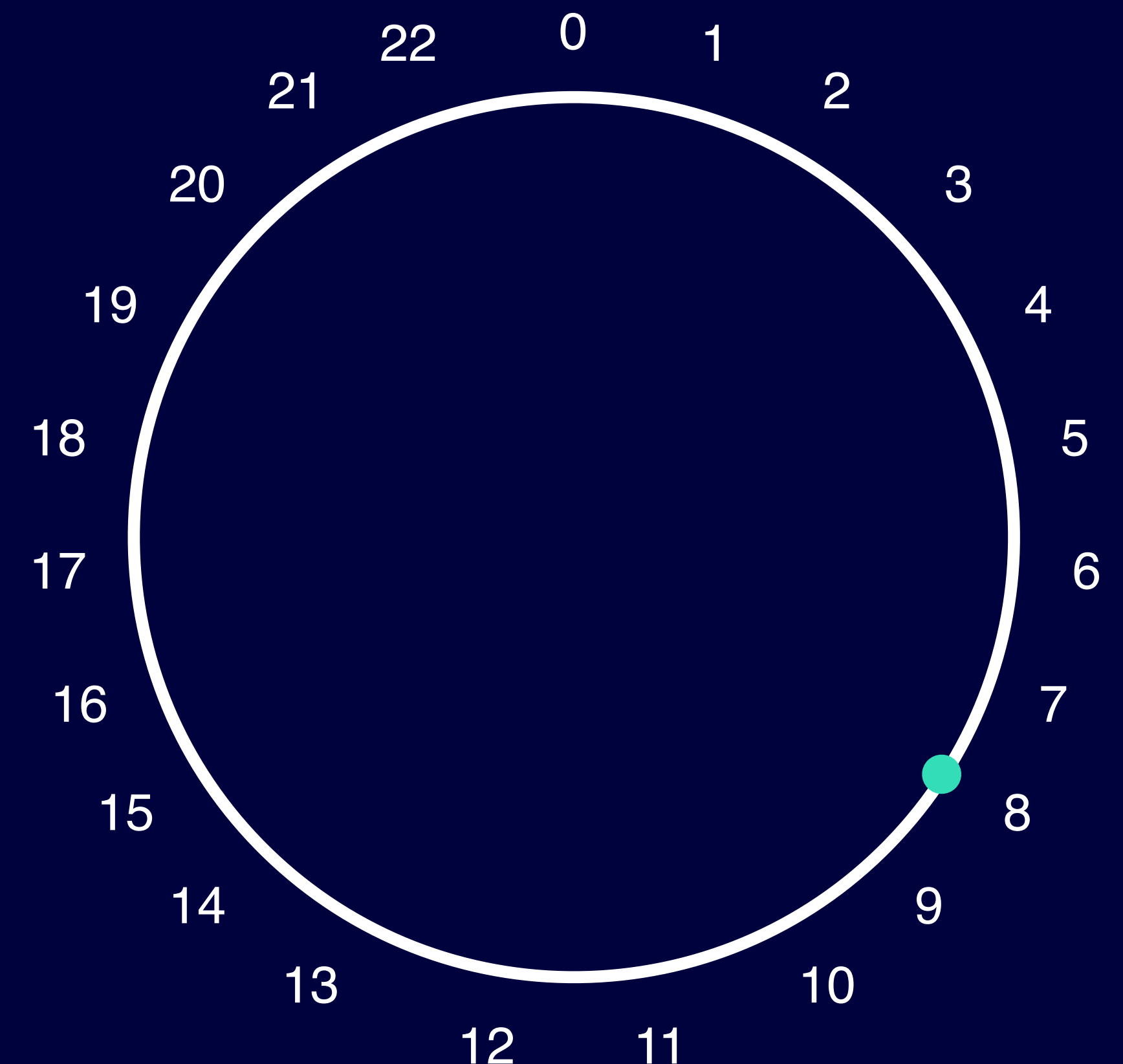
$5^3 \bmod 23 = 10$  No!

$5^4 \bmod 23 = 4$  No!

Ad nauseum! We have to check all combinations. If we assume  $a \leq p$  then we have  $p$  checks to make. The  $q$ th check involves  $q$  multiplications so a full check involves  $p^2$  multiplications.

Note1: if  $p = 23$  then this is not daunting. But a real  $p$  might be ...

15525180923007089351309181312584817556313340494345143132023511  
94902966239949102107258669453876591642442910007680288864229150  
80371891804634263272761303128298374438082089019628850917069131  
6593175367469551763119843371637221007210577919  $\sim 10^{464}$  with  $G = 2$



# Warning

Do not use  $G = 2$ ,

$p =$

1,552,518,092,300,708,935,130,918,131,258,481,755,631,334,049,434,514,313,202,351,194,902,966  
,239,949,102,107,258,669,453,876,591,642,442,910,007,680,288,864,229,150,803,718,918,046,342,  
632,727,613,031,282,983,744,380,820,890,196,288,509,170,691,316,593,175,367,469,551,763,119,8  
43,371,637,221,007,210,577,919

It has probably already been hacked!

Use a longer  $p$ , maybe over 1500 bits long!

**Problem:** as the key gets longer and longer encryption takes longer and longer

**Solution:** instead of using a circle to mix things up (modulo arithmetic) maybe we could use a curve?

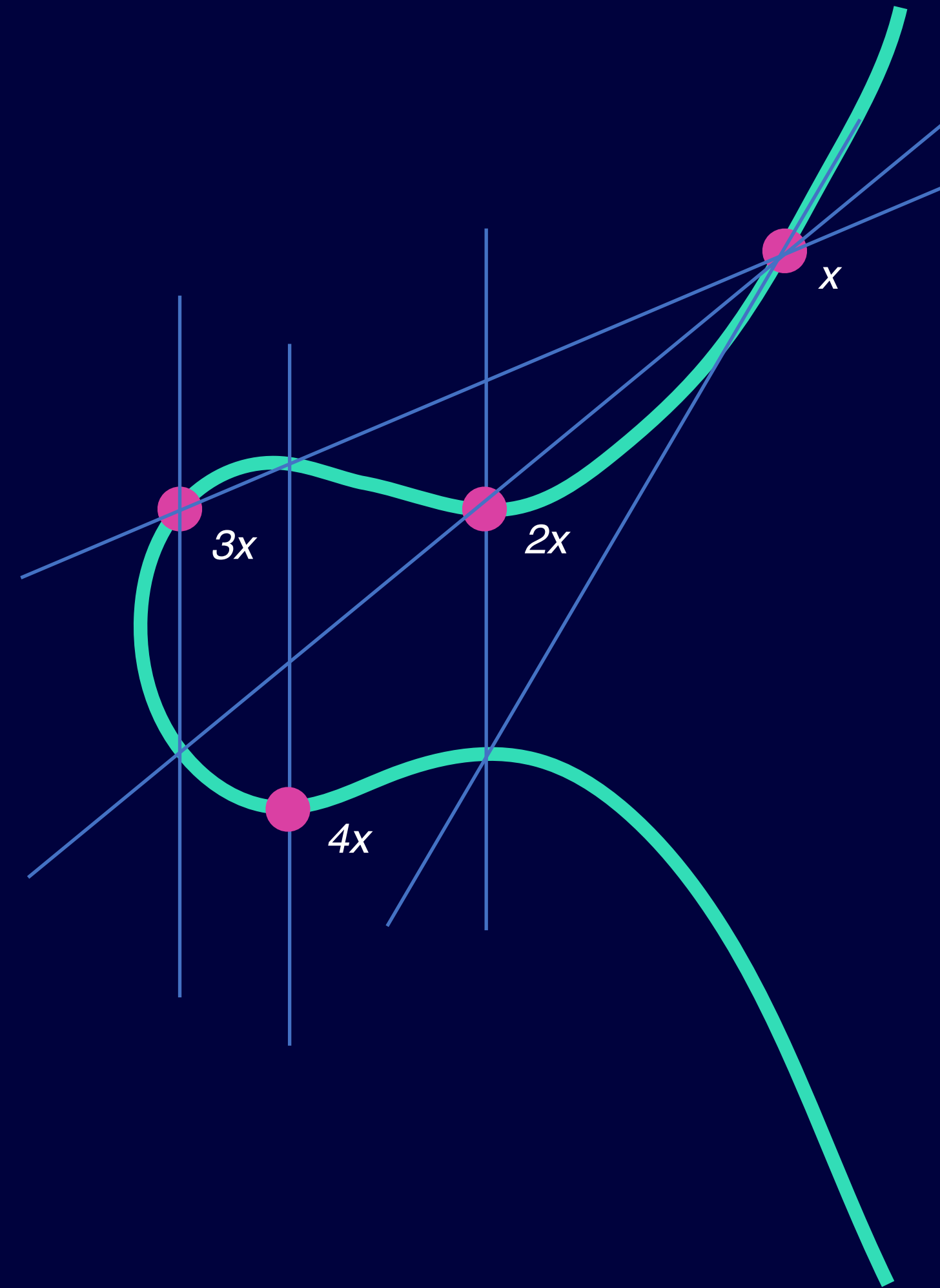


# Elptic curves

More complicated than modulo exponentiation so

- shorter keys
- harder to crack

the “Swiss Army knife of cryptography”



# A brief history of hacking

- Leaving aside professional cryptography...
  - Early 1980s: phone phreaking
  - 1984: Chaos Computer Club
  - 1988 Morris worm
- Early 1990s - internet used for commerce and everything changes.
- Three themes: intellectual curiosity; theft and/or extortion and cyber warfare



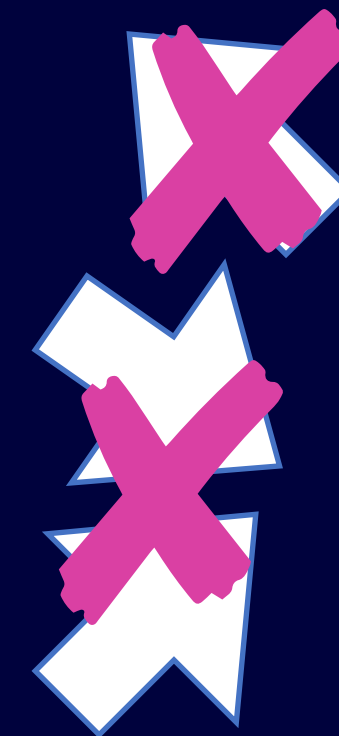
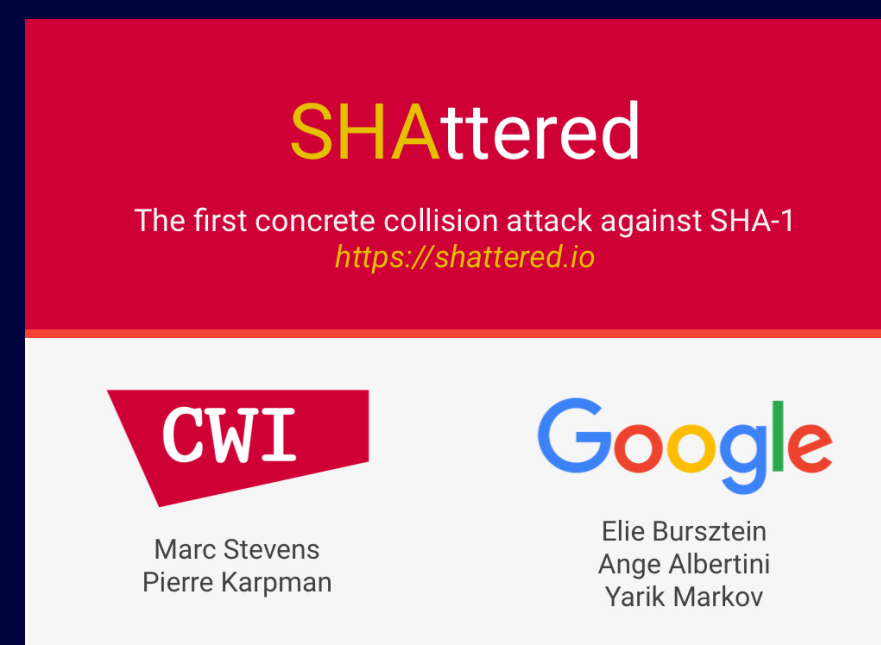
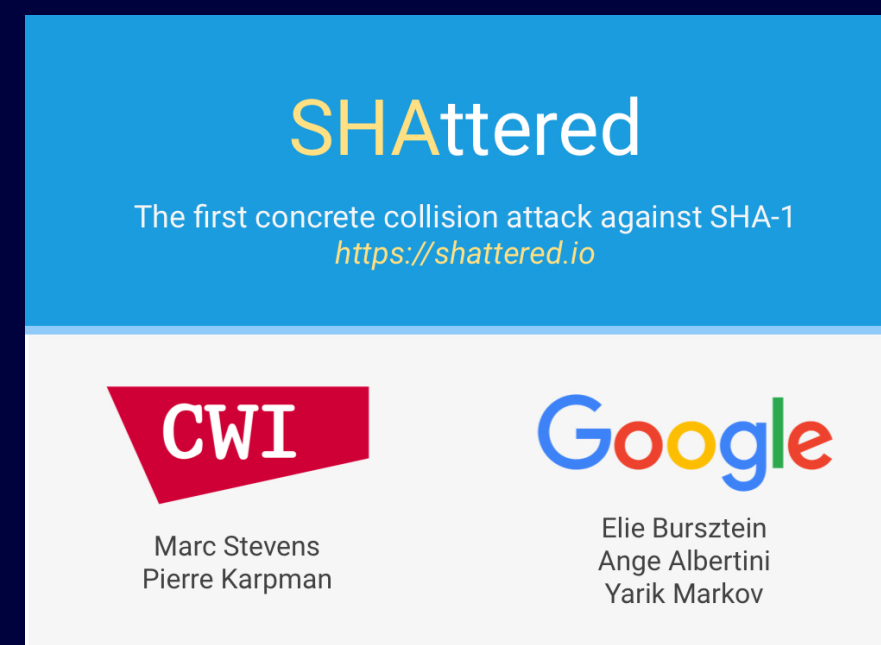
# Hash function

- How can we check that some transmitted data is correct?
- Easy - discussed in previous lecture, we use a check number that travels with the data
  1. Add a One so that the number of digits in the file is even - parity
  2. Sum up the Ones and append the count - a checksum
  3. Generate a string of digits that is a sort of digital finger print for the data.



# Cryptographic hash functions

- No inverse
- No collisions
- SHA-1 broken in 2017



38  
76  
2c  
f7  
f5  
59  
34  
b3  
4d  
17  
9a  
e6  
a4  
c8  
0c  
ad  
cc  
bb  
7f  
0a



# SHA256 Hash function

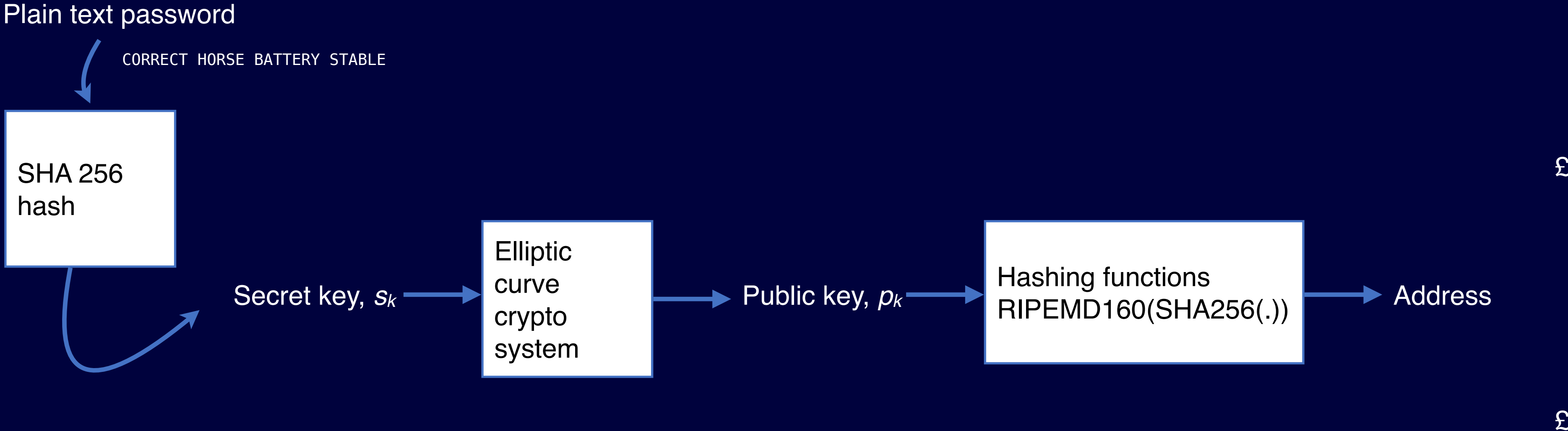
```
57 b0 d6 1d 03 af 07 4f 0c 36 91 fe ff 15 09 36
71 15 f5 2b f5 ab 86 9d 12 42 b8 8b 5a 81 73 d2
0d 97 2b af 85 de 76 bd 5e e3 4a 83 a9 a9 c0 b4
c0 dd f0 c6 b3 62 2e fc 71 e3 0e 8d a4 a7 77 2a
6a 53 d6 ad f5 7e 28 df 63 2f 0e bb 45 0e 7e d9
d3 4f 00 00 00 ff ff 03 00 50 4b 03 04 14 00 06
00 08 00 00 00 21 00 37 d7 51 f7 25 70 00 00 e6
e1 02 00 11 00 00 00 77 6f 72 64 2f 64 6f 63 75
6d 65 6e 74 2e 78 6d 6c ec 7d db 6e e3 c8 92 e0
fb 02 fb 0f 84 17 58 74 c3 76 89 a4 44 4a f2 99
ae 06 75 f3 55 be c8 b2 5d ae dd c5 80 22 93 12
6d de cc 8b 64 79 b0 40 ff c3 3c 0d 70 e6 e7 fa
4b 36 22 92 94 28 59 56 b9 aa 2c da dd b3 85 73
da 12 49 05 33 23 e3 1e 91 ff f2 fb a3 eb 08
63 16 46 b6 ef fd b6 25 7d 12 b7 04 e6 19 be 69
7b c3 df b6 ae fa 9d dd da 96 10 c5 ba 67 ea 8e
ef b1 df b6 a6 2c da fa fd f3 7f ff 6f ff 32 d9
33 7d 23 71 99 17 0b 00 c2 8b f6 26 81 f1 db d6
28 8e 83 bd 52 29 32 46 cc d5 a3 4f ae 6d 84 7e
e4 5b f1 27 c3 77 4b be 65 d9 06 2b 4d fc d0 2c
c9 a2 24 d2 a7 20 f4 0d 16 45 f0 be a6 ee 8d f5
68 2b 05 67 3c be 0e 9a 19 ea 13 f8 31 02 ac 94
8c 91 1e c6 ec 71 0e 43 fa 6e 20 4a a9 5e aa 3d
07 24 ff 00 20 98 a1 2c 3d 07 55 fe 6e 50 6a 09
47 f5 0c 50 e5 87 00 c1 a8 9e 41 52 7e 0c d2 8a
c9 a9 3f 06 49 7e 0e a9 fa 63 90 ca cf 21 d5 7e
0c d2 33 72 72 9f 13 b8 1f 30 0f 6e 5a 7e e8 ea
31 7c 0d 87 25 57 0f ef 93 60 17 00 07 7a 6c 0f
6c c7 8e a7 00 53 54 33 30 ba ed dd ff c0 88 e0
57 33 08 6e d9 fc 6e 08 d5 92 eb 9b cc 29 9b 19
14 ff b7 ad 24 f4 f6 d2 df ef ce 7e 8f 43 df e3
bf 4f ff 64 bf 08 5f 33 7f fe 93 56 ca 1c 68 e6
a5 90 39 80 0b df 8b 46 76 30 db e1 ee 8f 42 83
9b a3 0c c8 78 dd 24 c6 ae 93 3d 37 09 a4 57 6e
97 97 d8 53 8b a3 72 0e f0 35 c3 4f f1 ef 3a 7c
e4 eb 21 4a e2 2b 56 04 41 cc 7e f1 9a 21 2c be
33 1b 89 0b 54 38 7f f1 0f a1 26 87 5c e9 95 0c
```



d6e7c4bdba6e95522b6a3e9263c78d3496306e16662485929e15f1ebc3eb56a1

1. Not broken (yet)
2. Longer hash
3. Still speedy
4. Commonly used

# Crypto-currency hashes



E9873D79C6D87DC0FB6A5778633389\_SAMPLE\_PRIVATE\_KEY\_DO\_NOT\_IMPORT\_F4453213303DA61F20BD67FC233AA33262

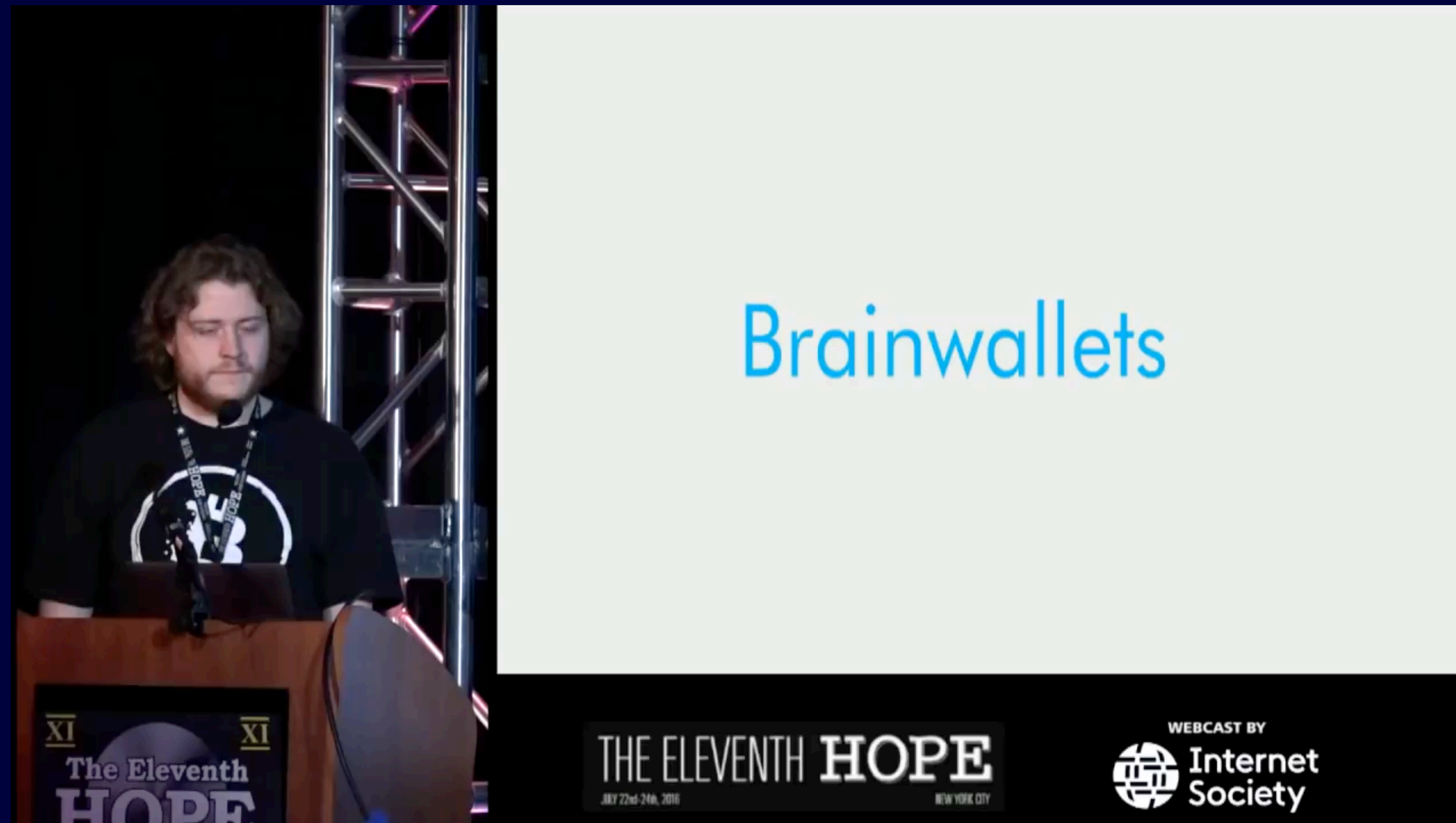
0450863AD64A87AE8A2FE83C1AF1A8403CB53F53E486D8511DAD8A04887E5B23522CD470243453A299FA9E77237716103ABC11A1DF38855ED6F2EE187E9C582BA6

17VZNX1SN5NtKa8UQFxbFeFc3iqRYhem

Bitcoin

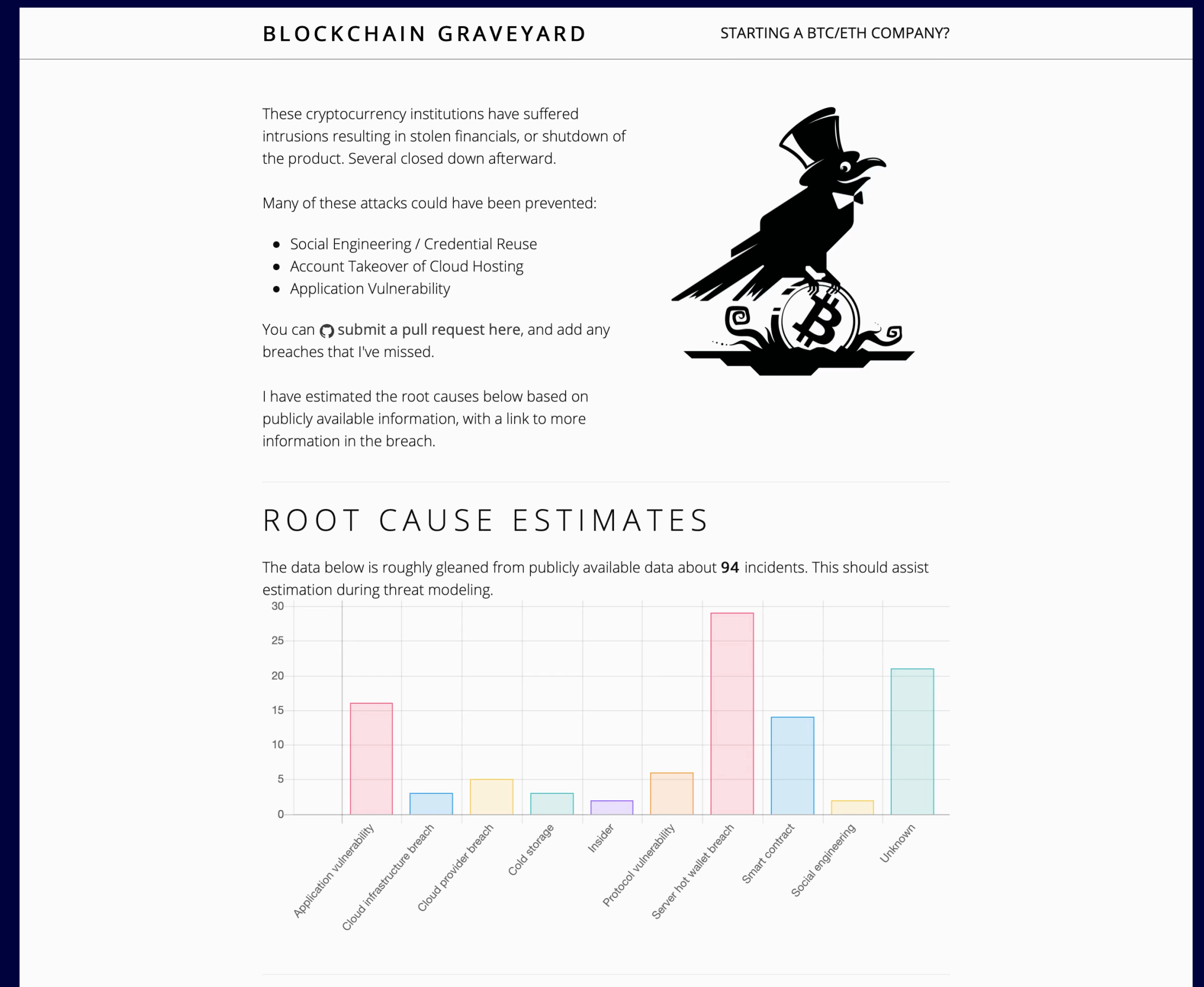


# Bad crypto hashes



# Public ledger attacks

- Lend themselves to “birthday problem” type attacks
- And each “hit” has a monetary reward



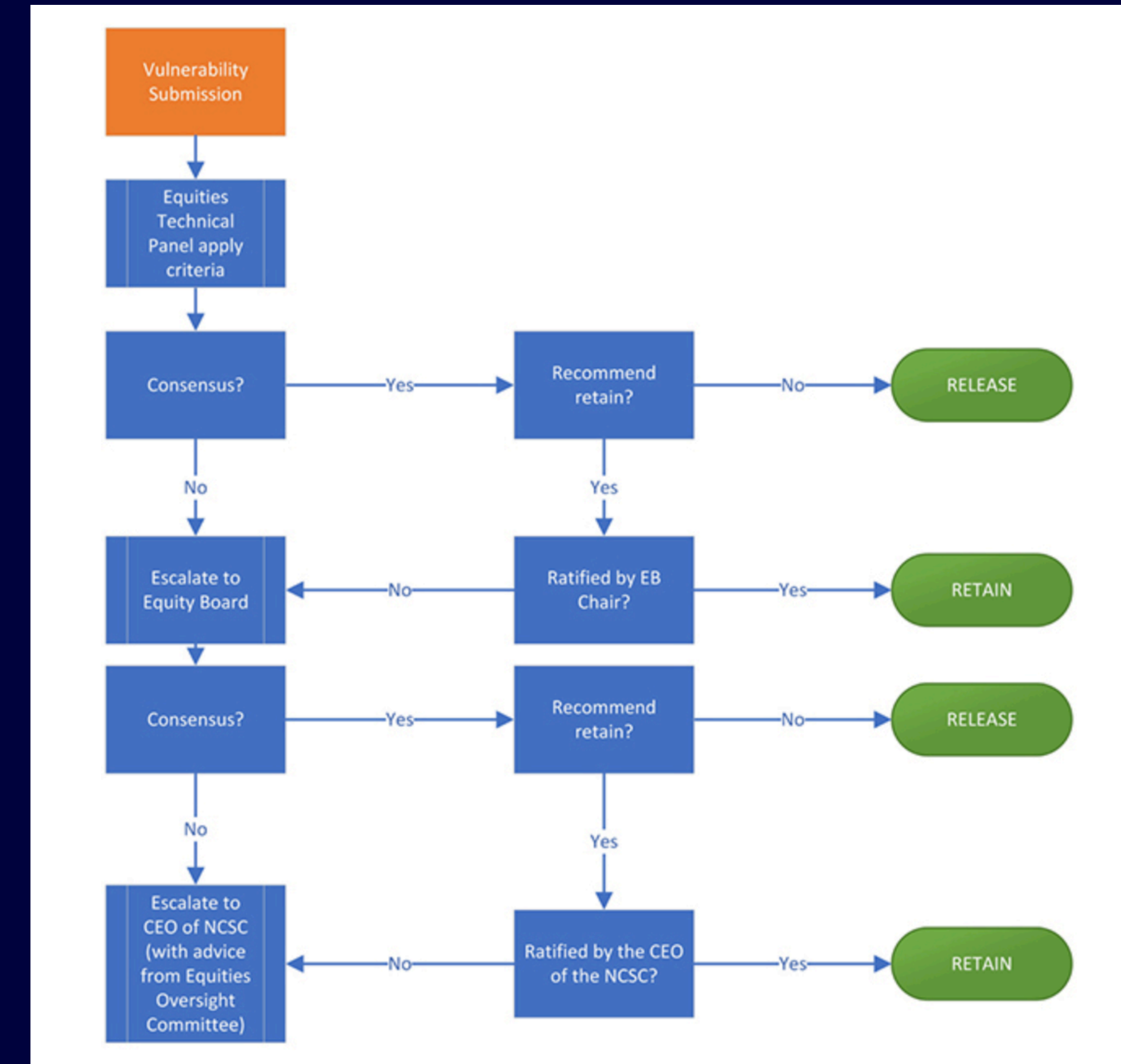


# State actors

- Snowden leaks describe three types of activity
  1. Code breaking
  2. Industrial espionage - creation of vulnerabilities
  3. Hacking - collecting and looking

# Vulnerabilities Equities Process

- Zero day vulnerabilities - vulnerabilities that the manufacturer is unaware of (but is known to someone)
- Should the state hoard knowledge of such vulnerabilities?
- A new twist on the classic ethical dilemma of intelligence gathering...
- Is it possible to gather intelligence that is so valuable that it cannot be revealed?





# Last week's news

Search quotes, news & videos

SIGN IN

MARKETS

BUSINESS

INVESTING

TECH

POLITICS

CNBC TV

WATCHLIST

PRO

MAKE IT

USA

INTL

16-19 JUNE PARIS ONLINE

VIVA TECHNOLOGY

MEET UP WITH ATTENDEES FROM 125 COUNTRIES

GET YOUR PASS

TECH

Hackers behind Colonial Pipeline attack reportedly received \$90 million in bitcoin before shutting down

PUBLISHED TUE, MAY 18 2021-9:04 AM EDT | UPDATED 3 MIN AGO

Ryan Browne  
@RYAN\_BROWNE\_

SHARE

f

t

in

e

KEY POINTS

- DarkSide, the hacker group behind the Colonial ransomware attack, received \$90 million in bitcoin ransom payments, according to blockchain sleuths Elliptic.
- The cybercriminal gang shut down last week after losing access to its servers and as its cryptocurrency wallets were emptied.
- Elliptic said DarkSide's bitcoin wallet contained \$5.3 million worth of the digital currency before its funds were drained.

yahoo!news

## NEWS

Home | Coronavirus | Brexit | UK | World | Business | Politics | Tech | Science | Health | Family & Education

World | Africa | Asia | Australia | Europe | Latin America | Middle East | US & Canada

## Cyber-crime: Irish health system targeted twice by hackers

2 days ago



GETTY IMAGES

Ireland's Department of Health and the Health Service Executive have both been targeted by hackers

**Ireland's healthcare system has twice been targeted in cyber-crime attacks, it has been confirmed.**

The Department of Health said it shut down its IT systems after a ransomware attack on Thursday.

A similar attack on the Health Service Executive (HSE) on Friday caused "substantial" cancellations to outpatient services.

The same cyber-crime group is believed to be behind both incidents, **RTÉ** has reported.

# The role of LEAs

“Sadly, at a time when we need to be taking more action, Facebook are pursuing end-to-end encryption plans that place the good work and progress achieved so far in jeopardy ... This is not acceptable. We cannot allow a situation where law enforcement’s ability to tackle abhorrent criminal acts and protect victims is severely hampered.”

Pritti Patel, 19th April 2021

“The hack on Solar Winds has shown that state actors have significant capability. We need to be able to understand that threat, protect ourselves from it, and bolster our cyber resilience. While addressing the danger from state and state-sponsored actors, it is rightly a key priority. We also know that criminal groups have the intent and technical means to operate in cyber space.”

Pritti Patel speech to CyberUk Conference 11th May 2021



By Richard Townshend - <https://members-api.parliament.uk/api/Members/4066/Portrait?cropType=OneOneGallery>; <https://members.parliament.uk/member/4066/portrait>, CC BY 3.0, <https://commons.wikimedia.org/w/index.php?curid=86678234>



# Quo vadis security?

- Public confusion over privacy rights versus security
- Western governments in denial over strong encryption
- Two recent features:
  - huge financial wins for successful hacks;
  - government sponsored hacking.
- Maybe wait a while before investing in bitcoin?



# And...if you fancy getting rich quick...



The teenage millionaire hacker - BBC News. Available on YouTube at <https://www.youtube.com/watch?v=J4ElhxxLUk8>

# Next season

*Six tech inventions that changed the world*

October 2021

Thanks and kudos to the Worshipful Company of Information Technologists who sponsor these lectures.

Special thanks to Laurie Mercer from HackerOne for talking me through some of the examples in this talk.